«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)

Направление	09.04.04 - Программная инженерия
Программа	Разработка распределённых программных систем
Факультет	КТИ
Кафедра	МО ЭВМ

К защите допустить

Зав. кафедрой, к.т.н. К.В. Кринкин

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА МАГИСТРА

Тема: РАЗРАБОТКА СИСТЕМЫ ВЫЯВЛЕНИЯ АНОМАЛИЙ В ПОВЕДЕНИИ СОТРУДНИКОВ ОРГАНИЗАЦИИ НА ОСНОВЕ ДАННЫХ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Студент		_____ *подпись*	Волков А.А.
Руководитель	к.т.н., доцент	_____ *подпись*	Новикова Е.С.
Консультанты	д.э.н., доцент	_____ *подпись*	Медынская И.В.
	к.т.н.	_____ *подпись*	Яновский В.В.

Санкт-Петербург

2018

ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Утверждаю

Зав. кафедрой МО ЭВМ

_____ Кринкин К.В.

«___»_____2018 г.

Студент Волков А.А. Группа 2304

Тема работы: Разработка системы выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа.

Место выполнения ВКР: СПбГЭТУ «ЛЭТИ».

Исходные данные (технические требования): Разработать программную систему для выявления нестандартного поведения сотрудников организации на основе данных системы контроля доступа (СКУД).

Содержание ВКР: Обзор современного состояния вопроса, выбор методов распознавания аномалий, разработка системы, анализ результатов.

Перечень отчетных материалов: пояснительная записка, презентация.

Дополнительные разделы: Составление бизнес-плана по коммерциализации результатов НИР магистранта.

Дата выдачи задания		Дата представления ВКР к защите
«___»_____2018 г.		«___»_____2018 г.
Студент	_____	Волков А.А.
Руководитель	к.т.н., доцент _____	Новикова Е.С.
Консультанты	д.э.н., доцент _____	Медынская И.В.
	к.т.н. _____	Яновский В.В.

КАЛЕНДАРНЫЙ ПЛАН ВЫПОЛНЕНИЯ
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Утверждаю

Зав. кафедрой МО ЭВМ

_____ Кринкин К.В.

«___»_____2018 г.

Студент Волков А.А Группа 2304

Тема работы: Разработка системы выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа.

№ п/п	Наименование работ	Срок выполнения
1	Обзор литературы по теме работы	15.03 – 26.03
2	Определение и разработка основных модулей реализуемой системы	27.03 – 02.05
3	Запуск и тестирование системы. Анализ полученных результатов	02.05 – 25.05
4	Оформление пояснительной записки	26.05 – 25.05
5	Оформление иллюстративного материала	25.05 – 01.06

Студент _____ Волков А.А.

Руководитель к.т.н., доцент _____ Новикова Е.С.

РЕФЕРАТ

Пояснительная записка 70 стр., 14 рис., 8 табл., 30 ист.

РАЗРАБОТКА СИСТЕМЫ ВЫЯВЛЕНИЯ АНОМАЛИЙ В ПОВЕДЕНИИ СОТРУДНИКОВ ОРГАНИЗАЦИИ НА ОСНОВЕ ДАННЫХ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Объектом исследования являются данные системы контроля доступа.

В данной выпускной квалификационной работе реализована задача по выявлению аномалий в поведении сотрудников на основе анализа журнала системы контроля доступа.

В данном проекте автоматизируются процессы анализа журналов системы контроля доступом. Показаны основные цели и задачи по построению таблиц аномального взаимодействия пользователей и результаты работы.

ABSTRACT

Physical access control and management systems (PACS) are now widely used by various institutions and businesses. They help to prevent unauthorized access of people, vehicles and other objects to the territory of the organization in order to provide anti-criminal protection.

The main task of such systems is to monitor and control the visits of employees, their movements, to detect and prevent threats. The most important data from PACS is: the duration of the working day, time and amount of delay, and location employees. Analysis of these data will allow diagnosing various anomalies that may indicate such threats as financial fraud, targeted attacks and unauthorized access to computer systems.

This paper presents an approach to the employees' interaction patterns formation and its possible anomalies identification. The approach is based on statistical analysis of employees' meetings, their duration and number. The developed system automates the processes of the physical access control system (PACS) log analysis.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей пояснительной записке применяют следующие термины с соответствующими определениями:

ЛЭТИ – Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) СПбГЭТУ;

ВУЗ – высшее учебное заведение;

ВКР - выпускная квалификационная работа;

БД - база данных;

ИС – информационная система;

ЖЗ – жизненный цикл;

СКУД – Средства и системы контроля и управления доступом;

Журнал СКУД (логи) – записи, содержащие временные метки, идентификатор доступа сотрудника и идентификатор котроллера доступа;

Временной интервал – время, в течение которого в данной точке доступа устанавливается заданный режим доступа;

Доступ – перемещение людей (объектов) в (из) зоны доступа;

Зона доступа – здание, помещение, территория, вход и (или) выход которых оборудованы средствами контроля и управления доступом (КУД);

Идентификатор доступа - уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код — предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак. Такие признаки как ФИО, должность или условные обозначения заносится в виде кодовой информации на карты, электронные ключи, брелоки и др. устройства;

Контроллер доступа (КД) - прибор приемно-контрольный доступа (ППКД): Аппаратное устройство в составе средств управления СКУД (турникеты, шлюзовые кабины, электромагнитные замки и считыватели);

Несанкционированный доступ – доступ субъектов или объектов, не имеющих право доступа;

Пользователь СКУД (сотрудник) – субъект, в отношении которого осуществляется мероприятия по контролю доступа.

.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Системы контроля и управления доступом (СКУД) сегодня широко используются различными учреждениями [1]. Они помогают предотвращать несанкционированный доступ людей, транспорта и других объектов на территорию предприятия или организации в целях обеспечения противокриминальной защиты [13][14][15].

Основной задачей таких систем является контроль посещения сотрудниками предприятия, их перемещений, обнаружение и предотвращение внутренних угроз, представляющих опасность для организации. Самыми важными являются такие получаемые от СКУД данные, как: продолжительность рабочего дня, время и количество опозданий, и местоположение сотрудников. Анализ этих данных позволит в дальнейшем выявить различные аномалии, которые могут свидетельствовать о таких угрозах, как внутренние нарушители, финансовые мошенничества, целенаправленные атаки и несанкционированный доступ к компьютерным системам [16][17].

В настоящей работе представлен подход к формированию шаблонов взаимодействия и выявления возможных аномалий в них. В основе подхода лежит статистический анализ встреч сотрудников, их продолжительность и количество. Разработанная система автоматизирует процессы анализа журналов системы контроля доступом.

Исходными данными при разработке программного обеспечения (ПО) являются записи в журналах СКУД. Каждая запись представлена следующим образом: «идентификатор пользователя, временная метка, зона».

Цель исследовательской работы – реализовать методики анализа взаимодействия сотрудников предприятия.

Для выполнения поставленной цели необходимо решить ряд задач:

1. Проанализировать существующие методики выявления аномалий в поведении сотрудников.
2. Определить методы автоматического анализа данных с учетом специфики предметной области.
3. Разработать систему выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа.

Описать результаты, полученные в ходе исследования на реальных данных, и определить направления дальнейших исследований.

ГЛАВА 1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ И ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К РАЗРАБОТКЕ

1.1 Описание задач системы

В качестве объекта исследования рассматривается процесс выявления аномалий в поведении сотрудников организации на основе анализа журнала системы контроля доступа.

1.1.1 Описание предметной области, для которой разрабатывается ПО

Системы контроля и управления доступом (СКУД) сегодня широко используются различными учреждениями. Они помогают предотвращать несанкционированный доступ людей, транспорта и других объектов на территорию предприятия или организации в целях обеспечения противокриминальной защиты [12][29].

Принцип работы СКУД заключается в обеспечении безопасности на предприятии с помощью программно-аппаратных технических средств [1]. Последние могу ограничивать вход-выход с различных контролируемых зон, регистрировать новые объекты (людей, транспорт). Пример средства контроля и управления доступом (самым распространённым на предприятиях является турникет) представлен на рисунке 1.

Рисунок 1 – Турникет

Основной задачей таких систем является идентификация сотрудников, имеющих доступ в зону доступа, ограничение их перемещений, контроль посещения предприятия, обнаружение и предотвращение внутренних угроз, представляющих опасность для организации. Дополнительно некоторые СКУД могут учитывать рабочее время, рассчитывать заработную плату при условии настройки работы с системами бухгалтерского учёта, хранить информацию о каждом сотруднике и посетителе и взаимодействовать с системами безопасности, например, с системами видеонаблюдения, охранной сигнализации и системой пожаротушения.

Самыми важными являются такие получаемые от СКУД данные, как: продолжительность рабочего дня, время и количество опозданий, и местоположение сотрудников. Анализ этих данных позволит в дальнейшем выявить различные аномалии, которые могут свидетельствовать о таких угрозах, как внутренние нарушители, финансовые мошенничества, целенаправленные атаки и несанкционированный доступ к компьютерным системам [23][28]. Пример записей журнала посещений (логов) приведён на рисунке 2 [18].

```
earpa,60,Arpa,Emile,Facilities,1070,2016-05-31 05:57:40,fixed-prox,earpa001,1,6
vawelon,61,Awelon,Varro,Facilities,1070,2016-05-31 05:57:41,fixed-prox,vawelon001,1,6
jsanjorge,57,Sanjorge Jr.,Sten,Executive,3000,2016-05-31 07:00:50,fixed-prox,jsanjorge001,1,4
ibarranco,50,Barranco,Ingrid,Executive,3120,2016-05-31 07:00:51,fixed-prox,ibarranco001,1,4
jsanjorge,57,Sanjorge Jr.,Sten,Executive,3000,2016-05-31 07:01:32,fixed-prox,jsanjorge001,2,4
ibarranco,50,Barranco,Ingrid,Executive,3120,2016-05-31 07:01:32,fixed-prox,ibarranco001,2,4
jsanjorge,57,Sanjorge Jr.,Sten,Executive,3000,2016-05-31 07:02:03,fixed-prox,jsanjorge001,3,4
ibarranco,50,Barranco,Ingrid,Executive,3120,2016-05-31 07:02:03,fixed-prox,ibarranco001,3,4
jsanjorge,57,Sanjorge Jr.,Sten,Executive,3000,2016-05-31 07:02:28,fixed-prox,jsanjorge001,3,6
knielson,35,Nielson,Karole,Engineering,2550,2016-05-31 07:15:50,fixed-prox,knielson001,1,4
knielson,35,Nielson,Karole,Engineering,2550,2016-05-31 07:16:32,fixed-prox,knielson001,2,4
iborrasca,20,Borrasca,Isande,Engineering,2355,2016-05-31 07:17:38,fixed-prox,iborrasca001,1,4
ldedos,26,Dedos,Lidelse,Engineering,2100,2016-05-31 07:17:38,fixed-prox,ldedos001,1,4
iborrasca,20,Borrasca,Isande,Engineering,2355,2016-05-31 07:18:19,fixed-prox,iborrasca001,2,4
ldedos,26,Dedos,Lidelse,Engineering,2100,2016-05-31 07:18:19,fixed-prox,ldedos001,2,4
ldedos,26,Dedos,Lidelse,Engineering,2100,2016-05-31 07:18:37,fixed-prox,ldedos001,2,2
iborrasca,20,Borrasca,Isande,Engineering,2355,2016-05-31 07:18:43,fixed-prox,iborrasca001,2,6
sparrino,41,Parrino,Silvio,Engineering,2125,2016-05-31 07:24:35,fixed-prox,sparrino001,1,4
sparrino,41,Parrino,Silvio,Engineering,2125,2016-05-31 07:25:16,fixed-prox,sparrino001,2,4
monda,38,Onda,Marin,Engineering,2400,2016-05-31 07:28:35,fixed-prox,monda001,1,4
monda,38,Onda,Marin,Engineering,2400,2016-05-31 07:29:16,fixed-prox,monda001,2,4
monda,38,Onda,Marin,Engineering,2400,2016-05-31 07:29:35,fixed-prox,monda001,2,2
lorosco,55,Orosco,Lenna,Executive,3320,2016-05-31 07:31:35,fixed-prox,lorosco001,1,4
ostrum,58,Strum,Orhan,Executive,3200,2016-05-31 07:31:35,fixed-prox,ostrum001,1,4
lorosco,55,Orosco,Lenna,Executive,3320,2016-05-31 07:32:06,fixed-prox,lorosco001,2,4
ostrum,58,Strum,Orhan,Executive,3200,2016-05-31 07:32:06,fixed-prox,ostrum001,2,4
epavone,13,Pavone,Emma,Administration,3150,2016-05-31 07:32:20,fixed-prox,epavone001,1,4
lorosco,55,Orosco,Lenna,Executive,3320,2016-05-31 07:32:37,fixed-prox,lorosco001,3,4
ostrum,58,Strum,Orhan,Executive,3200,2016-05-31 07:32:37,fixed-prox,ostrum001,3,4
epavone,13,Pavone,Emma,Administration,3150,2016-05-31 07:33:01,fixed-prox,epavone001,2,4
ostrum,58,Strum,Orhan,Executive,3200,2016-05-31 07:33:02,fixed-prox,ostrum001,3,6
ostrum,58,Strum,Orhan,Executive,3200,2016-05-31 07:33:10,fixed-prox,ostrum001,3,3
epavone,13,Pavone,Emma,Administration,3150,2016-05-31 07:33:32,fixed-prox,epavone001,3,4
epavone,13,Pavone,Emma,Administration,3150,2016-05-31 07:33:46,fixed-prox,epavone001,3,2
```

Рисунок 2 – Логи СКУД предприятия за 2 часа работы

Основная информация для анализа поведения идёт от контролёров доступа. Они используются на проходных предприятий Сотрудник организации или её посетитель должны иметь личный идентификатор (карточка, брелок), который взаимодействует со считывателем СКУД. Человек предъявляет идентификатор, СКУД сравнивает считанный код с хранящимся в базе и записывает данные в журнал учёта посещений.

Информацию с идентификаторов доступа получают считыватели. Некоторые т.н. «таблетки» представляют собой два контакта, для proximity-карты — это электронная плата с антенной в корпусе, а для считывания, например, рисунка радужной оболочки глаза в состав считывателя должна

входить камера. К ним могут применяться различные условия и ограничения, например, уличные считыватели должны выдерживать климатические нагрузки — перепады температур, осадки — особенно, если речь идет об объектах в районах с суровыми климатическими условиями. А если существует угроза вандализма, необходима ещё и механическая прочность (стальной корпус) [5].

Основой автоматизированного контроля доступа является СКУД. Она занимается сбором, хранением, изменением и анализом всей информации о сотрудниках и их перемещениях по предприятию. СКУД может быть установлена как на один, так и на несколько ПК, объединённых в сеть [5].

Применение таких систем разнообразно: офисы компаний, бизнес-центры, банки, учреждения образования (школы, техникумы, вузы), промышленные предприятия, охраняемые территории, автостоянки, парковки, места проезда автотранспорта, частные дома, жилые комплексы, коттеджи, гостиницы, общественные учреждения (спорткомплексы, музеи, метрополитен и др.) [2][22][23].

1.1.2 Описание проблемы, которую необходимо решить

Проблема: Автоматическое выявление аномалий в поведении сотрудников организации на основе данных, получаемых из журналов учёта посещений системы контроля доступа.

Такой поиск аномалий затруднён из-за количества записей в журналах учёта и нечётким определением формулировок. Например, основным шаблоном поведения является встреча двух и более сотрудников. В таком случае сложно оценить лишь по данным журналов СКУД [1], сколько человек имели контакт. Вторая сложность состоит в большой (больше двух) размерности таблиц для поиска аномалий. При построении матрицы встреч необходимо учитывать как минимум следующие параметры: идентификатор

сотрудника, время встречи, помещение и этаж здания. Всё это делает алгоритмы поиска аномалий сложными.

На абстрактном уровне аномалия определяется как шаблон, не соответствующий ожидаемому нормальному поведению объекта. Прямой подход к обнаружению аномалий в траекториях подразумевает поиск шаблонов, определяющих области нормального поведения объектов. Любые наблюдения в данных, которые не относятся к таким областям, интерпретируются как аномальные.

В случае отсутствия каких-либо априорных данных о типичном поведении (движении) объектов, для анализа траекторий часто применяются алгоритмы кластеризации данных [27]. Полученные кластеры используются в дальнейшем для описания модели нормального поведения объектов, на основе которой производится последующее обнаружение аномалий [24]. Она позволяет оценить разницу в поведении объектов, построить шаблоны типичного поведения и определить временные и пространственные атрибуты, соответствующие сильным отклонениям от нормы [19][20][21].

1.1.3 Состояние и стратегия развития схожих решений

Статья [3] приводит данные о том, что уже в 2010 году более 70% американских компаний отслеживали поведение сотрудников с помощью видеонаблюдения, ведения учёта посещений интернет страниц и электронной почты. На данный момент на рынке представлены десятки компаний, которые предоставляют свои решения для контроля работы сотрудников [4]. Большинство из них основаны на анализе, набираемого на компьютере, текста, активности в интернете и учёта времени нахождения на рабочем месте.

Системы контроля сотрудников делятся на три основных типа. Первые kickidler [https://www.kickidler.com/]— делают основной упор на записи

действий персонала за компьютером на видео, онлайн-наблюдение и контроль нарушений. Безусловным плюсом такого подхода является тот факт, что от видео спрятаться невозможно. Минус – для хранения видео необходимо достаточное место на диске (как утверждает производитель, от 190 Мб до 1,2 Гб в день на сотрудника в зависимости от того, чем он непосредственно занят на рабочем месте). Пример работы программы Kickidler представлен на рисунке 3.

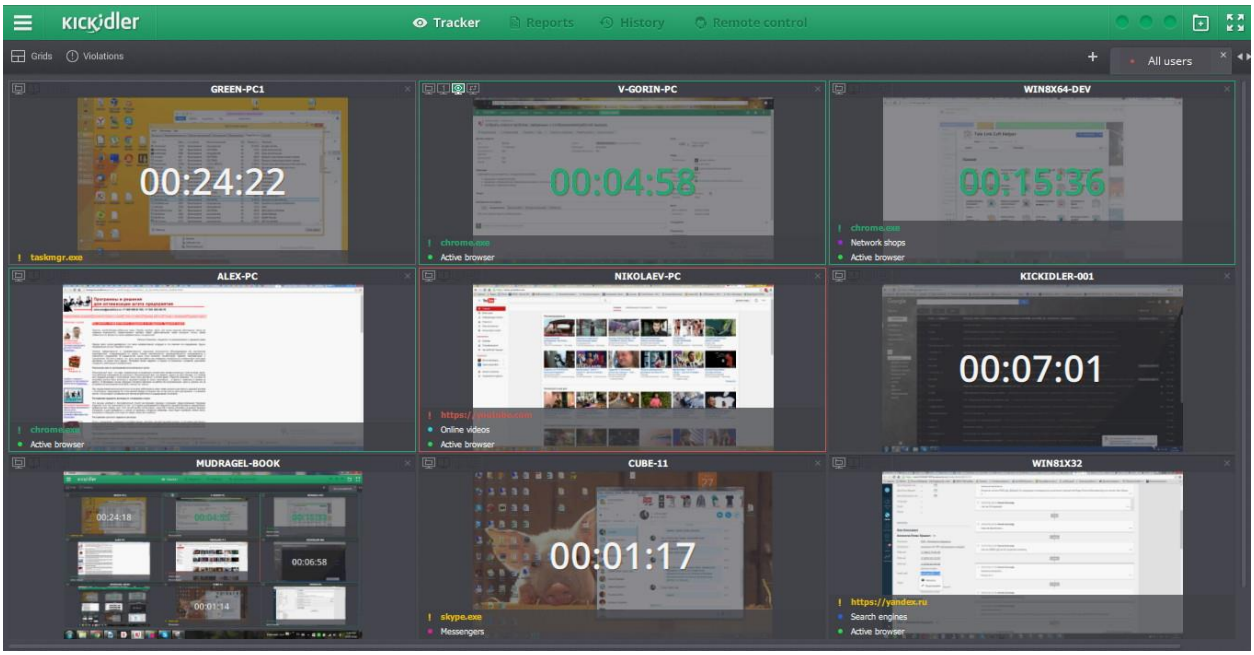

Рисунок 3 – Слежение за работой компьютеров сотрудников

Другие — StaffCop [https://www.staffcop.com/], Lanagent [http://www.lanagent.com/] и Стахановец [https://stakhanovets.ru/] – собирают максимальный объём данных о действиях пользователя (письма, файлы, сообщения) и предлагают использовать для их анализа отчёты. Плюс такого похода в том, что путём поиска по полученным и отправленным письмам, сообщениям и прочему можно найти возможные нарушения сотрудника. Минус – очень тяжело проанализировать большой объем информации. Пример работы таких программ приведён на рисунке 4.

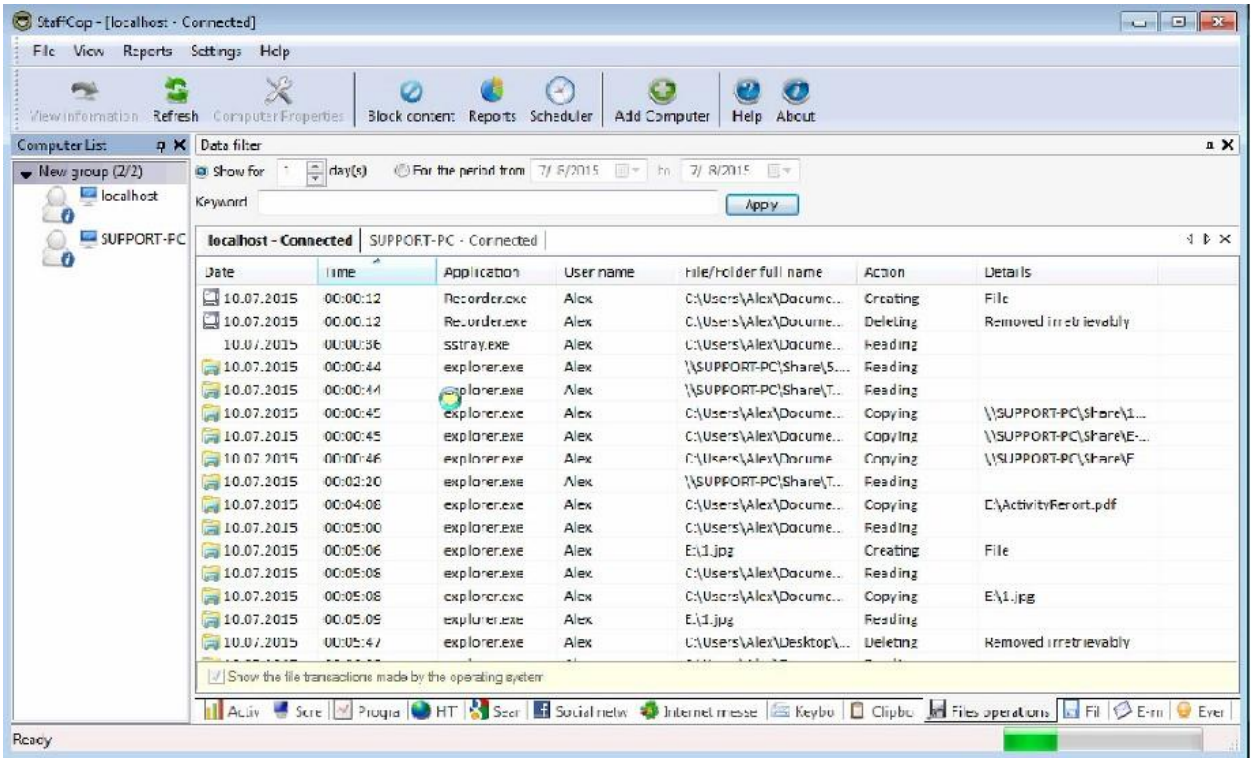

Рисунок 4 – Слежение за файлами, с которыми работает пользователь

Третья группа — сохраняют минимум данных: только посещённые сайты и запущенные программы. Такие программы, к которым относятся CrocoTime [https://crocotime.com/en/], BitCop [https://bitcop.ru/], WorkTime Monitor [https://www.worktime.com/] и Yaware [https://yaware.com/], делят активность на продуктивную, непродуктивную, нейтральную и формируют отчёты, в которых работодатель сможет увидеть, на что тратили время его подчиненные.1.

Плюс подобных систем в их простоте и малом объёме данных для хранения и передачи. Поскольку конфиденциальная информация не передается, то руководителю можно не бояться за её сохранность. Однако нельзя не отметить целый набор минусов. Во-первых, подобного рода программы бесполезны для службы безопасности и IT, поскольку такие системы не могут дать ответ, что именно делал человек в той или иной

программе или на сайте. Во-вторых, эти программы очень просто обмануть, симулируя активность.

Главное отличие данных систем от предлагаемой реализации заключается в том, что они сфокусированы на мониторинге активности сотрудников с целью повышения эффективности их рабочей производительности и оперируют множеством разнородных данных, для обработки которых используются отдельные компоненты и решения. Они не проводят анализа для того, чтобы выявить нестандартное поведение. Большинство таких систем лишь ведут учёт деятельности сотрудников и предоставляют отчёты.

Разработанная система нацелена в первую очередь на обнаружение внутренних нарушителей. Реализующее её программное обеспечение интегрируется в систему контроля доступа, выступая в качестве отдельного её компонента, который снабжает аналитиков информацией о перемещениях сотрудников по зданию организации и их совместных встречах.

1.2 Выводы

Литература показывает немалое количество подходов к анализу поведения сотрудников. Важно, что большинство из них не используют логи СКУД для выявления аномального поведения, а лишь для контроля посещаемости и подсчёта проведённого на рабочем месте времени. Так же многие программные продукты предоставляют визуализацию данных и используют интерактивные модели [24][25][26][30], включающие в себя как пространственные, так и временные атрибуты перемещений.

ГЛАВА 2. ПРОЕКТ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССА ВЫЯВЛЕНИЯ АНОМАЛИЙ В ПОВЕДЕНИИ СОТРУДНИКОВ ОРГАНИЗАЦИИ НА ОСНОВЕ ДАННЫХ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

2.1 Цели и задачи проекта

Основными целями анализа активности сотрудников являются повышение рабочей производительности и контроль соблюдения мер и политик безопасности, установленных на предприятии, а также обнаружение внутренних нарушителей.

Цель исследовательской работы – реализовать методики анализа взаимодействия сотрудников предприятия.

Для выполнения поставленной цели необходимо решить ряд задач:

1. Проанализировать существующие методики выявления аномалий в поведении сотрудников.
2. Определить методы автоматического анализа данных с учетом специфики предметной области.
3. Разработать систему выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа.
4. Описать результаты, полученные в ходе исследования на реальных данных, и определить направления дальнейших исследований.

При последовательном выполнении данных этапов, у аналитика формируется общее понимание существующих проблем связанных с построением шаблонов перемещений сотрудников и выявлением в них аномалий. При этом предполагается, что поставленные задачи соответствуют основным этапам анализа взаимодействия сотрудников предприятия по данным журналов СКУД [1].

2.2 Ключевые элементы предложенной методики поиска аномалий

Ключевыми элементами методики являются журналы СКУД, предприятие и сотрудники. Каждому сотруднику, например, выдаётся магнитный ключ в виде пластиковой карты (идентификатор доступа) с микрочипом и магнитным механизмом для открытия электронного замка. На каждого сотрудника предприятия приходится одна карта, по уникальным признакам которой можно идентифицировать сотрудника. Все данные о сотрудниках и выданных им картах заносится в базу данных СКУД.

Идентификаторы доступа бывают двух типов [6]:

Постоянные – выдаются, обычно, сотрудникам предприятия после согласования правил пользования и подписания соответствующих бумаг.

Временные – выдаются гостям предприятия. Гости могут быть заранее приглашены предприятием либо их учёт ведётся по документам удостоверяющим личность.

На большинстве предприятий вход так же может осуществляться и без наличия карты, однако, в данной работе это не рассматривается.

Обычно сотрудник предприятия или его гость обязан:

- предъявлять карту по требованию сотрудника КПП;
- проходить через КПП только по своей личной карте;
- бережно относиться к оборудованию СКУД и личной карте.

Анализируемое поведение сотрудников включает в себя в основном анализ журнала СКУД (логов). Логи представляют собой данные вида: «Временная метка», «Идентификатор Сотрудника», «Идентификатор зоны доступа» и «Идентификатор этажа». Каждая запись заносится в журнал после того, как человек прикладывает, например, магнитный ключ, что бы зайти в определённую зону.

Для простоты анализа считается, что встреча между двумя сотрудниками состоялась, когда оба находились в зоне доступа в одно время (погрешность ± минута). Разрабатываемая система нацелена на анализ поведения каждого сотрудника, поэтому удобнее и нагляднее рассматривать встречи от лица каждого сотрудника. Другими словами, встреча трёх сотрудников рассматривается как шесть отдельных встреч со всеми сотрудниками (по две в отношении каждого).

Аномальным считается поведение, в котором частота встреч с отдельными сотрудниками или их продолжительность отличается от среднего статистического за весь рассматриваемый период.

2.3 Описание реализуемых процессов

Так как система не имеет разграничения прав пользователей, то основным и единственным актёром является обычный пользователь.

Актёр	Краткое описание
Пользователь системы	Обычный пользователь системы может совершать все действия

Контекстная диаграмма «Как есть» представлена на рисунке 5.

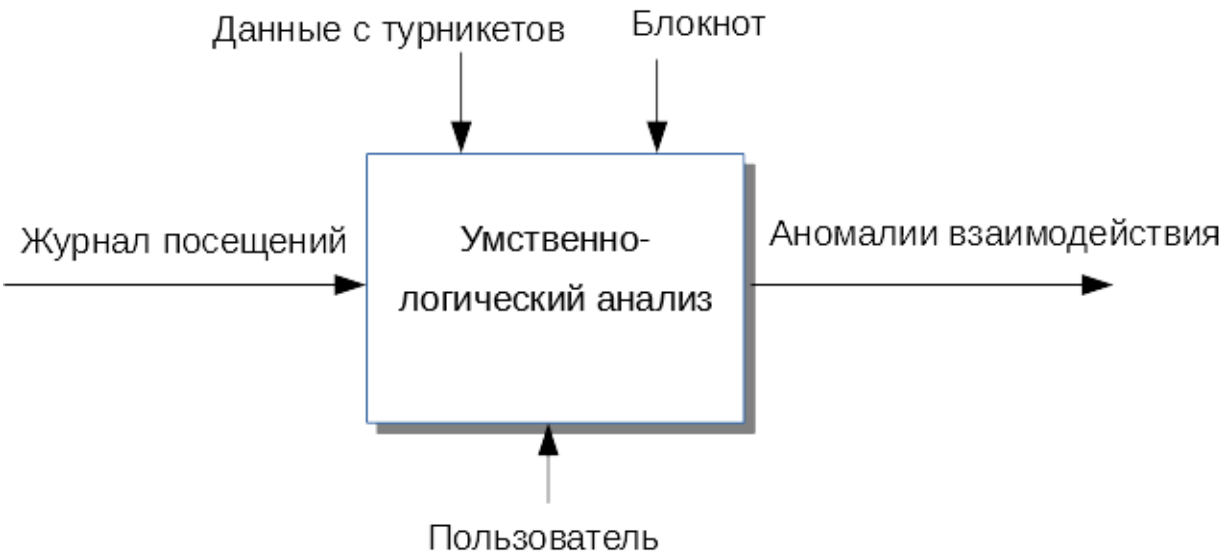

Рисунок 5 - Контекстная диаграмма «Как есть»

Пользователь (сотрудник безопасности на предприятии) читает журнал посещений предприятия. Информация в журнал поступает от контроллеров доступа, расположенных на входах в зоны доступа. Далее он проводит мысленные операции и анализирует данные. В итоге, находит аномалии в поведении сотрудников.

2.4 Построение и обоснование модели разрабатываемой системы

На рисунках ниже представлена модель разрабатываемой системы «Как должно быть» в нотации IDEF0. Контекстная диаграмма «Как должно быть» представлена на рисунке 6.

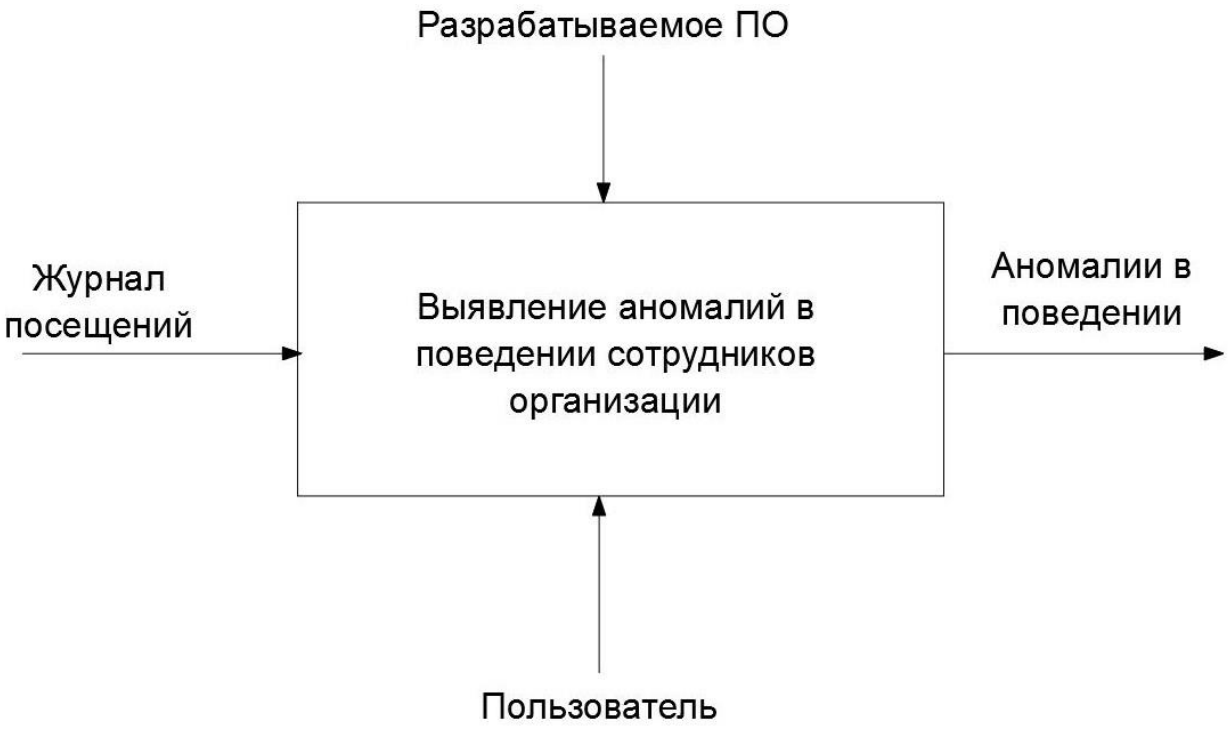

Рисунок 6 - Контекстная диаграмма «Как должно быть»

2.5 Описание предлагаемого подхода

При автоматизации процесса выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа пользователь должен загрузить логи СКУД в разрабатываемое ПО. Пользователь имеет возможность выделить желаемый временной период. В итоге, ПО создаёт файл со всеми обнаруженными аномалиями на данном временном отрезке.

Основная сложность разработки ПО заключается в написании парсера – инструмента для работы с журналами СКУД. Среднее количество записей для одного человека за один день составляет ~ 500 строк. Учитывая, что на

среднем предприятии могут работать до 100 человек, получаем файл, содержащий около 50 000 строк в день, что составит 4 500 000 строк за три месяца. Ясно, что требуется вычислительная мощность для обработки таких файлов и дальнейшего их анализа.

Пусть $E = \{e_i\}_{i=1}^{n}$ - множество сотрудников, где e_i – сотрудник, n – количество сотрудников предприятия. $Z = \{z_j\}_{j=1}^{m}$ – множество контролируемых зон, где z_j – контролируемая зона, m – количество зон на предприятии (включая этажи). $T = \{t_k : t_i < t_j; i < j\}_{k=1}^{p}$ – множество упорядоченных временных меток.

Тогда, сами логи могут быть представлены следующим образом $LOGS = \{(e_i, z_j, t_k)\}, i = 1 \div n, j = 1 \div m, k = 1 \div p.$

Встречу между двумя сотрудниками можно представить следующим образом $Meet(e_i, e_j) = \{z_k, t, t_{duration}\}$, где z_k - контролируемая зона, где состоялась встреча, t - временная метка, обозначающая начало встречи, $t_{duration}$ – длительность встречи. Таблица GraphByDate базы данных заполняется именно такими записями.

Исходя из всех ограничений на специфику работы с большими данными, был разработан следующий алгоритм:

1. На первом этапе работы ПО пользователь загружает логи и запускает работу парсера.
2. Парсер в свою же очередь запускает обработку логов в фоновом потоке через команду RunWorkerAsync.
3. Фоновый поток в цикле по файлу логов выбирает те записи, даты которых не превышают ограничений, наложенных пользователем.

4. Для каждой выбранной записи создаётся отдельный поток через команду ThreadPool.QueueUserWorkItem. Далее работа программы останавливается до окончания работы всех потоков.
5. Каждый поток [7] повторно проходит по всему файлу логов, чтобы выделить промежутки (интервалы) времени, в которых сотрудник находился в определённом помещении. Все интервалы записываются в таблицу Intervals локальной базы данных.
6. На втором этапе работы ПО запускается SQL файл для работы с таблицей GraphByDate локальной базы данных. Следуя SQL инструкциям система в цикле проходит таблицу Intervals и для каждой строки (так же в цикле выбираются записи которые произошли во временной промежуток текущего сотрудника) мы заполняем таблицу GraphByDate, указывая встречи с каждым другим сотрудником.
7. На третьем этапе работы ПО запускается SQL файл для работы с таблицей AnomaliesTEMP локальной базы данных [8]. Следуя SQL инструкциям система в цикле проходит таблицу GraphByDate и для каждой строки находит среднее значение числа встреч и времени встречи. Сравнивания найденные значения с текущими делается вывод об «аномальности» встречи. Каждая аномалия записывается в таблицу AnomaliesTEMP.
8. На последнем этапе работы пользователь может сохранить все полученные данные в виде txt файла (сохранение файлов происходит в многопоточном режиме).

2.6 Блок-схема

Далее этот алгоритм описан в виде Блок-Схемы. Некоторые алгоритмы и части кода, которые не имеют функционального смысла, а были написаны для дизайна, пояснений, удобства или из-за конкретных ограничений языка C# или среды разработки Visual Studio, не представлены на данной схеме.

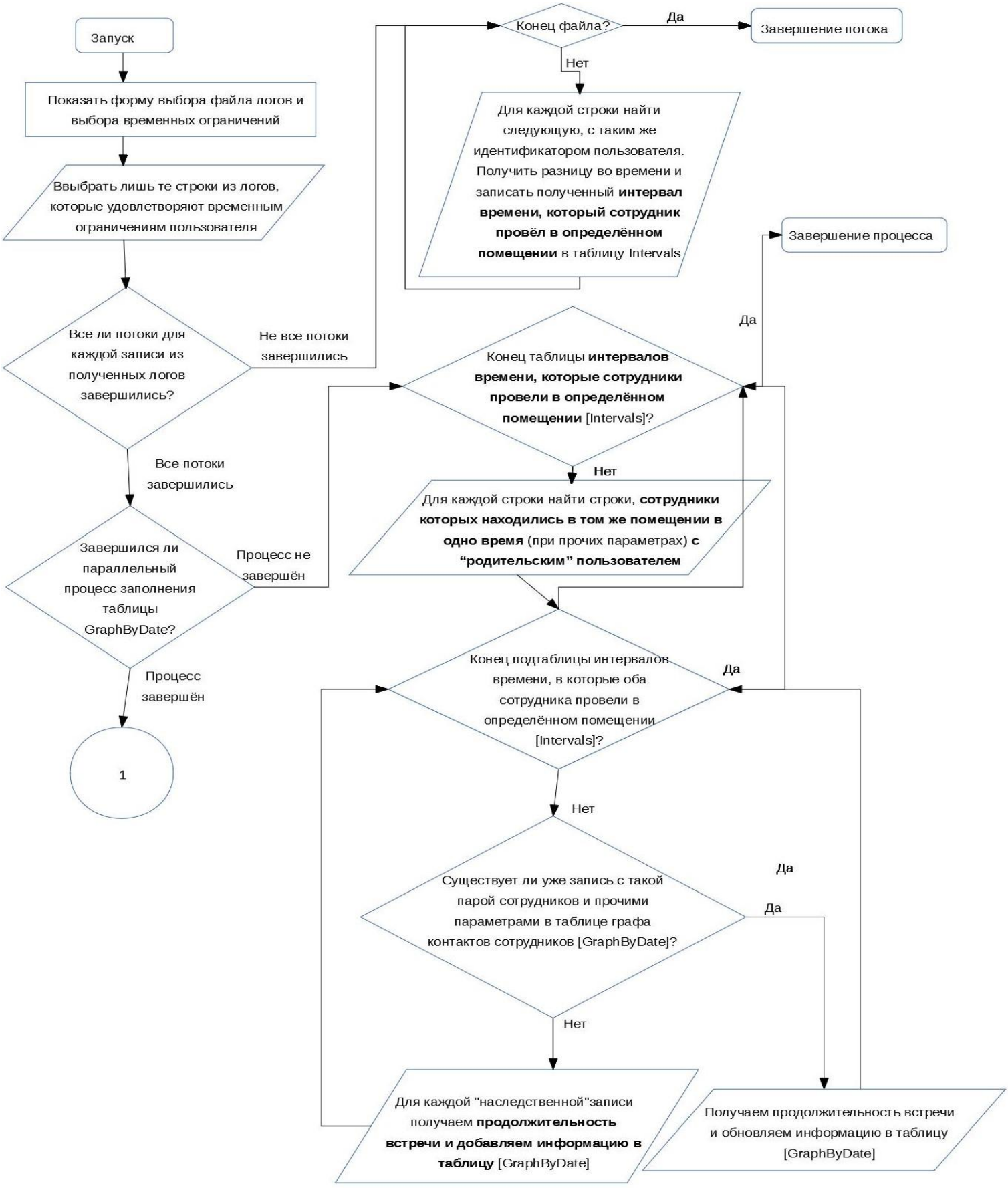

Рисунок 7 - Блок-схема. Часть 1

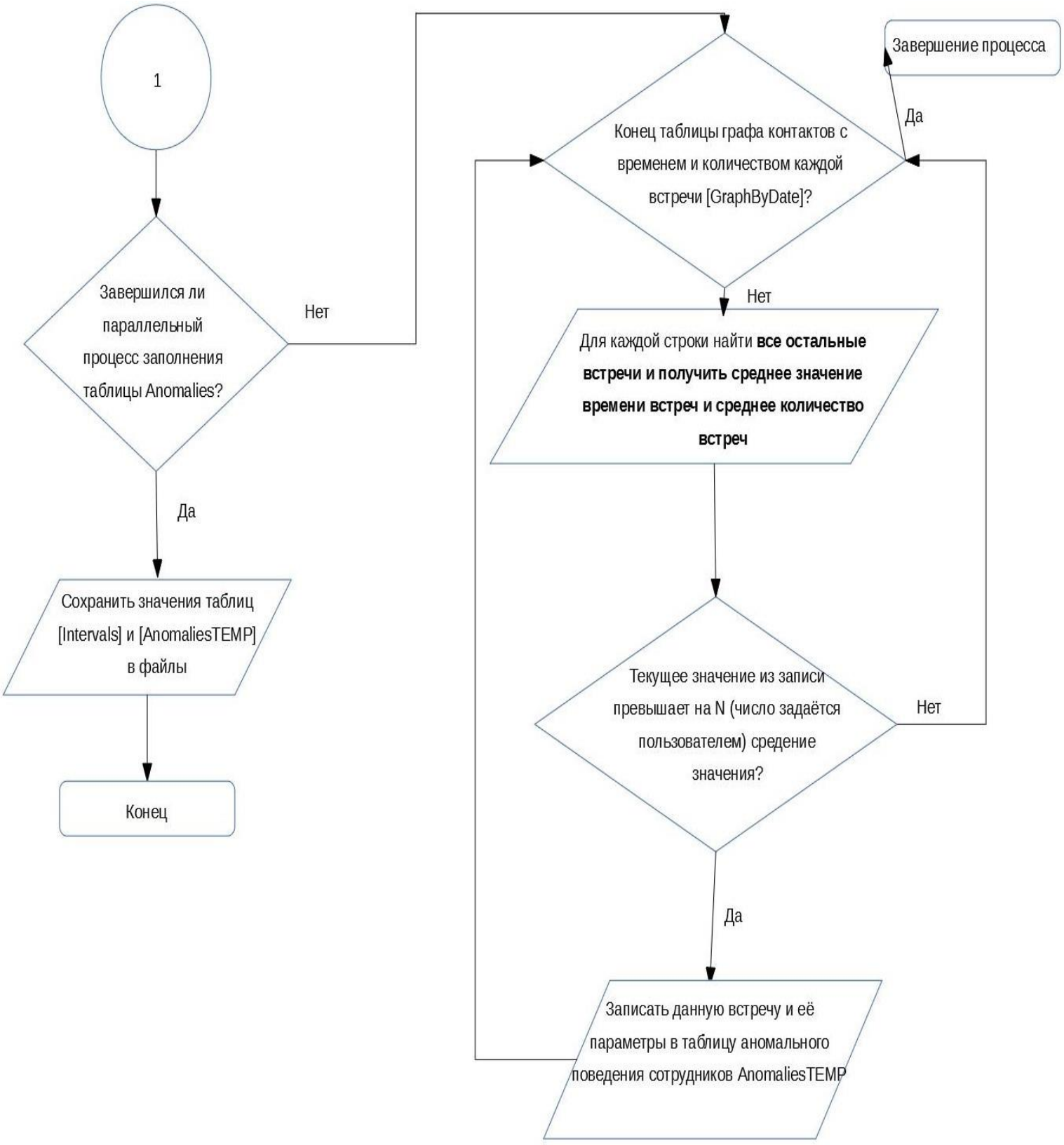

Рисунок 8 - Блок-схема. Часть 2

ГЛАВА 3. РАЗРАБОТКА СИСТЕМЫ ВЫЯВЛЕНИЯ АНОМАЛИЙ В ПОВЕДЕНИИ СОТРУДНИКОВ ОРГАНИЗАЦИИ НА ОСНОВЕ ДАННЫХ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

3.1 Спецификация и обоснование нефункциональных требований

3.1.1 Удобство использования

Понятность интерфейса: интерфейс системы должен быть спроектирован так, чтобы пользователь мог понимать назначение каждого элемента управления [1].

Охват всех функций интерфейсом: обеспечивать доступ ко всем функциям системы.

Простота интерфейса: исключать излишние действия пользователя при работе с системой.

Отсутствие не функциональных элементов управления: интерфейс не должен содержать лишних элементов, элементов не несущих функциональной нагрузки.

Наличие описания элементов управления: все поля для ввода данных должны быть подписаны.

Информативность сообщений: система должна выводить только информативные сообщения об ошибках.

Для большей понятности интерфейса, элементы управления могут использовать фоновые изображения, если их использование не приведёт к усложнению восприятия и не приведёт к чрезмерному замедлению загрузки страницы.

3.1.2 Доступность

Система должна обеспечивать возможность быть доступной 95% времени. Доступность системы для конечного пользователя определяется

набором используемого аппаратного обеспечения и каналом передачи данных на стороне сервера и клиента.

3.1.3 Наработка на отказ

Система не должна нагружать аппаратное обеспечение без необходимости и минимизировать проведение записи данных на жёсткий диск. Система должна иметь возможность работать в режиме 24 / 7.

3.1.4 Норма дефектов

В работе системы не должны появляться критические ошибки, приводящие к остановке работы системы.

Допускается отсутствие обработки таких ситуаций как:

- Сбой операционной системы сервера;
- Возникновение ошибки платформы, на которой базируется система и используемой базы данных при условии их корректного использования;
- Внезапные сбои аппаратного обеспечения сервера (например, потеря электропитания или механическое повреждение аппаратуры).

3.1.5 Время отклика

Время отклика системы зависит от используемого аппаратного обеспечения пользователя и сервера. Однако система должна обеспечивать оптимальное использование имеющихся ресурсов. Перед выполнением потенциально продолжительных операций, пользователь должен быть уведомлен об этом с помощью появления изображения или анимации загрузки или текстового сообщения.

3.1.6 Масштабируемость

Система должна быть спроектирована таким образом, чтобы добавление новых модулей редактирования изображений выполнялось

быстро и могло производиться человеком, не имеющим представления о принципе работы остальной части системы. Кроме того, должен быть обеспечен наименее возможный уровень неявных зависимостей и излишних связей между её компонентами для их облегченного сопровождения, изменения и добавления новых.

3.1.7 Требования к информационному обеспечению

- Сообщения и элементы управления содержат текст на английском языке.
- Комментарии в коде могут быть написаны на русском и английском языке.
- Названия модулей, переменных и функций только на английском языке.

3.1.8 Требования к программному обеспечению

- Операционная система: Microsoft Windows 7 и выше (32/64 бита);
- Процессор Intel Atom 1.6 ГГц и выше;
- Видеокарта Intel GMA950 с видеопамятью объемом не менее 64 МБ (или совместимый аналог);
- Минимальное разрешение экрана 1024×600;
- Microsoft .Net Framework 4 или выше.

3.2 Календарно-ресурсное планирование проекта, анализ бюджетных ограничений и рисков

3.2.1 Описание выбранной методологии

Rational unified process — методология разработки программного обеспечения, созданная компанией Rational Software [1][17].

В основе методологии лежат 6 основных принципов:

1. Компонентная архитектура, реализуемая и тестируемая на ранних стадиях проекта;
2. Работа над проектом в сплочённой команде, ключевая роль в которой принадлежит архитекторам;
3. Ранняя идентификация и непрерывное устранение возможных рисков;
4. Концентрация на выполнении требований заказчиков к исполняемой программе;
5. Ожидание изменений в требованиях, проектных решениях и реализации в процессе разработки;
6. Постоянное обеспечение качества на всех этапах разработки проекта.

Использование методологии RUP направлено на итеративную модель разработки. Особенность методологии состоит в том, что степень формализации может меняться в зависимости от потребностей проекта. Можно по окончании каждого этапа и каждой итерации создавать все требуемые документы и достигнуть максимального уровня формализации, а можно создавать только необходимые для работы документы, вплоть до полного их отсутствия. За счет такого подхода к формализации процессов методология является достаточно гибкой и широко популярной. Данная методология применима как в небольших и быстрых проектах, где за счет

отсутствия формализации требуется сократить время выполнения проекта и расходы, так и в больших и сложных проектах, где требуется высокий уровень формализма, например, с целью дальнейшей сертификации продукта. Это преимущество дает возможность использовать одну и ту же команду разработчиков для реализации различных по объему и требованиям. Графически методология изображена на рисунке 9.

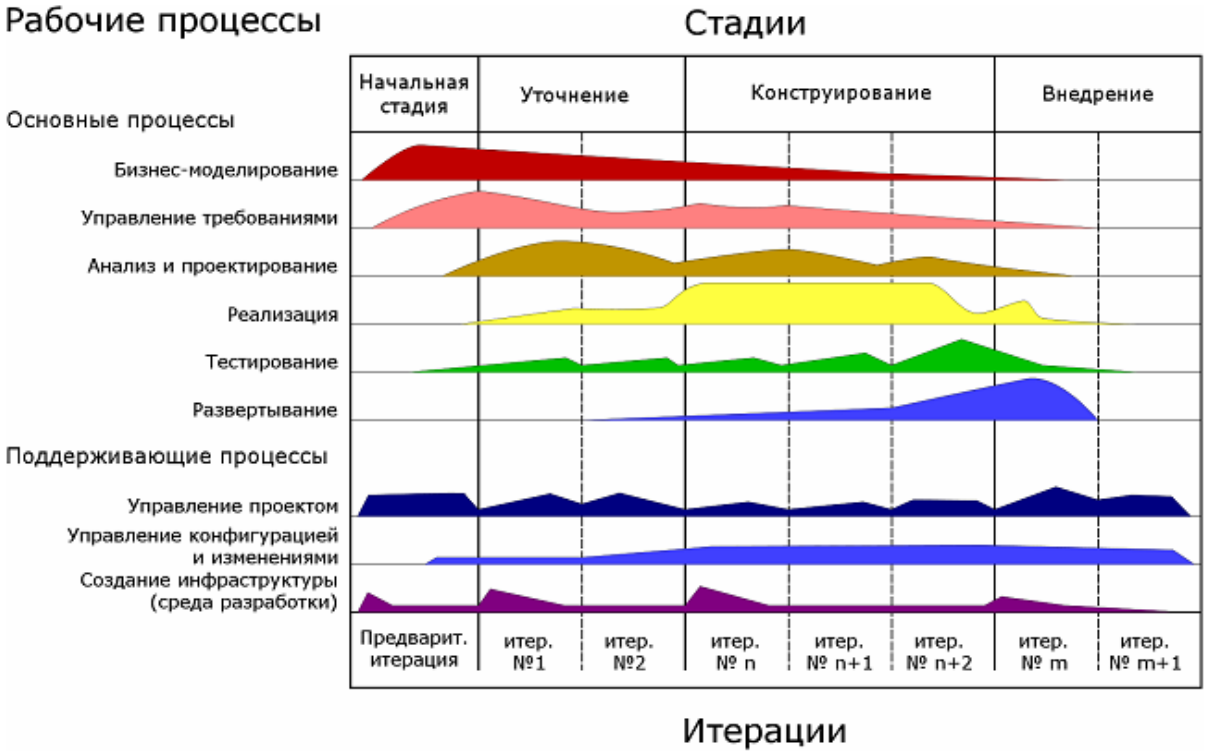

Рисунок 9 - RUP

На начальной фазе будут сформированы следующие документы: видение и границы проекта, экономическое обоснование, основные требования, ограничения и ключевая функциональность продукта, версия модели прецедентов, риски.

На фазе проектирования будет производиться анализ и документирование требований, обновляться экономическое обоснование проекта и риски проекта, создаваться и тестироваться архитектура проекта.

На фазе построения будут производиться основные работы по кодированию системы.

Параллельно с моделированием будет начат процесс реализации для модулей системы, к которым уже есть требования. После окончания каждой итерации будет производиться документирование разработанных модулей. При изменении требований или добавления новых требований будут изменяться все документы, в которых они описаны.

3.2.2 Анализ рисков

При разработке модуля возникнет сложность в связи с возможностью проблем со здоровьем у разработчика.

Если данная разработка не будет выполнена, то это повлечет недостижимость поставленных бизнес-целей. При разработке возможны проблемы, связанные со сложностью реализации (связанной со специфической предметной областью), недостаток навыков разработки, что влечет за собой увеличение времени разработки. Риски представлены в таблице 1.

Таблица 1. Риски

Наименование риска	**Влияние риска, %**	**Вероятность риска, %**	**Техника управления риском**	**Приоритет**	**Временные потери (в днях)**
Неверно выбранные технологии	60	20	Продуманный выбор технологий. Анализ проблем, связанных с их использованием.	2	3-7
Ошибки в распределении времени на задачи	40	70	Тщательное планирование временных сроков.	2	5
Незнание технологий	30	40	Изучение необходимых технологий заранее.	3	2
Ошибки при проектировании	90	20	Детализированный анализ предметной области, формулирование четких требований к системе	1	20-25

3.2.3 Календарный план проекта

Для разработки в рамках первой итерации были выбраны следующие варианты использования: загрузка файлов, сохранение файлов, вставка файлов. План выполнения работ первой итерации представлен в таблице 2.

Таблица 2. План выполнения работ

Дни	***Работы***
1-3	Главная форма приложения, подключение библиотек для работы с CSV файлами.
3-10	Создание БД. Заполнение таблицы интервалами посещений сотрудников.
10-12	Распараллеливание процессов чтения с файла и записи в БД

Примечание: Каждый этап работы включает в себя тестирование работоспособности.

Для разработки в рамках второй итерации были выбраны следующие варианты использования: выбор файла в системе, редактирование файла, сохранение изменённого файла. План выполнения работ второй итерации представлен в таблице 3.

Таблица 3. План выполнения работ

Дни	***Работы***
1-4	Сохранение векторов встреч в отдельные файлы для каждого сотрудника
4-11	Рефакторинг кода. Заполнение таблицы аномалий, выявленных в файле CSV.
11-15	Исправления в дизайне главной формы приложения. Настройка обработки различных ошибок (отсутствие файла, неверный формат данных и прочее).

Примечание: Каждый этап работы включает в себя тестирование работоспособности.

3.3 Функциональная структура

Диаграмма вариантов использования

На рисунке 10 представлена диаграмма вариантов использования [20].

1. Пользователь загружает логи в систему.
    a. Есть возможность детально настроить временной период, за который он желает найти аномалии.
2. После настроек, необходимо запустить основной алгоритм и ПО сформирует таблицу аномалий, которую можно будет сохранить в формате txt. Так же можно сохранить и векторы встреч.

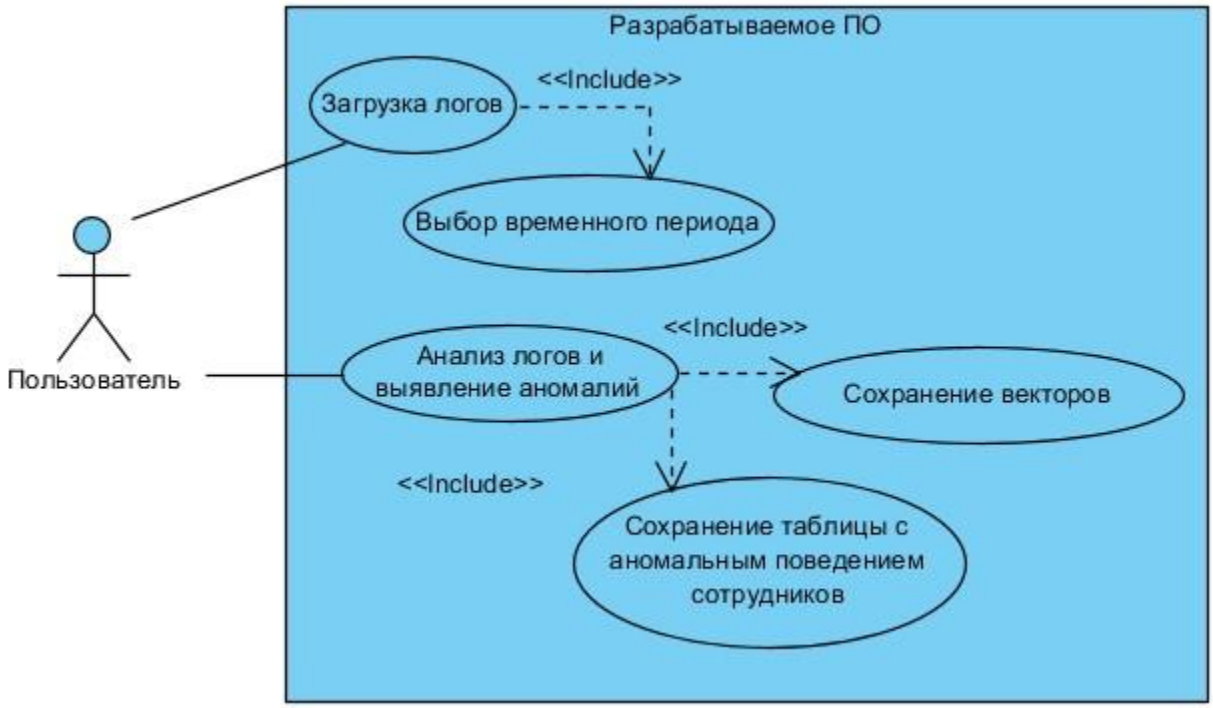

Рисунок 10 - Диаграмма вариантов использования

Реестр вариантов использования находится в приложении Б.

3.4 Информационное обеспечение

Диаграмма классов

Диаграмма классов является статической структурной диаграммой, описывающей структуру системы, демонстрирует классы системы, их атрибуты, методы и зависимости между классами.

- Класс FormCoreShare содержит поля для обмена информацией между потоками;
- Класс Zone содержит данные о зоне доступа;
- Класс Department содержит данные о должности сотрудника;
- Класс User содержит идентификационные данные о сотруднике;
- Класс Floor содержит данные об этаже здания;
- Класс Office содержит данные об отдельных кабинетах в зоне доступа.

Диаграмма классов для проектируемой системы в нотации UML представлена на рисунке 11.

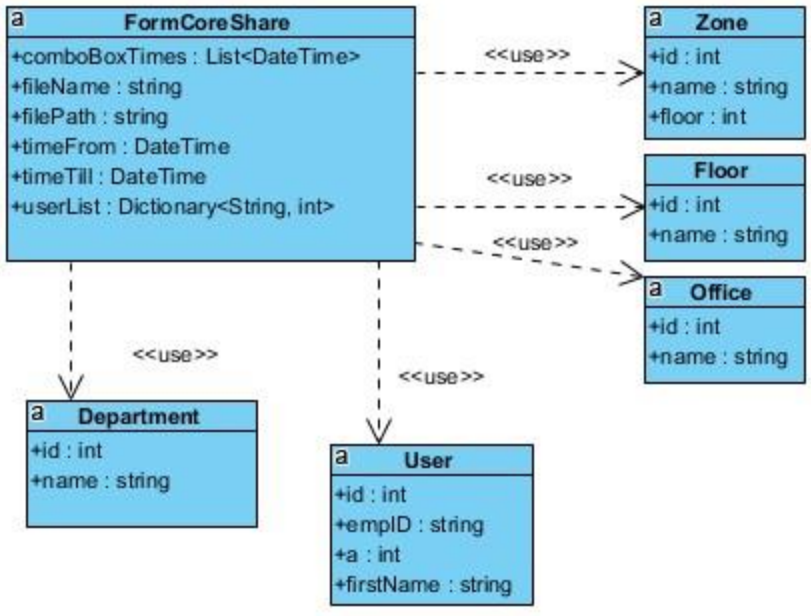

Рисунок 11 - Диаграмма классов

3.5 Программное обеспечение

Диаграмма компонентов

На рисунке 12 представлена диаграмма компонентов разрабатываемой системы. На ней отображены все файлы, используемые при разработке системы:

- PACS Analyzer.exe – Главный исполняемый файл;
- DatabaseMain.mdf – Файл базы данных, который хранит все таблицы проекта;
- Example.csv – Пример лог файла (содержит записи о нескольких сотрудниках);
- Anomalies.sql – Набор SQL команд для поиска аномалий в таблице [GraphByDate];
- FileHelpers.dll – Сторонняя библиотека для работы с CSV файлами;
- GraphByDateFillIn.sql – Набор SQL команд для заполнения таблицы [GraphByDate].

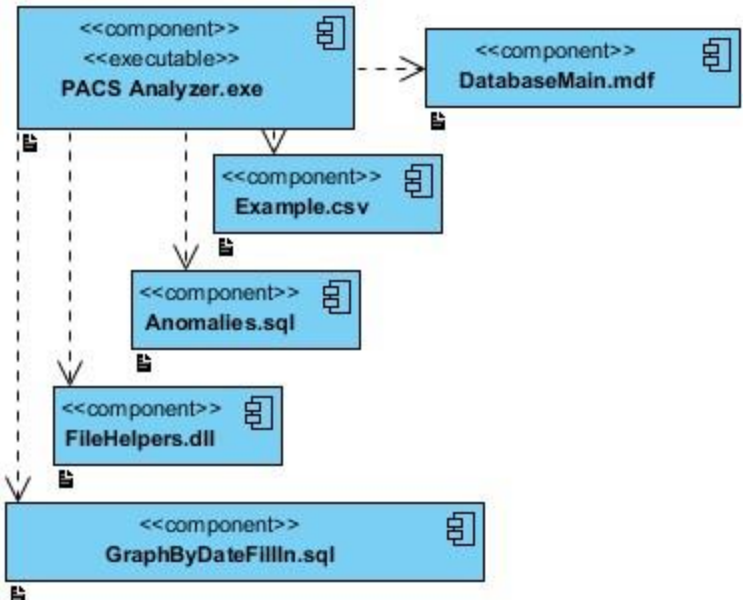

Рисунок 12 - Диаграмма компонентов

Диаграмма последовательностей

Диаграмма последовательностей используется для моделирования взаимодействия объектов во времени [21]. На ней изображаются те объекты, которые непосредственно участвуют во взаимодействии и не показываются статические ассоциации с другими объектами. Взаимодействия объектов можно рассматривать во времени в двух измерениях: слева направо в виде вертикальных линий, каждая из которых изображает линию жизни отдельного объекта, участвующего во взаимодействии, и вертикальная временная ось, направленная сверху вниз. Диаграмма представлена на рисунке 13.

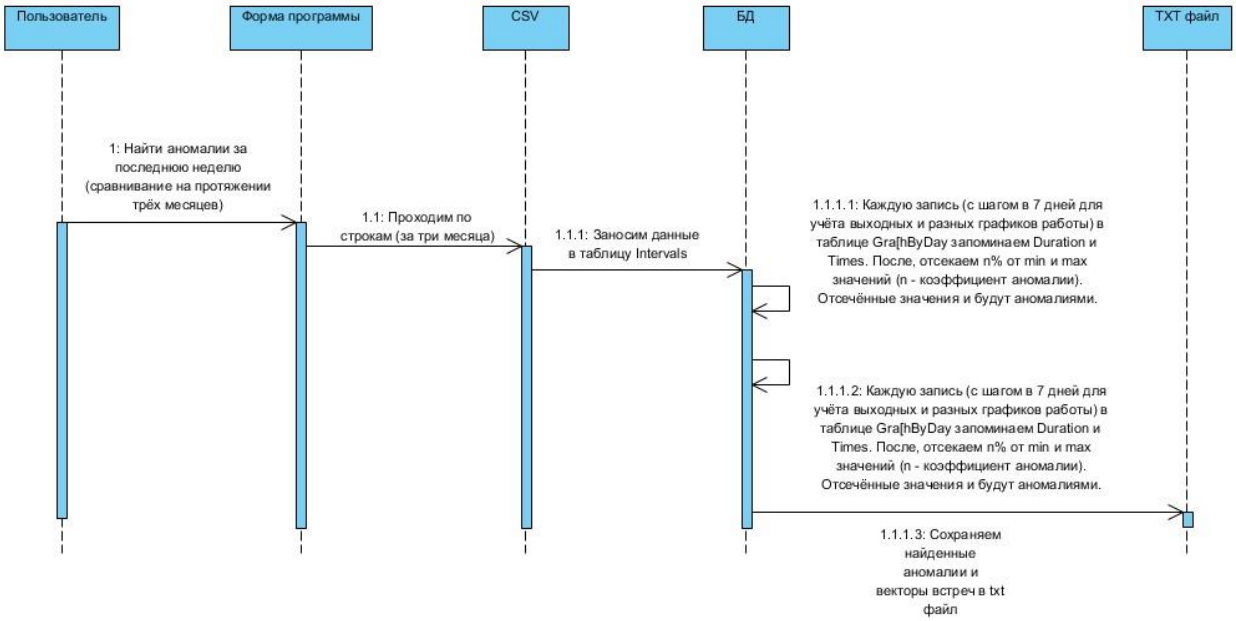

Рисунок 13 - Диаграмма последовательности

3.6 Обеспечение информационной безопасности

Любой пользователь может работать с системой без идентификации.

3.7 Технологическое обеспечение

Разработанная программа должна работать на операционной системе Windows. Основным языком для написания программ для данной системы является C# (по количеству строк кода на крупнейшем веб-сервисе для хостинга IT-проектов и их совместной разработки – GitHub [9][10]). При разработке применялись следующие технологии:

- Visual Studio Community 2017 [11] – Интегрированная среда разработки программного обеспечения. Данное приложение было выбрано, так как оно является официальным продуктом для разработки под Windows, создана, поддерживается и рекомендуется компанией Microsoft;
- FileHelpers 3.2 – библиотека функций для работы с CSV файлами.

Для выполнения сложных запросов к базе данных использованы курсоры SQL, для обеспечения быстродействия использовались несколько потоков вычислений.

Интерфейс (главное окно) программы на английском языке.

3.8 Контрольный пример

1. Необходимо запустить файл PACS Analyzer.exe из папки проекта.
2. Появится главная форма программы (пример представлен на рисунке 14).

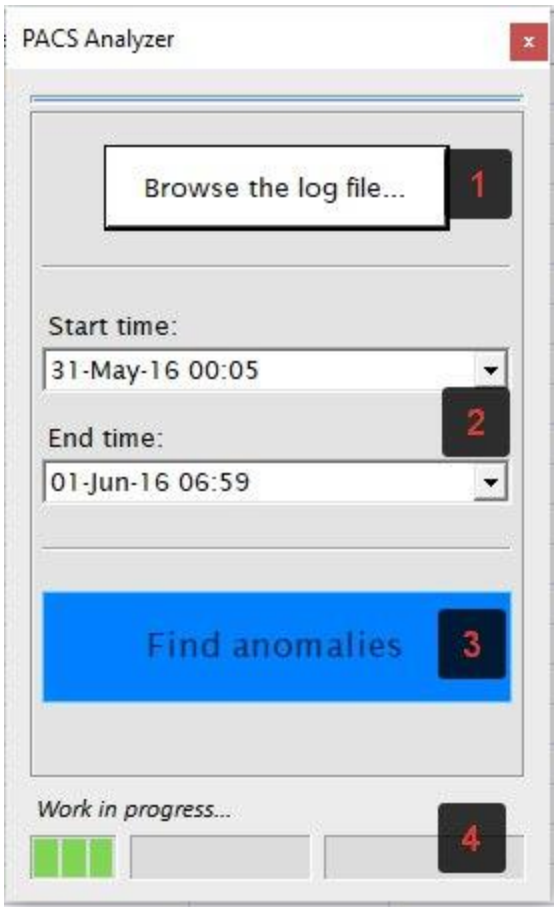

Рисунок 14 - Форма входа на сайт

3. Для загрузки логов СКУД в систему необходимо нажать на кнопку «Browse the log file...».
4. Следует выбрать файл на компьютере и нажать кнопку «Выбрать» в диалоговом окне операционной системы.
5. Для выбора временного промежутка необходимо изменить значения двух выпадающих списков: «Start time» и «End time» соответственно.
6. Следует нажать кнопку «Find anomalies» для запуска процесса поиска аномалий.
7. После успешного поиска аномалий они будут занесены в таблицу базы данных.

a. Чтобы сохранить значения векторов встреч следует нажать появившуюся кнопку «Save Vectors».
b. Чтобы сохранить таблицу аномального поведения сотрудников следует нажать появившуюся кнопку «Save Anomalies».

3.9 Выходные файлы

После завершения работы программы на компьютере пользователя остаются две папки: «users» и «anomalies». В папке «users» хранятся векторы, описывающие поведение сотрудников с точки зрения встреч с выбранным сотрудником. Файлы «условное_имя_пользователя.txt» содержат следующие записи:

```
date (whole day); user1; user2; average duration (sec); times; floor; zone
31-May-16 12:00:00 AM;earpa;vawelon;5430;16;2;2
31-May-16 12:00:00 AM;earpa;knielson;5418;16;2;2
31-May-16 12:00:00 AM;earpa;ldedos;8700;10;2;2
01-Jun-16 12:00:00 AM;vawelon;earpa;5422;16;2;2
01-Jun-16 12:00:00 AM;earpa;knielson;5388;16;2;2
…
```

Первая строка файла описывает последующие записи. Каждая следующая строка содержит в себе записи о векторах вида: «Временная метка встречи; идентификатор первого сотрудника; идентификатор второго сотрудника; средняя продолжительность встречи в этот день; количество встреч; этаж; помещение.

В папке «anomalies» хранится файл «anomalies.txt», содержащий записи типа:

```
date (whole day); user1; user2; odd duration (sec); average duration (sec); odd times; average times; floor; zone
03-Jun-16 AM;monda;jcastellanos;44952;13512;5;4;1;4
10-Jun-16 AM;jcastellanos;monda;74840;22520;3;3;1;4
31-May-16 AM;jcastellanos;ncalixto;17500;13600;3;2;1;4
01-Jun-16 AM;jcastellanos;ncalixto;17460;13600;3;5;1;4
02-Jun-16 AM;ncalixto;jcastellanos;26280;20400;2;3;1;4
```

…

Первая строка файла описывает последующие записи. Каждому столбцу соответствует своё название, например, «date» показывает, что все символы до первой точки с запятой означают дату аномалии и так далее. Каждая следующая строка содержит в себе записи об аномалиях, найденных в поведении сотрудников, представлена пара сотрудников, которые встречались в указанном времени и месте. Ключевые показатели – это аномальное время встречи («`odd duration (sec)`») и аномальное количество встреч («`odd times`»). Эти значения можно сравнивать соответственно со среднем временем встреч («`average duration (sec)`») и среднем числом встреч («`average times`») этих сотрудников. Разработанная система анализирует логи, сравнивает все значения и заносит аномалии в «anomalies.txt».

3.10 Оценка качества результата работы системы

Оценка качества результатов, полученных после работы системы, ограничивается политикой предприятия. Система определяет аномалии статистическим методом. Другими словами: система просматривает журнал посещений СКУД и определяет аномальное поведение лишь на основе количественных данных. Для многих компаний так же важны и качественные данные, такие как должность сотрудника, его ставка, рабочее время и внутренний регламент. Такие ограничения не накладывались на результат работы системы.

Для наглядности тестирования результатов, взяты данные журналов посещения СКУД с 13 мая по 13 июня. Далее были найдены аномалии экспертами (сотрудник безопасности предприятия или человек, знакомый со спецификой нахождения аномалий на основе таких данных).

Описание аномалий по исходным данным (определены человеком):

1. Monda и Ncalixto провели вместе 7 часов 31 мая, когда обычно они находились в одном помещении (1 этаж, кабинет №4) 3.5 часов.
2. Monda и Vawelon провели вместе 14 часов 3 июня, когда обычно они находились в одном помещении (1 этаж, кабинет №4) 4 часа.
3. Slea и Ncalixto провели вместе 21 час 3 июня, когда обычно они находились в одном помещении (1 этаж, кабинет №4) 4 часа.

Аномалий по исходным данным (определены разработанной системой):

```
1.31-May-16;ncalixto;monda;25800;12540;2;3;1;4
2.03-Jun-16;vawelon;monda;51660;14835;4;4;1;4
3.03-Jun-16;slea;ncalixto;75180;15100;3;3;1;4
4.03-Jun-16;monda;acalzas;111750;14220;2;1;1;1
5.10-Jun-16;jsanjorge;sparrino;7400;20120;3;3;1;4
```

Как видно, все тестовые аномалии были найдены системой, однако присутствуют ещё две записи. Четвёртая строка показывает, что Mmonda и Acalzas провели вместе 31 час. Такие данные не могут считаться аномальными, так как это следствие того, что система считает разницу между двумя идентификациями сотрудника. Скорее всего, в этом случае Monda просто покинул рабочее место и зашёл на территорию лишь через 31 час. Пятая строка показывает слишком малое время встречи, 2 часа. Как пример, можно сказать, что согласно внутренней политике компании, такие встречи являются нормой и не подлежат к рассмотрению.

Таким образом, с помощью разработанной системы реально и легко находить аномалии в поведении сотрудников, однако с выходными данными необходимо ещё работать сотрудникам безопасности.

3.11 Направления дальнейших исследований

В данной работе были описаны методики анализа, позволяющие выявить аномалий в поведении сотрудников организации на основе данных системы контроля доступа, и была разработана соответствующая программа.

Одно из основных направлений будущей работы будут посвящено улучшению формального описания взаимоотношений между сотрудниками и уточнению зависимостей между ними. Особое внимание планируется уделить интеграции ролей сотрудников (должность), рабочее время и внутренний регламент.

Так же важнейшим шагом будет разработка автоматизированной системы для визуализации таблиц базы данных (Intervals, GraphByDate и AnomaliesTEMP). Другое направление будущих работ затрагивает анализ данных, полученных из различных источников. Журналы операционной системы, например, события входа-выхода и события клавиатуры являются

доказательствами того, что сотрудник находится на рабочем месте. Корреляция этих данных требует разработки новых методов визуального анализа с учетом особенностей исходных данных.

ГЛАВА 4. СОСТАВЛЕНИЕ БИЗНЕС-ПЛАНА ПО КОММЕРЦИАЛИЗАЦИИ РЕЗУЛЬТАТОВ НИР МАГИСТРА

В выпускной квалификационной работе рассматривается задача по разработке системы выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа..

Решение поставленной задачи невозможно без оценки технико-экономической эффективности разрабатываемого проекта.

Чтобы рассчитать затраты на выполнение выпускной квалификационной работы необходимо:

1. Составить детализированный план-график выполнения работ, позволяющий определить совокупную трудоемкость написания программы;
2. Оценить величину заработной платы и социальных отчислений участников исследования (технико-экономическое обоснование предполагает осуществление оплаты труда);
3. Оценить затраты, связанные с содержанием и эксплуатацией (возможно, приобретением) оборудования используемого при написании программы;
4. Определить величину амортизационных отчислений используемых основных средств;
5. Оценить накладные расходы;
6. Рассчитать совокупную величину затрат, связанных с написанием программы.

4.1 Расчет длительностей этапов разработки

Для расчета затрат на этапе проектирования необходимо определить продолжительность каждой работы. Продолжительность работ определяется

либо по нормативам, либо по факту, либо расчетным путем с помощью экспертных оценок по формуле:

$$t_{oj} = \frac{3t_{min}+2t_{max}}{5} \quad (1)$$

Где t_{oj} - ожидаемая длительность j-й работы; t_{min} и t_{max} – меньшая и большая по мнению эксперта длительность работы.

Месячная заработная плата студента составляет 15000 (пятнадцать тысяч) рублей. Месячная заработная плата руководителя – 35000 (тридцать пять тысяч) рублей. Если в месяце 21 рабочий день, то ставка студента в день составляет 714,29 рублей, а ставка руководителя в день составляет 1666,67 рублей.

Таблица 4– Длительность этапа разработки

№	Наименование этапа	Исполнитель	Трудоёмкость, дн.	Ставка руб/дн.
1	Разработка ТЗ	Руководитель	5	1666,67
		Студент	5	714,29
2	Изучение справочной литературы	Руководитель	10	1666,67
		Студент	25	714,29
3	Разработка архитектуры	Руководитель	5	1666,67
		Студент	5	714,29
4	Разработка приложения	Руководитель	10	1666,67
		Студент	25	714,29
5	Отладка и тестирование приложения	Руководитель	3	1666,67
		Студент	8	714,29
6	Оформление	Руководитель	2	1666,67

	пояснительной записки	Студент	7	714,29
	Итого	**Руководитель**	**35**	**1666,67**
		Студент	**75**	**714,29**

На основе данных о трудоемкости выполняемых работ и ставки (за день или час) соответствующих исполнителей необходимо определить расходы на заработную плату исполнителей и отчислений на страховые взносы на обязательное социальное, пенсионное и медицинское страхование.

4.2 Расходы на заработную плату

Расходы на основную заработную плату определяются по формуле:

$$З_{осн.\ з/п} = \sum T_i * C_i,$$

где $З_{осн.\ з/п}$ - расходы на основную заработную плату исполнителей (руб.); *Ti* - время, затраченное i-м исполнителем на проведение исследования (дни или часы); *Ci* - ставка i-го исполнителя (руб./день или руб./час).

$З_{осн.\ з/п\ ст.} = 75 * 714,29 = 53571,75$ (руб.)

$З_{осн.\ з/п\ рук.} = 35 * 1666,67 = 58333,45$ (руб.)

Расходы на дополнительную заработную плату исполнителей определяются по формуле:

$$З_{доп.з/пл} = З_{осн.з/пл} * \frac{Ндоп}{100\%},$$

где $З_{доп.з/пл}$ – расходы на дополнительную заработную плату исполнителей в рублях; $З_{осн.з/пл}$ – расходы на основную заработную плату исполнителей в рублях; $H_{доп}$ – норматив дополнительной заработной платы в процентах. При выполнении расчетов в ВКР норматив дополнительной заработной платы принимаем равным 14%.

$З_{доп.з/пл} = (53571,75 + 58333,45) * 0,14 = 15666,73$ (руб.)

Отчисления на страховые взносы на обязательное социальное, пенсионное и медицинское страхование с основной и дополнительной заработной платы исполнителей определяются по формуле:

$$З_{соц} = (З_{осн.з/пл} + З_{доп.з/пл})*Н_{соц}/100,$$

где $З_{соц}$ - отчисления на социальные нужды с заработной платы (руб.);
$З_{осн.\ з/п}$ - расходы на основную заработную плату исполнителей (руб.);
$З_{доп.\ з/п}$ - расходы на дополнительную заработную плату исполнителей (руб.);
$Н_{соц}$ - норматив отчислений на страховые взносы на обязательное социальное, пенсионное и медицинское страхование (%). Ставка отчислений на страховые взносы на обязательное социальное, пенсионное и медицинское страхование $Н_{соц}$ составляет 30%.

Зсоц = ((53571,75 + 58333,45) + 15666,73) * 0,3 = 38271,58 (руб.)

4.3 Расчёт материальных затрат

Так как выполнение данной выпускной квалификационной работы не предполагает изготовления стендов, приборов или опытных образцов, то затраты на сырье и услуги сторонних организаций сводятся к нулю. Несмотря на это, необходимо учесть затраты на офисные материалы и комплектующие. Затраты на покупные комплектующие изделия рассчитываются по формуле:

$$З_{п} = \sum_{i=1}^{n} Ni Цi\left(1 + \frac{Нт.з.}{100\%}\right), \quad (5)$$

Где $З_{п}$ - затраты на покупные комплектующие изделия в рублях; N_i – количество i-тых комплектующих изделий входящих в единицу продукции; $Ц_i$ – цена приобретения единицы i-го комплектующего; $Н_{т.з.}$ – норма транспортно-заготовительных расходов в процентах. При выполнении расчетов в ВКР норму транспортно-заготовительных расходов принимаем

равной 10%. Все комплектующие изделия и материалы можно представить в таблице 5.

Таблица 5 - Расходы на комплектующие и материалы

Наименование	**Количество, шт.**	**Цена за ед., руб.**	**Сумма, руб.**
Картридж для принтера	1	1999	1999
Бумага	1	249	249
Канцтовары	2	49	98
		Итого:	**2346**

Более того необходимо рассчитать затраты на эксплуатацию оборудования. Затраты на содержание и эксплуатацию оборудования определяются из расчета на 1 час работы оборудования с учетом стоимости и производительности оборудования:

$$З_{эо} = \sum_{i=1}^{n} C_i^{мч} t_i^m, \quad (6)$$

Где $З_{эо}$ - затраты на содержание и эксплуатацию оборудования в рублях; $C_i^{мч}$ – расчетная себестоимость одного машино-часа работы оборудования на i-й технологической операции (руб./м-ч); t_i^m – количество машино-часов, затрачиваемых на выполнение i-й технологической операции (м-ч).

Рассчитаем себестоимость одного машинного часа работы за компьютером:

Мощность, потребляемая компьютером, при учете специфики разработки программного обеспечения, составляет 90 Вт/час. Мощность, потребляемая принтером – 12 Вт/час. Общая потребляемая мощность в размере 0.1 кВт/ч складывается из потребляемых мощностей ноутбука и

принтера, что при тарифе 4,32 руб./кВт составляет 0,43 руб./час или 10,32 руб./день (= 0,43 * 24).

Подставим полученные данные в формулу для расчета затрат на эксплуатацию оборудования:

$$З_{эо} = \sum_{i=1}^{m} C_i^{мч} t_i^m = 10{,}32 * 50 = 516{,}00 \text{ (руб.)}, \quad (7)$$

Где $З_{эо}$ – затраты на содержание и эксплуатацию оборудования ; $C_i^{мч}$ – расчетная себестоимость одного машино-часа работы оборудования на i-й технологической операции(руб./м-ч); t_i^m – количество машино-часов, затрачиваемых на выполнение i-й технологической операции(м-ч).

4.4 Расчёт амортизационных отчислений

Если для проведения исследования, разработки устройства, написания программы используются какие-либо основные средства, то необходимо учесть и включить в затраты амортизационные отчисления по этим основным средствам.

Амортизационные отчисления по основному средству i за год определяются как:

$$A_i = Ц_{п.н.i} * \frac{H_{ai}}{100}\ , \quad (8)$$

Где A_i – амортизационные отчисления за год по i-му основному средству в рублях; $Ц_{п.н.i}$ – первоначальная стоимость i-го основного средства в рублях; H_{ai} – годовая норма амортизации i-го основного средства в процентах. Так как приведенная техника по классификации относится к группе средств, чей срок полезного использования составляет до пяти лет, то годовую норму амортизации можно принять:

$$H_{ai} = \frac{100\%}{5} = 20\%$$

Для определения величины амортизационных отчислений по основным средствам, используемым в процессе выполнения ВКР необходимо определить время, в течение которого было используемо это основное средство. Далее, определяем, какую часть от года составляет период, в течение которого студент использовал основное средство. Величина амортизационных отчислений по i-му основному средству, используемому студентом при работе над ВКР, определяется по формуле:

$$A_{iBKP} = A_i * \frac{T_{i\text{ВКР}}}{12}, \quad (9)$$

где – амортизационные отчисления по i-му основному средству, используемому в работе над ВКР в рублях; A_i – амортизационные отчисления за год по i-му основному средству в рублях; $T_{i\text{ВКР}}$ – время, в течение которого использовалось i-ое основное средство в месяцах. Полученные результаты по величинам амортизационных отчислений удобно представить в таблице 6.

Таблица 6 – Амортизационные отчисления

№	Наименование	Цена, руб.	Кол-во, шт.	Годовые отчисления, руб.	Итоговая величина отчислений, руб.
1	Компьютер	45990	2	18396,00	2772,00
2	Принтер	3490	1	698,00	210,36
3	Планшет	12990	1	2598,00	782,96
Итого:		**108460**		**21692,00**	**3765,32**

На последнем этапе расчета затрат на выполнение ВКР необходимо определить величину накладных расходов. Расчёт затрат на накладные расходы производится по формуле:

$$З_{н.р.} = (З_{доп.з/пл} + З_{осн.з/пл}) * \frac{Н_{н.р.}}{100\%}, \quad (10)$$

где Н.Р. – процент принятых накладных расходов от основной и дополнительной заработной платы составляет 40%.

$$З_{н.р.} = (15666,73 + 111905,2) * 0,4 = 51028,77 \text{ (руб.)}$$

Для расчета совокупной величины затрат, связанных с проведением исследования, разработкой устройства или написанием программы, рекомендуется все проведенные расчеты оформить в виде таблицы.

Общие затраты на выполнение ВКР приведены в таблице 7.

Таблица 7 – Затраты на ВКР

№ п/п	Наименование статьи затрат	Сумма, руб.
1	Расходы на оплату труда	127572,23
2	Отчисления на социальные нужды	38271,58

3	Материальные затраты	2346,00
4	Расходы на содержание и эксплуатацию оборудования	516,00
5	Амортизационные отчисления	3765,32
6	Накладные расходы	51028,77
	Итого затрат:	**223499,90**

4.5 Бизнес-модель

В таблице 8 представлена бизнес-модель получившейся системы.

Таблица 8 – Бизнес-модель

Потребительский сегмент	Предприятия с охраняемыми помещениями
Ценностное предложение	Комплексная система выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа, недорогая в сравнении с конкурентами, возможность внедрения в автоматизированные системы предприятий
Каналы сбыта	Презентации системы на тематических конференциях, личные встречи с клиентами
Взаимоотношения с клиентами	Разработка, внедрение, техническое обслуживание
Структура издержек	Аренда офиса, закупка комплектующих, заработная плата сотрудников
Ключевые виды деятельности	Обеспечение безопасности на предприятии и предотвращение противоправных действий

	внутренними нарушителями
Ключевые ресурсы	Финансирование, персонал
Потоки поступления доходов	Ежемесячная оплата за техническое обслуживание

4.6 Вывод

В данном разделе рассмотрены вопросы по коммерциализации результатов выпускной квалификационной работы по разработке системы выявления аномалий в поведении сотрудников организации на основе данных системы контроля доступа, а так же представлена бизнес-модель по реализации системы.

В результате затраты на коммерциализацию данного проекта составят 223499,90 рублей.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы были построены модели предметной области и разработанной системы. Модель предметной области включает в себя диаграмму бизнес-процесса "Как есть" и диаграмму бизнес-процесса "Как должно быть" в нотации IDEF0 . Модель системы проектировалась в нотации UML и включает в себя описание функциональных возможностей системы, ее логической и физической структуры, а так же схему взаимодействия модулей. Объем кода составляет более 800 строк.

Полученный программный модуль отвечает всем требованиям пользователей, а так же выполняет все задачи и цель ВКР. Разработанная система готова к использованию в системе безопасности предприятия виде дополнительной программы контроля, а так же для последующего распространения.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. - База нормативных документов www.complexdoc.ru [Электронный ресурс]. – Режим доступа: http://expert-01.com/assets/images/uslugi/kontrol_dostupa/GOST%20R%2051241-2008.pdf
2. A Multi-agent Based Framework for the Simulation of Human and Social Behaviors during Emergency Evacuations. - Stanford Engineering Informatics Group [Электронный ресурс]. - Режим доступа: http://eil.stanford.edu/publications/xiaoshan_pan/AI&Society.pdf
3. Insider threats: Detecting and controlling malicious insiders. - Semantic Scholar - An academic search engine for scientific articles [Электронный ресурс]. – Режим доступа: https://pdfs.semanticscholar.org/018f/70a19824c433b32f1edfaf18e51dc1fca5e1.pdf
4. Лучшие системы контроля сотрудников и учета рабочего времени [Электронный ресурс]. - Режим доступа: https://employee-monitoring-software.ru/
5. Система контроля и управления доступом. - Википедия — свободная энциклопедия [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/Система_контроля_и_управления_доступом
6. Положение о системе контроля управлением доступом (СКУД). - ГАУЗ СО «СОСП» [Электронный ресурс]. - Режим доступа: http://sosp.ru/files/file/polozhenie-o-polzovanii-skud.doc

7. BackgroundWorker Class. - Microsoft Developer Network [Электронный ресурс]. - Режим доступа: https://msdn.microsoft.com/en-us/library/system.componentmodel.backgroundworker(v=vs.110).aspx
8. Async/await vs BackgroundWorker. - Stack Overflow - Where Developers Learn, Share, & Build Career [Электронный ресурс]. - Режим доступа: https://stackoverflow.com/questions/12414601/async-await-vs-backgroundworker
9. GitHut - Programming Languages and GitHub [Электронный ресурс]. - Режим доступа: http://githut.info/
10. GitHub. - Википедия — свободная энциклопедия [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/GitHub
11. Visual Studio IDE, Code Editor, VSTS, & App Center [Электронный ресурс]. - Режим доступа: https://www.visualstudio.com/
12. L. Tan, M. Hu, H. Lin. “Agent-based simulation of building evacuation”. International Journal of Information Sciences. 2015. vol. 295 no.C. pp. 53-66.
13. Hubstuff Employee Monitoring Software. [Online], Available: https://hubstaff.com/employee_monitoring_software
14. WaveTrend Access Control, [Online], Available: http://www.wavetrend.net/access-control.php
15. Employee Monitoring and Productivity Analysis. [Online], Available: https://www.intesecurity.com/employee-monitoring-and-productivity-analysis/
16. ObserveIT Insider Threat Solution. [Online], Available: https://www.observeit.com/insider-threat-solution

17. T.Bussa, A. Litan, T. Phillips. Market Guide for User and Entity Behavior Analytics [Online], Available: https://www.gartner.com/doc/3538217/market-guide-user-entity-behavior
18. Vast Challenge Website [Online], Available: http://vacommunity.org/
19. T. M. T. Do and D. Gatica-Perez, "GroupUs: Smartphone Proximity Data and Human Interaction Type Mining," 2011 15th Annual International Symposium on Wearable Computers, San Francisco, CA, 2011, pp. 21-28.
20. N. Andrienko, G. Andrienko, "Visual analytics of movement: an overview of methods, tools and procedures. Information Visualization", vol.12(1), 2013, pp. 3-24.
21. S. Gupta, M. Dumas, M. J. McGuffin and T. Kapler, "MovementSlicer: Better Gantt charts for visualizing behaviors and meetings in movement data," 2016 IEEE Pacific Visualization Symposium (PacificVis), Taipei, 2016, pp. 168-175.
22. (2017) LinkedIn Network Visualization and Analysis [Online], Available: http://socilab.com/#home
23. D. N Philip. “Social network analysis to examine interaction patterns in knowledge building communities”, Canadian Journal of Learning and Technology, Vol 36.
24. L. Chittaro, R. Ranon, L. I, “VU-Flow: A Visualization Tool for Analyzing Navigation in Virtual Environments”. IEEE Transactions on Visualization and Computer Graphics 12, 2006, pp. 1475-1485
25. H. Guo et al., "TripVista: Triple Perspective Visual Trajectory Analytics and its application on microscopic traffic data at a road intersection", IEEE Pacific Visualization Symposium PacificVis, 2011, pp.163-170.

26. G. Andrienko , N. Andrienko, H. Schumann, C. Tominski, “Visualization of Trajectory Attributes in Space–Time Cube and Trajectory Wall”, 2014, pp. 157-163.
27. E.S. Novikova, I.N. Murenin, A.V. Shorov. “Visualizing Anomalous Activity in the Movement of Critical Infrastructure Employees”, IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2017, pp. 504-509.
28. E. Novikova, I. Murenin. “Visualization-Driven Approach to Anomaly Detection in the Movement of Critical Infrastructure” Computer Network Security. MMM-ACNS 2017. Lecture Notes in Computer Science, vol 10446. Springer, Cham.
29. I.N.Murenin, E.S.Novikova, A.A. Volkov. “Uncovering Interaction Patterns between Employees of the Organization”, Proceedings of the XX International Conference on Soft Computing And Measurements (SCM'2017), Saint Petersburg, Russia, 2017, pp. 746-749.
30. Hout, M. C., Papesh, M. H., & Goldinger, S. D. (2013). Multidimensional scaling. Wiley Interdisciplinary Reviews. Cognitive Science, 4(1), 93–103. http://doi.org/10.1002/wcs.1203

ПРИЛОЖЕНИЕ А. ЛИСТИНГ ПРОГРАММЫ

GraphByDateFillin.sql

```
TRUNCATE TABLE [graphbydate]

DECLARE @minTimeDiff INT-- choose minimum
time for [duration]

DECLARE parent_table_cursor CURSOR --
ОБЬЯВЛЯЕМ КУРСОР
FOR
SELECT start_time,
end_time,
[user_id],
[floor],
[zone],
duration
FROM[intervals]
ORDER BY [start_time]

OPEN parent_table_cursor -- ОТКРЫВАЕМ КУРСОР
-- КУРСОР СОЗДАН, ОБЬЯВЛЯЕМ ПЕРЕМЕННЫЕ И
ОБХОДИМ НАБОР СТРОК В ЦИКЛЕ
DECLARE @parent_COUNTER INT,
@parent_loop INT,
@parent_start_time DATETIME,
@parent_end_timeDATETIME,
@parent_user_id INT,
@parent_floorINT,
@parent_zone VARCHAR(50),
@parent_durationINT

SET @parent_COUNTER = 0

FETCH next FROM parent_table_cursor INTO
@parent_start_time, @parent_end_time,
@parent_user_id, @parent_floor,
@parent_zone, @parent_duration

SET @parent_loop = @@FETCH_STATUS

WHILE @parent_loop = 0
BEGIN
DECLARE child_table_cursor CURSOR --
ОБЬЯВЛЯЕМ КУРСОР
FOR
SELECT start_time,
end_time,
[user_id],
[floor],
[zone],
duration
FROM[intervals]
WHERE[start_time] >= @parent_start_time
AND [start_time] <= @parent_end_time
AND [floor] = @parent_floor
AND [zone] = @parent_zone
AND [user_id] <> @parent_user_id
ORDERBY [start_time]

OPEN child_table_cursor -- ОТКРЫВАЕМ КУРСОР

DECLARE @child_COUNTER INT,
@child_loop INT,
@child_start_time DATETIME,
@child_end_timeDATETIME,
@child_user_id INT,
@child_floorINT,
@child_zone VARCHAR(50),
@child_durationINT

SET @child_COUNTER = 0

FETCH next FROM child_table_cursor INTO
@child_start_time, @child_end_time
,
@child_user_id, @child_floor, @child_zone,
@child_duration

SET @child_loop = @@FETCH_STATUS

WHILE @child_loop = 0 -- read
[intervals]Child line by line
BEGIN -- for each user who has been there
IF EXISTS (SELECT *
FROM[graphbydate]
WHERE[user_source_id] <> [user_target_id]
AND (
 ([user_source_id] = @parent_user_id
AND [user_target_id] = @child_user_id )
 OR ( [user_source_id] = @child_user_id
AND [user_target_id] = @parent_user_id )
 )
 AND [date] = CONVERT(date,
@parent_start_time)
 AND [zone] = @parent_zone
 AND [floor] = @parent_floor)
BEGIN -- line already exists, then UPDATE
DECLARE @graph_duration INT,
@graph_times INT

SELECT @graph_duration = duration,
 @graph_times = times
FROM[graphbydate]
WHERE[user_source_id] <> [user_target_id]
 AND (
 ([user_source_id] = @parent_user_id
AND [user_target_id] = @child_user_id )
 OR ( [user_source_id] = @child_user_id
AND [user_target_id] = @parent_user_id )
 )
AND [date] = CONVERT(date,
@parent_start_time)
AND [zone] = @parent_zone
AND [floor] = @parent_floor
ORDERBY [date]

IF ( Datediff(minute, @child_start_time,
@parent_end_time) >=
Datediff(minute, @child_start_time,
@child_end_time) )
SET @minTimeDiff = Datediff(minute,
@child_start_time,
@child_end_time)
ELSE
SET @minTimeDiff = Datediff(minute,
@child_start_time,
@parent_end_time)

BEGIN try-- try to UPDATE
 UPDATE [graphbydate]
 SET [duration] = @graph_duration
+ @minTimeDiff,
```

```
[times] = @graph_times + 1
 WHERE[user_source_id] <> [user_target_id]
AND (
 ([user_source_id] = @parent_user_id
AND [user_target_id] = @child_user_id )
 OR ( [user_source_id] = @child_user_id
AND [user_target_id] = @parent_user_id )
 )
AND       [date]       =       CONVERT(date,
@parent_start_time)
AND [zone] = @parent_zone
AND [floor] = @parent_floor
END try

BEGIN catch
 -- ...UPDATE or nothing
 PRINT 'Cannot UPDATE [GraphByDate]'
END catch
END-- of IF EXISTS
ELSE
BEGIN -- there is no such lines, then INSERT

IF   (   Datediff(minute,   @child_start_time,
@parent_end_time) >=
Datediff(minute,           @child_start_time,
@child_end_time) )
SET    @minTimeDiff    =    Datediff(minute,
@child_start_time,
@child_end_time)
ELSE
SET    @minTimeDiff    =    Datediff(minute,
@child_start_time,
@parent_end_time)

BEGIN try-- try to INSERT
SET @numberOfLines = @numberOfLines + 1
 INSERT INTO [graphbydate]
 ([date],
user_source_id,
user_target_id,
duration,
times,
[zone],
[floor])
 VALUES(CONVERT(date, @parent_start_time),
@parent_user_id,
@child_user_id,
@minTimeDiff,
1,
@parent_zone,
@parent_floor)
END try

BEGIN catch
 -- ...UPDATE or nothing
 PRINT 'Cannot INSERT INTO [GraphByDate]'
END catch
END-- IF EXISTS

FETCH  next  FROM  child_table_cursor  INTO
@child_start_time,
@child_end_time
,
@child_user_id,  @child_floor,  @child_zone,
@child_duration

SET @child_loop = @@FETCH_STATUS
END

--SELECT @child_COUNTER AS FINAL_COUNT
CLOSE child_table_cursor

DEALLOCATE child_table_cursor

SET @parent_COUNTER = @parent_COUNTER + 1

FETCH  next  FROM  parent_table_cursor  INTO
@parent_start_time,
@parent_end_time,            @parent_user_id,
@parent_floor, @parent_zone,
@parent_duration

SET @parent_loop = @@FETCH_STATUS
END

CLOSE parent_table_cursor

DEALLOCATE               parent_table_cursor
```

Anomalies.sql

```
TRUNCATE TABLE [AnomaliesTEMP]
DECLARE unique_floors_cursor CURSOR
FOR
SELECT DISTINCT [floor]
FROM [intervals]
OPEN   unique_floors_cursor   --   ОТКРЫВАЕМ
КУРСОР
DECLARE @floor_COUNTER INT,
@floor_loopINT,
@floor_idINT
SET @floor_COUNTER = 0
FETCH  next  FROM  unique_floors_cursor  INTO
@floor_id
SET @floor_loop = @@FETCH_STATUS
WHILE @floor_loop = 0
BEGIN
DECLARE unique_zones_cursor CURSOR
FOR
SELECT DISTINCT [zone]
FROM [intervals]
OPEN unique_zones_cursor -- ОТКРЫВАЕМ КУРСОР
DECLARE @zone_COUNTER INT,
@zone_loopINT,
@zone_idINT
SET @zone_COUNTER = 0
FETCH  next  FROM  unique_zones_cursor  INTO
@zone_id
SET @zone_loop = @@FETCH_STATUS
WHILE @zone_loop = 0
BEGIN
DECLARE unique_users_cursor CURSOR
FOR
SELECT DISTINCT [user_id]
FROM [intervals]
OPEN unique_users_cursor -- ОТКРЫВАЕМ КУРСОР
DECLARE @parent_COUNTER INT,
@parent_loopINT,
@parent_user_id INT
SET @parent_COUNTER = 0
FETCH  next  FROM  unique_users_cursor  INTO
@parent_user_id

SET @parent_loop = @@FETCH_STATUS
WHILE @parent_loop = 0
```

```
BEGIN
DECLARE target_users_cursor CURSOR
FOR
SELECT DISTINCT [user_id]
FROM [intervals]

OPEN target_users_cursor
DECLARE @child_COUNTER INT,
@child_loopINT,
@child_user_id INT

SET @child_COUNTER = 0
FETCH  next  FROM  target_users_cursor  INTO
@child_user_id
SET @child_loop = @@FETCH_STATUS

WHILE @child_loop = 0
BEGIN
DECLARE @avg_duration INT
SELECT @avg_duration = Avg([duration])
FROM graphbydate
WHERE[user_source_id] <> [user_target_id]
 AND ( ( [user_source_id] = @parent_user_id
 AND [user_target_id] = @child_user_id )
OR ( [user_source_id] = @child_user_id
 AND [user_target_id] =
 @parent_user_id
 ) )

IF EXISTS (SELECT *
 FROM [graphbydate]
 WHEREduration > @avg_duration
AND [user_source_id] <>
[user_target_id]
AND ( ( [user_source_id] =
@parent_user_id
AND [user_target_id] =
@child_user_id
)
 OR ( [user_source_id] =
@child_user_id
AND [user_target_id] =
@parent_user_id
)
))
BEGIN -- if there is such pair of people
IF (SELECT Count(*)
FROM [anomaliestemp]
WHEREduration > @avg_duration
 AND [user_source_id] <>
 [user_target_id]
 AND ( ( [user_source_id] =
 @parent_user_id
 AND [user_target_id] =
 @child_user_id
 )
OR ( [user_source_id] =
 @child_user_id
 AND [user_target_id] =
 @parent_user_id
 )
 )) =0
--if anomaly is in [AnomaliesTEMP]
BEGIN
BEGIN try-- try to INSERT
INSERT INTO [anomaliestemp]
([date],
 user_source_id,
 user_target_id,
 duration,
 times,
 [zone],
 [floor])
SELECT [date],
 user_source_id,
 user_target_id,
 duration,
 times,
 [zone],
 [floor]
FROM graphbydate
WHEREduration > @avg_duration
 AND [user_source_id] <>
 [user_target_id]
 AND ( ( [user_source_id] =
 @parent_user_id
 AND [user_target_id] =
 @child_user_id
 )
OR ( [user_source_id] =
 @child_user_id
 AND [user_target_id]
 =
 @parent_user_id
 )
 )
END try-- try to INSERT

BEGIN catch
PRINT
'Cannot INSERT INTO [AnomaliesTEMP]'
END catch
END
END -- if there is such pair of people

SET @child_COUNTER = @child_COUNTER + 1
FETCH  next  FROM  target_users_cursor  INTO
@child_user_id

SET @child_loop = @@FETCH_STATUS
END
CLOSE target_users_cursor

DEALLOCATE target_users_cursor

SET @parent_COUNTER = @parent_COUNTER + 1
FETCH  next  FROM  unique_users_cursor  INTO
@parent_user_id

SET @parent_loop = @@FETCH_STATUS
END
CLOSE unique_users_cursor

DEALLOCATE unique_users_cursor

SET @zone_COUNTER = @zone_COUNTER + 1
FETCH  next  FROM  unique_zones_cursor  INTO
@zone_id

SET @zone_loop = @@FETCH_STATUS
END
CLOSE unique_zones_cursor

DEALLOCATE unique_zones_cursor

SET @floor_COUNTER = @floor_COUNTER + 1
FETCH  next  FROM  unique_floors_cursor  INTO
@floor_id
-- ЗАВЕРШЕНИЕ ЛОГИКИ ВНУТРИ ЦИКЛА
END
CLOSE unique_floors_cursor
```

```
DEALLOCATE              unique_floors_cursor
```