Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы – Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«____» _____ 2022 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка средств защиты данных для Правительства Амурской области

Исполнитель
студент группы 855-об _____ А.А. Барсук
(подпись, дата)

Руководитель
доцент, канд.техн.наук _____ А.В. Бушманов
(подпись, дата)

Консультант
по безопасности и
экологичности
доцент, канд.техн.наук _____ А.Б. Булгаков
(подпись, дата)

Нормоконтроль
инженер _____ В.Н. Адаменко
(подпись, дата)

Благовещенск 2022

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____ А.В. Бушманов
«____» _____ 2022 г.

ЗАДАНИЕ

К выпускной квалификационной работе студента Барсук Алёны Алексеевны

1. Тема выпускной квалификационной работы: Разработка средств защиты данных для Правительства Амурской области.

(утверждена приказом от 05.04.2022 № ____-уч)

2. Срок сдачи студентом законченной работы (проекта):_____

3. Исходные данные к выпускной квалификационной работе: отчет по преддипломной практике.

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): описание предметной области и документооборота, обоснование необходимости разработки и определение требований, разработка программного продукта, обоснование безопасности и экологичности программного продукта, руководство пользователя.

5. Перечень материалов приложения (наличие чертежей, таблиц, графиков, схем, программных продуктов, иллюстративного материала и т.п.): техническое задание, блок-схема алгоритма работы программного продукта.

6. Консультанты по выпускной квалификационной работе (с указанием относящихся к ним разделов): консультант по безопасности и экологичности Булгаков А.Б., доцент, канд.техн.наук.

7. Дата выдачи задания: _____

Руководитель выпускной квалификационной работы: Бушманов А.В., доцент, канд.техн.наук.

Задание принял к исполнению (_____): _____

(подпись студента)

РЕФЕРАТ

Бакалаврская работа содержит 53 страницы, 1 таблицу, 8 рисунков, 21 источник, 2 приложения.

РАСПОЗНАВАНИЕ ОБРАЗОВ, РАСПОЗНАВАНИЕ ЛИЦА, РАЗРАБОТКА ПРИЛОЖЕНИЯ, МОДЕЛЬ НАРУШИТЕЛЯ, ПОЛИТИКА ИБ, БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ

В ходе работы сделан документооборот и произведён анализ безопасности на предприятии, на основе этого выполнена разработка десктопного приложения для защиты данных от несанкционированного допуска.

Цель работы – разработка приложения распознавания лица с функцией блокировки экрана.

Объект исследования – Правительство Амурской области

Задачами выпускной квалификационной работы являются анализ безопасности предприятия и разработка средства защиты данных.

Результатом бакалаврской работы является анализ безопасности на предприятии и разработка десктопного приложения для распознавания лица с функцией блокировки экрана, для защиты персональных данных и данных различной степени секретности от несанкционированного доступа к ним.

(Вся информация, представленная в данной работе, является общедоступной)

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АО – Амурская область;

ИБ – информационная безопасность;

ИС – информационная система;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПК – персональный компьютер;

ПО – программное обеспечение;

РФ – Российская Федерация;

СБ – служба безопасности;

ТЗ – техническое задание.

ВВЕДЕНИЕ

В настоящее время современные технологии развиваются с невероятной скоростью, это касается, как и вполне обыденных вещей, например, нового смартфона или бытовой техники, так и тех, о которых все знают, но думают в последнюю очередь. Речь идёт о технологиях, что обеспечивают безопасность человека что в сети интернет, что в реальной жизни.

Одной из таких технологий является распознавание лица, и она знакома уже многим, так как уже присутствует во многих смартфонах и известна как «Face ID». Одна из областей применения это поиск преступников, данные лиц, которых загружены в систему поиска. Подобные системы сейчас используют в уличных камерах видеонаблюдения, на контрольно-пропускных пунктах предприятий и некоторых частных домах.

Однако, данная технология применяется не только для определения лица в толпе или хозяина устройства, сейчас данная система может распознать возраст человека и испытываемые им эмоции. Такие распознаватели применяются в исследовании реакций людей на какие-либо явления, а также маркетологами, чтобы выяснить, на сколько приятен человеку то или иной продукт.

Целью данной работы является разработка десктопного приложения для распознавания лица с функцией блокировки экрана. Данная программа поможет защитить данные, с которыми работает пользователь, от несанкционированного доступа к ним.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Технологии распознавания образов

Распознавание образов развивающаяся активными темпами дисциплина, что относится к математической кибернетике. Оно нашло применение во многих областях, таких как медицина, экономика, социология, физика, биология, а также в других сферах.

Распознавание по лицу также относится к распознаванию образов и является его частным случаем. Распознавание образов выявляет объекты с помощью системы классификаторов и критериев.

Распознавание можно применить только в том случае, если есть схожие объекты, ведь, несмотря на то что, все предметы разные, между ними также есть много сходств, будь то размер, цвет, форма и другие признаки.

1.2 Механизм распознавания лиц

Чтобы начать процесс распознавания, необходимо обнаружить само лицо. Нейронные сети очень хорошо подходят для подобной работы, однако, это дорого, поэтому, в данной бакалаврской работе для обнаружения лица метод Виолы — Джонса.

Этот алгоритм сканирует изображение при помощи прямоугольников, которые называются примитивами (вейвлетами) Хаара (Рисунок 1 – Рисунок 2).

Эти объекты предполагают нахождение на изображении наиболее тёмных и светлых областей, которые характерны для человеческого лица. (Рисунок 3).

Подобных признаков очень много, поэтому их нужно классифицировать, а также отделять от других изображений, так как подобные признаки присущи не только человеку.

Первый этап. Происходит поиск первого признака. После того как он будет обнаружен, система уже точно будет знать, что на фото есть лицо человека и дальше будет искать признаки. После нахождения трёх признаков система отделяет от остального изображения область, на которой присутствует только искомое лицо.

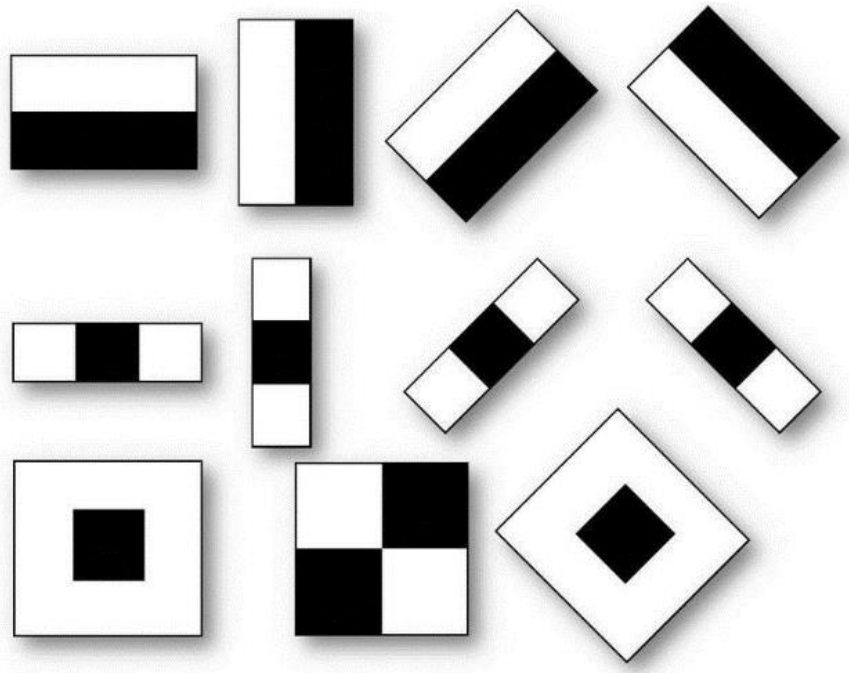

Рисунок 1 – Примитивы Хаара

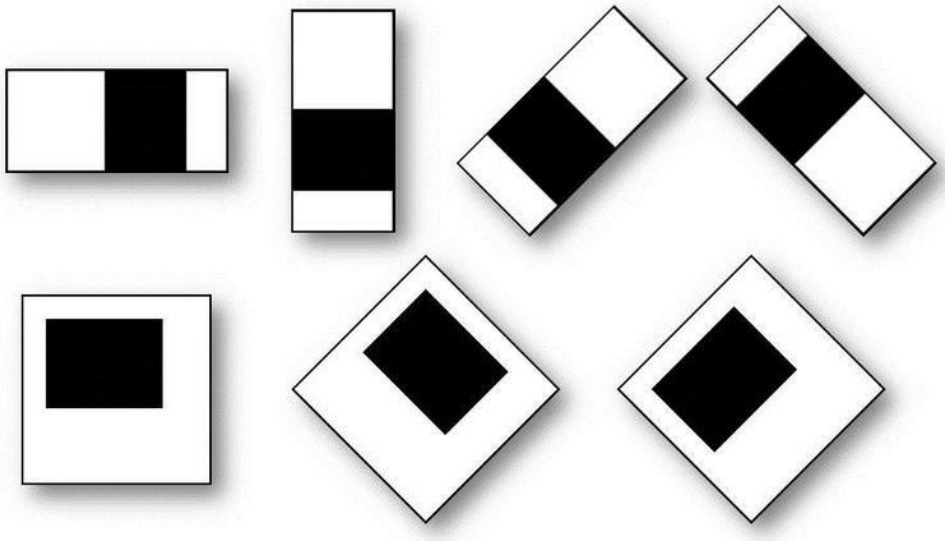

Рисунок 2 – Примитивы Хаара

Второй этап. Получив область для анализа, свою работу начинает биометрический алгоритм. Данный алгоритм расставляет на найденном лице специальные точки, по расстоянию между которыми, в дальнейшем, будут вычисляться индивидуальные особенности человека (форма носа, родинки, положение бровей и т.д.). Таких точек может быть очень много, но, как минимум, их должно быть шестьдесят восемь.

Третий этап. В идеальных условиях система должна распознавать лицо, которое смотрит анфас. Однако, человек не может всё время смотреть только в одну точку, сидя или стоя в одной и той же позе. Для этого в систему встроен специальная функция, которая «достраивает» и поворачивает лицо до нужного ракурса, что значительно повышает качество распознавания.

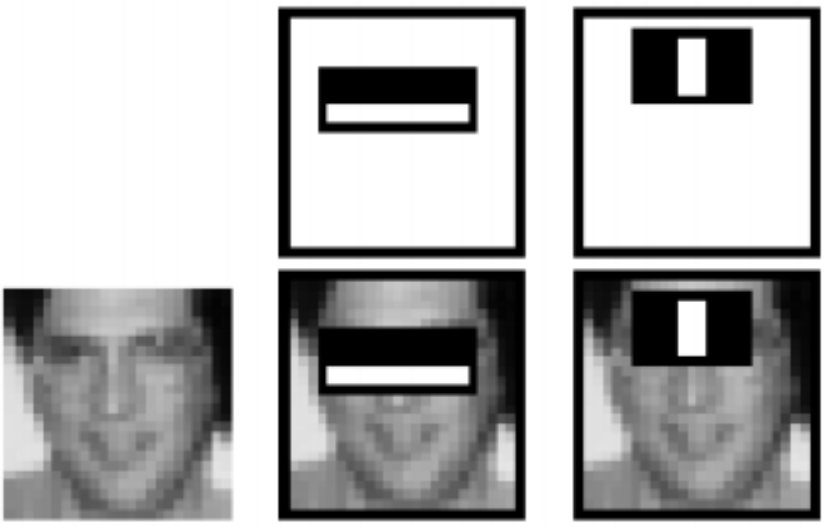

Рисунок 3 – Примерное обозначение тёмных и светлых областей на лице человека

Четвёртый этап. Далее нейросеть присваивает каждому лицу вектор признаков, а именно это число, являющееся суммой ранее найденных характеристик. Их также может быть очень много. Главное преимущество данного алгоритма в том, что он не учитывает посторонние факторы при распознавании (прическа, макияж).

Пятый этап. Система сравнивает полученный вектор с базой других векторов и идентифицирует, либо не идентифицирует пользователя.

1.3 Исследование и описание предметной области

Правительство Амурской области является высшим постоянно действующим коллегиальным исполнительным органом государственной власти области.

Деятельность Правительства Амурской области осуществляется в соответствии с принципами, установленными Федеральным законом «Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации».

Правительство Амурской области в пределах своих полномочий организует исполнение Конституции Российской Федерации, федеральных конституционных законов, федеральных законов, указов Президента Российской Федерации, постановлений Правительства Российской Федерации, Устава (Основного Закона) Амурской области, закона Амурской области «О Правительстве Амурской области», законов области, нормативных правовых актов губернатора Амурской области, осуществляет систематический контроль за их исполнением другими органами государственной власти и органами местного самоуправления.

1.4 Внешний документооборот

Внешний документооборот - движение документов в правовом пространстве, где действуют и реализуют правоотношения различные субъекты права – физические и юридические лица, граждане, предприятия и организации, органы местного самоуправления, органы государственной власти как между однородными по виду субъектами, так и с другими их видами.

Правительство Амурской области обменивается документацией с другими органами государственной власти.

Диаграмма внешнего документооборота, это контекстная диаграмма, построенная в нотации DFD (Рисунок 4).

1.5 Внутренний документооборот

Внутренний документооборот предполагает движение документации внутри предприятия или организации (например, между отделами), для их регуляции используются правила внутреннего распорядка, корпоративные акты и иные документы, индивидуальные для каждой организации.

Канцелярия – (Отдел по обеспечению деятельности исполнительных ор-

ганов государственной власти области ГБУ АО «Управление делами Правительства области») осуществляет обработку и регистрацию входящей и исходящей документации в Правительстве АО.

Рисунок 4 – Диаграмма внешнего документооборота Правительства Амурской области

Все входящие и исходящие документы правительства проходят через Канцелярию, а после сортировки отправляются в отделы по назначению.

Диаграмма внутреннего документооборота представляет собой диаграмму декомпозиции внешнего документооборота (Рисунок 5).

1.6 Обоснование необходимости приложения

На данный момент распознавание лиц является распространенным явлением, однако, используется далеко не везде. Чаще всего причина в дорогостоящем оборудовании, а именно видеокамерах. Также, для распознавания большого потока данных необходим соответствующий объём памяти, что тоже не дёшево. В рабочих кабинетах могут быть обычные видеокамеры, но, в большинстве своём, технологией распознавания они не оснащены. В Правительстве Амурской области существуют два типа рабочих мест, для которых подойдёт данная система.

Первое это защищаемое помещение, где, помимо всех уже имеющихся

мер защиты, можно использовать распознавание как ещё один защитный эшелон на пути злоумышленника. Конечно, такая система на долго его не остановит, но выиграет немного времени для службы безопасности Правительства.

Второе место это кабинеты, где обрабатывают обращения граждан, а также ведётся приём граждан. Так как сотрудники работают с ПДн, то было бы замечательно, если бы никто посторонний не смог их увидеть. В таком случае даже, если посторонний случайно или намеренно заглянет в монитор, то ничего не увидит.

Если обобщенно, то разработанное приложение добавляет ещё одну небольшую степень защиты, а именно идентификацию и аутентификацию по лицу.

Идентификация – присвоение уникального имени пользователю, который он должен предоставить системе защиты информации при попытке получения доступа к объекту. В данной работе, идентификатором выступает фотография пользователя.

Аутентификация – это подтверждение идентификатора пользователя, проверка принадлежности идентификатора к конкретному пользователю и его подлинность. Приложение сверяет получаемый образ с камеры с уже загруженной фотографией пользователя.

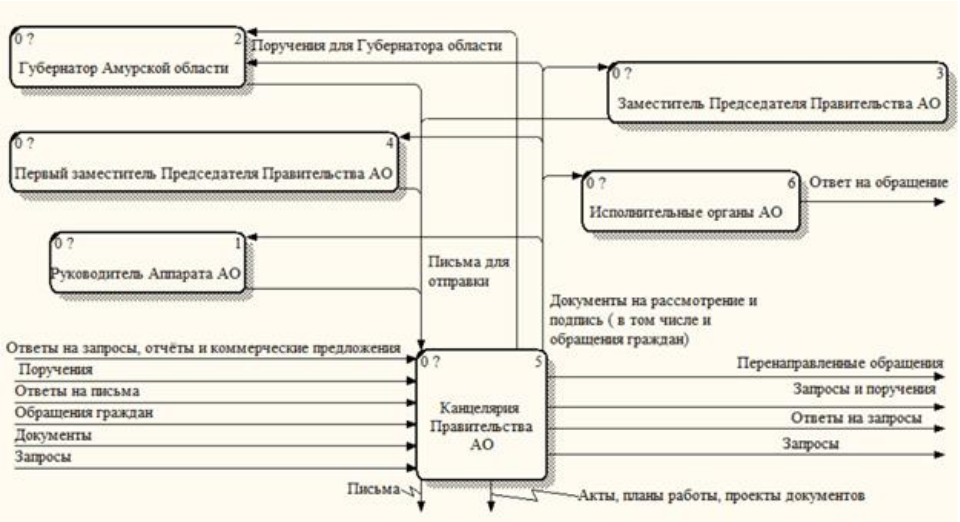

Рисунок 5 – Диаграмма внутреннего документооборота Правительства Амурской области

2 ПРОЕКТИРОВАНИЕ ПРИЛОЖЕНИЯ И АНАЛИЗ ЗАЩИЩЕННОСТИ ПРЕДПРИЯТИЯ

Настольное (desktop) приложение - программа, обрабатываемая на стороне клиента и запускаемая в виде обыкновенного исполняемого файла на устройстве пользователя. В качестве такого устройства может быть компьютер, коммуникатор или смартфон.

2.1 Цель и задачи проектирования

Цель проектирования приложения – разработка приложения для обеспечения безопасности данных пользователей с помощью механизма распознавания лица.

При проектировании необходимо решить следующие задачи:

– определить язык для разработки приложения;

– выбрать среду для разработки приложения с учетом выбранного ранее языка;

– разработать функциональные модули в соответствии с функциями, которые будут реализованы в программе;

– реализовать программный продукт в соответствии с требованиями заказчика.

Для разработки данного приложения составлено техническое задание, с которым можно ознакомиться в приложении А.

2.2 Средства разработки приложения

Для разработки приложения была выбрана среда разработки «PyCharm».

PyCharm это интегрированная среда разработки для языка программирования Python. Предоставляет средства для анализа кода, графический отладчик.

В качестве языка программирования был выбран язык «Python»

Python – высокоуровневый интерпретируемый язык программирования общего назначения. Его философия дизайна подчеркивает читабельность кода с использованием значительных отступов.

Python динамически типизируется и собирает мусор. Это легко читаемый язык. Его форматирование визуально не загромождено и часто использует английские ключевые слова, где другие языки используют знаки препинания. В отличие от многих других языков, хоть в нём и предусмотрены в синтаксисе фигурные скобки и точки с запятой, но используются редко. В нем меньше синтаксических исключений и особых случаев, чем в языках семейства C.

Для работы для разработки меню было выбрано несколько основных библиотек Python.

Пакет tkinter («интерфейс Tk») — стандартный интерфейс Python для набора инструментов Tk GUI. И Tk, и tkinter доступны на большинстве платформ Unix, а также в системах Windows.

Python Imaging Library (сокращенно PIL) — библиотека языка Python (версии 2), предназначенная для работы с растровой графикой.

Разработка библиотеки прекращена (последняя правка датируется 2011 годом). Однако проект под названием Pillow, являющийся форком PIL, развивается и включает, в том числе, поддержку Python 3.x.

Face_recognition это библиотека, построенная на C++ библиотеке dlib. Отличается высокой точностью, очень удобна в использовании, ее легко развернуть на сервере.

Функционал библиотеки:

- поиск и идентификация лиц на фото;
- поиск черт лица на фотографиях;
- создание карты координат специфических лицевых точек;
- применима в realtime-решениях.

OpenCV — это библиотека обработки изображений и видео, которая используется для их анализа. Ее применяют для обнаружения лиц, считывания номерных знаков, редактирования фотографий, расширенного роботизированного зрения, оптического распознавания символов и многого другого.

Основные преимущества OpenCV:

- имеет открытый программный код и абсолютно бесплатна;

– написана на C/C++ и в сравнении с другими библиотеками работает быстрее;

– не требует много памяти и хорошо работает при небольшом объеме RAM;

– поддерживает большинство операционных систем, в том числе Windows, Linux и MacOS.

Функционал библиотеки:

– кадрирование (выделение нужного участка картинки);

– изменение размера;

– поворот изображения;

– перевод цветного изображения в чёрно-белое/ градации серого;

– размытие/ сглаживание;

– рисование прямоугольников и линий (места для подписи объектов);

– надписи (текст на изображении);

– распознавание лица.

2.3 Выбор модели жизненного цикла ПО

Модель жизненного цикла (ЖЦ) есть последовательность, взаимодействие и смысловая наполненность этапов жизненного цикла. С выбора (или построения) модели жизненного цикла начинается работа над проектом. Она должна определяться в общих чертах ещё на этапе предпроектного анализа.

Основными моделями ЖЦ являются:

– каскадная;

– инкрементная

– спиральная.

Каждая модель является процессом, который структурно состоит из четырёх этапов:

– анализ и планирование;

– проектирование;

– кодирование;

– верификация и аттестация.

Каскадная модель предполагает строгую последовательность и документирование этапов. Переход к следующему этапу осуществляется только по окончанию предыдущего.

Инкрементная модель похожа на каскадную, но в данном случае, разработка ведётся в несколько инкрементов (версий), которые предполагают улучшение продукта, пока ЖЦ разработки ПО не прекратится. Это означает, что на каждом этапе ЖЦ возможны обратные связи, которые являются межэтапными корректировками. При этом, процесс ЖЦ растягивается на весь период разработки. Работа над проектом начинается с определения основных требований к системе. Далее, разработчик по принципу приращений, добавляют определенную функциональность в систему, при этом, сначала разрабатывает компоненты с наивысшем приоритетом и постепенно их детализирует. В то же время, возможно уточнение требований других частей системы.

При разработке определенно работающего компонента, он предоставляется клиенту, который может уточнить требования на основе использования этого компонента.

Недостатки и достоинства данной модели такие же, как и у каскадной, но в данном случае, заказчик может раньше увидеть результат и скорректировать требования, при этом, корректировка требований не является настолько затратной процедурой, по сравнению с каскадной моделью. Основным недостатком является ухудшение структуры системы, когда при добавлении новых компонентов и изменение требований ухудшают структуру системы. Чтобы избежать этого, нужно дополнительное время на рефакторинг.

Спиральная модель жизненного цикла представляет представлена последовательностью этапов, которые выполняются в каждой модели, в виде спирали. Начало витка – это анализ рисков и оценка вариантов, а также целесообразность разработки в целом и данного, витка в частности. Данная модель позволяет уделять внимание рискам, влияющим на организацию жизненного цик-

ла, что является недостатком для проектов, имеющих низкую степень риска, так как оценка рисков на каждом витке ведёт к большим затратам.

Так как на этапе кодирования возможны определенные изменения и при этом, необходимо предъявлять заказчику каждый модуль и согласовывать с ним необходимые изменения, было принято решение использовать инкрементную модель ЖЦ.

На основе проведённого анализа предметной области, анализа защищенности и других документов происходит проектирование структуры будущей программы.

Далее проводятся предварительные испытания, включающие в себя опытную эксплуатацию и приемочные испытания на предприятии.

После этого необходима установка готового приложения на рабочие станции, его настройка и обязательное тестирование всех компонентов приложения на работоспособность в различных условиях.

Для минимизации ошибок необходимо создать два руководства, одно для пользователя, другое для администратора, а также провести инструктаж сотрудников по работе с программой в штатном режиме, а также проработать варианты действий на случай сбоев работы.

2.4 Требования

2.4.1 Требования к пользователям

Для корректной работы программы на одном ПК необходим один пользователь и один администратор.

Администратор должен обладать высокими навыками владения ПК и пройти по работе с программой и технике безопасности. Также, администратор должен иметь право (в организации) оперировать созданием, выдачей и удалением паролей.

Пользователь также должен иметь навыки работы с персональным компьютером, и также пройти инструктаж по работе с программой.

2.4.2 Требования к методическому обеспечению

Приложение должно отвечать требованиям надежности:

– наличие идентификации и аутентификации пользователя;

– наличие защиты от некорректных действий пользователей.

На восстановление при отказе нужно несколько секунд, исправное функционирование пользователь может вернуть самостоятельно, не прибегая к помощи администратора, просто заполнив нужные поля и избавившись от некорректно внесённых данных.

2.4.3 Требования к техническому обеспечению

Для нормального функционирования программы, необходимы следующие технические средства: монитор, системный блок (либо же моноблок), источник бесперебойного питания, устройство видеофиксации (веб-камера, либо же встроенная камера), мышь, клавиатура.

Требуемые технические характеристики ПК:

– объем жесткого диска должен быть не менее 500 Гбайт;

– ОЗУ - 512 Мб или более;

– тактовая частота процессора не менее – 2.1 ГГц

2.5 Анализ защищенности предприятия

Службы безопасности предприятия каждый день сталкиваются с проблемой организации безопасного доступа членов персонала к своим рабочим местами. В связи с высокой численностью рабочих, службам безопасности необходимо прибегать к использованию специализированных систем и методов, чтобы автоматизировать процесс прохождения контроля в частности и обеспечения безопасности в целом.

Источники угроз ИБ делятся на внешние и внутренние.

К внешним источникам относятся:

– увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

– деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

– разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

– деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

– стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

– обострение международной конкуренции за обладание информационными технологиями и ресурсами;

К внутренним источникам относятся:

– недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

– недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

– неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

– недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

– недостаточная экономическая мощь государства;

– снижение эффективности системы образования, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

– недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

– отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

– критическое состояние отечественных отраслей промышленности;

– неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере;

– факт получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

В Правительстве Амурской области реализованы все требования безопасности в соответствии с приказом ФСТЭК России от 25 декабря 2017 г. N 239. Одни из них это:

– контрольно-пропускные пункты на каждом входе в здание;

– вооруженная охрана на КПП;

– система электронных пропусков;

– видеокамеры в коридорах;

– решетки на окнах первого этажа и на защищаемых помещениях;

– системы противопожарной безопасности;

– системы противодымной безопасности;

– датчики движения;

– антивирусные системы;
– парольная защита;
– аудит;
– криптографическая защита входящей и исходящей информации;
– разграничение доступа.

Объектами защиты являются: информация, обрабатываемая в ИС, и технические средства ее обработки и защиты.

2.6. Модель нарушителя

Злоумышленник - нарушитель, который намеренно идёт на нарушение из корыстных побуждений.

Есть два типа лиц, что могут находиться на предприятии это внутренние и внешние. К внешним относятся только посетители или гости (специально приглашенные лица), внутренними являются все сотрудники.

Мотивом действий у внешних лиц чаще всего является корыстный интерес, однако, зачастую, носит и непреднамеренный характер. У сотрудников мотивы более разнообразны, это, как и желание самоутвердиться (если человек занимает низкую должность), так и корыстный интерес. Однако, есть вероятность что сотрудник может быть просто безответственным, либо совершать противоправные действия по незнанию.

В соответствии с уровнем доступа, нарушитель может совершить большее, либо меньшее количество нарушений. Так, рядовой пользователь ПК, который может работать только с одной программой, будет более ограничен, чем его коллега, которому доступно две и более программ. Нарушителем может быть и сотрудник службы безопасности, который, помимо доступа к ПК, знает принципы работы охранных систем, а следовательно, может их обмануть, либо вовсе отключить. Если нарушителем является руководящее лицо, либо человек, который является разработчиком ПО, то ущерб, который они нанесут будет иметь очень серьёзные последствия, так как эти лица имеют доступ к обширному объёму данных предприятия, которым, зачастую, присваивают степень секретности.

Технические средства, используемые злоумышленниками, довольно сложно обнаружить, так как они являются предметами что есть почти у каждого человека. Нарушитель может вынести информацию на флешке, диске, на бумажном носителе, может сфотографировать документы или записать на диктофон (с помощью того же телефона) нужную информацию. Также, нарушитель может взломать камеры видеонаблюдения, установить подслушивающие устройства, принести носитель с вредоносной программой или просто устроить поджег.

К особой категории нарушителей относятся хакеры, так как хакером может являться кто угодно – посетитель, сотрудник, бывший сотрудник. Хакер может взломать систему или внедрить вирус по заказу, ради собственной выгоды, либо же просто ради веселья.

2.7 Политика информационной безопасности

Политика безопасности – это совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Негативные последствия нарушения политики могут включать в себя раскрытие или утрату чувствительной и конфиденциальной информации, утрату или раскрытие персональных данных, кражу интеллектуальной собственности, репутационные последствия, а также влияние на важные внутренние системы.

Любой сотрудник, нарушивший политику, может быть подвержен взысканию вплоть до увольнения, ему могут выписать штраф в соответствии с нанесённым ущербом, а также быть подвержен административной или иной ответственности в случае строгого нарушения или преднамеренного умысла, повлекшего большой ущерб учреждению.

2.7.1 Политика по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу

Настоящая политика определяет требования по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу.

Для найма персонала организация даёт соответствующее объявление в средствах массовой информации. Отдел кадров принимает резюме соискателей и наиболее подходящие по критериям передаёт начальнику соответствующего отдела. Начальник отдела ещё раз просматривает резюме и после выбора кандидатов относит список для согласования заместителю руководителя. Заместитель руководителя совместно с руководителем приглашают выбранных кандидатов на собеседование и формируют состав комиссии, что будет оценивать соискателя. Комиссия может быть созвана один раз или несколько, в зависимости от числа человек в самой комиссии и количестве соискателей.

Нанимаемый персонал, после собеседования, проходит различные тесты, определяющие уровень лояльности к различным слоям населения и группировкам, а также психологические, проверяющие её здравость и устойчивость. По результатам сотрудник попадает в одну из групп с различными уровнями допуска к информации, также, данная группа зависит и от занимаемой должности.

2.7.2 Политика парольной защиты

Все проводимые операции с паролями регулируются отделом по защите информации Правительства Амурской области, а ответственность за генерацию, использование, хранение и прочие операции с паролями возлагаются на администраторов соответствующего уровня допуска.

Длина пароля должна быть не менее восьми символов. Пароль должен включать в себя символы как минимум трех различных типов (например, цифры и буквы верхнего и нижнего регистра).

Пароль не должен включать в себя:

– легко вычисляемые сочетания символов, а также общепринятые сокращения и любые другие данные, которые можно определить исходя из информации о пользователе;

– последовательности из более чем 2 символов, расположенных рядом на клавиатуре;

– состоять из одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов.

Ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан. При вводе паролей необходимо исключить возможность его просмотра посторонними лицами или техническими средствами. Пользователь не имеет права сообщать личный пароль другим пользователям и допускать их к работе в своей учетной записи в ИС.

При хранении паролей должны быть приняты все возможные меры по минимизации возможности компрометации либо утери пароля. Запрещается:

– записывать пароли в файлах, электронных записных книжках, других электронных носителях информации;

– указывать пароли на бумажных и других материальных носителях информации, в том числе на предметах;

– хранить пароли в ИС в открытом виде.

Смена паролей должна происходить не реже одного раза в девяносто дней.

При потере пароля или его компрометации, пользователь должен обратиться к ответственному за пароли лицу. После этого пользователю выдаётся новый пароль, а старый блокируется. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 символах. При смене пароля новое значение не должно совпадать с 10 предыдущими значениями паролей.

Пароль прекращает действовать при:

– истечении срока действия или внеплановой смене;

– увольнении сотрудника или его переходе на другую должность.

3 РАЗРАБОТКА ПРОГРАММНОГО ПРОДУКТА

3.1 Общие сведения

Полное наименование программы «Приложение для защиты данных от несанкционированного доступа «Faseblock» для Правительства Амурской области».

Программный продукт написан на языке Python.

3.2 Описание логической структуры

Блок-схема (алгоритм) работы программы приведена в приложении Б.

Схематичная структура программы представлена на рисунке 6.

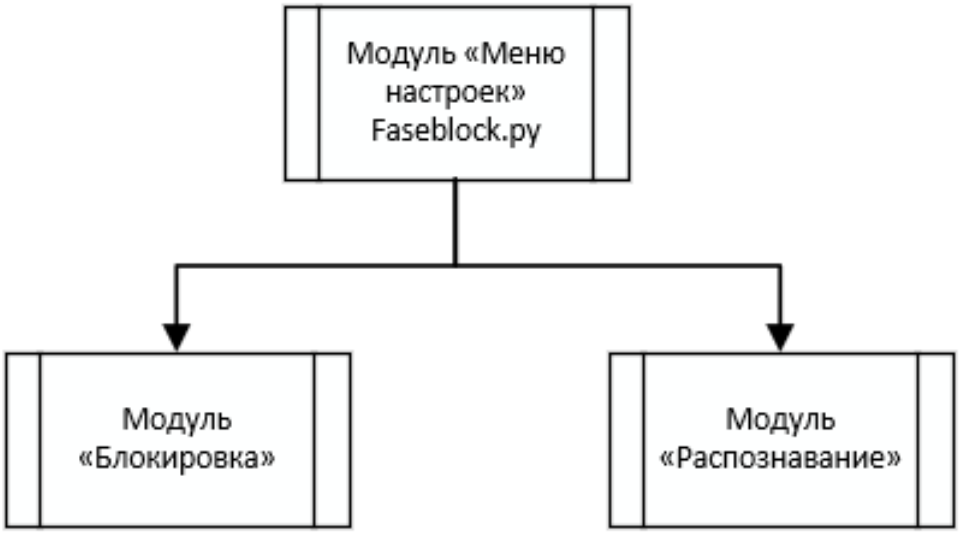

Рисунок 6 – Структура программного продукта

Модуль «Меню настроек» (Рисунок 7) предназначен для создания первичных настроек, с которыми будет работать приложение, открывается сразу после первого запуска программного продукта. Повторный запуск возможен при вводе комбинации клавиш (во время работы другого блока), либо при удалении файла настроек. Пользователь вводит своё имя, загружает снимок лица (что будет являться идентификатором), или же делает текущее фото, и выбирает фон экрана блокировки, который будет выводиться при непосредственной блокировке экрана (по умолчанию стоит тёмная тема; также можно выбрать

любую картинку из памяти компьютера). Далее администратор устанавливает пароль для выхода из режима блокировки экрана, а также тайм-аут для пользователя и тайм-аут для посторонних лиц.

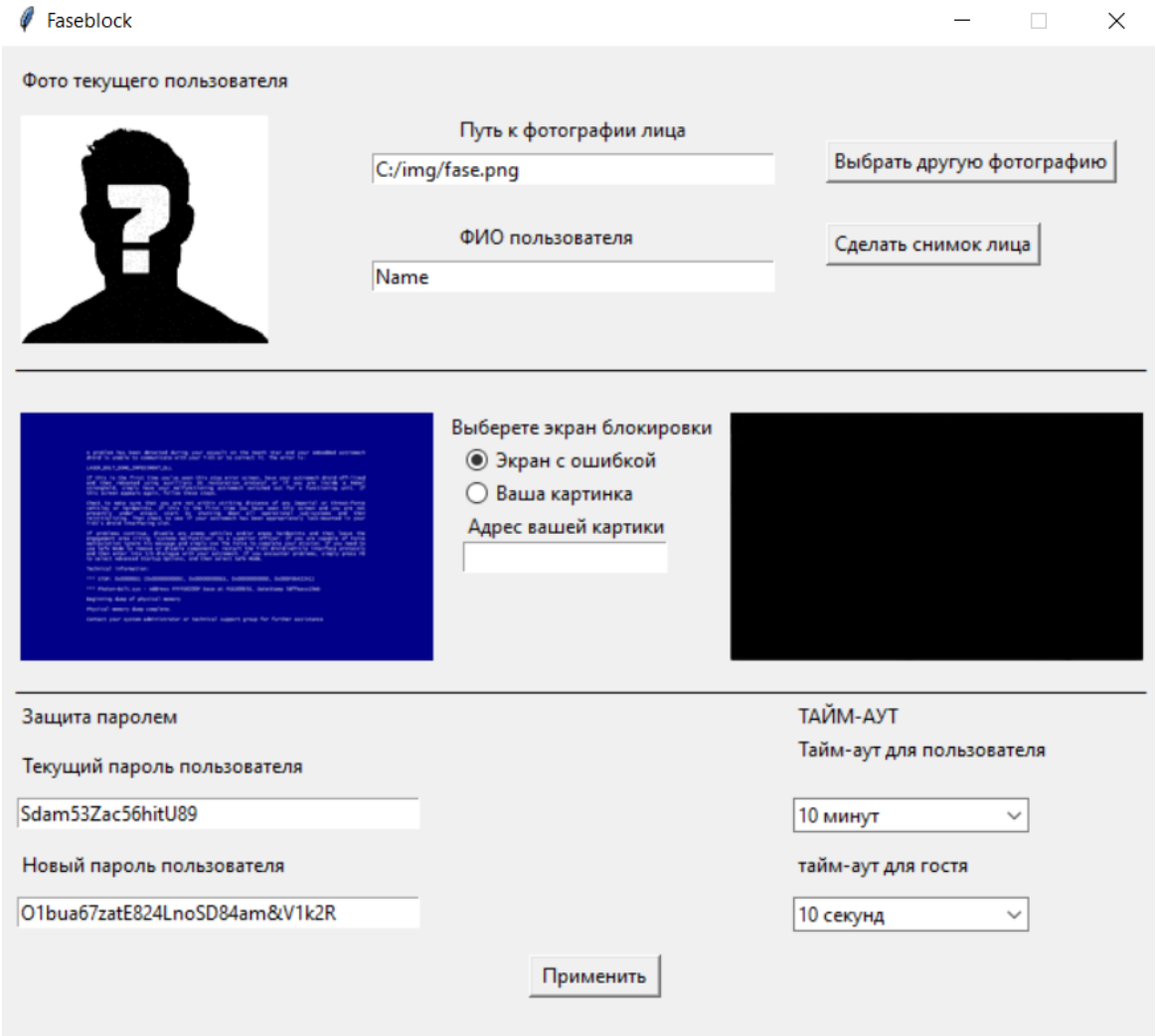

Рисунок 7 – Меню настроек

Модуль «Распознавание» предназначен для распознавания лица пользователя. Камера фиксирует лицо пользователя и сравнивает его с загруженным идентификатором (фотографией лица). То есть производится процесс идентификации и аутентификации. При обнаружении совпадений, модуль блокировки не вызывается, если совпадения не обнаружены, то вызывается модуль «Блокировка». Если камера фиксирует два лица вместо одного, то также вызывется модуль блокировки.

Модуль «Блокировка» предназначен для выведения масштабируемой картинки на экран монитора. После того как модуль «Распознавание» обнаружил нарушителя, запускается данный модуль и «поверх всего» появляется выбранная пользователем картинка, тем самым защищая информацию, выведенную на экране монитора от несанкционированного доступа. Данный модуль нельзя закрыть с помощью ввода комбинаций клавиш, а также, после его активации невозможно работать с другими приложениями. Возможен только вызов меню «Пуск» и использование команды Alt+Ctrl+Del. Чтобы прекратить работу модуля , либо, нужно предъявить правильный идентификатор, либо администратор должен ввести пароль.

3.3 Используемые технические средства

Для работы с приложением используются персональные компьютеры с операционной системой Windows 7/8/8.1/10 или Ubuntu.

3.4 Вызов и загрузка

Для запуска/загрузки программы нужно запустить файл Faseblock.exe.

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

В данной главе рассмотрим безопасность, экологичность и возможные чрезвычайные ситуации для офисного помещения Правительства Амурской области

4.1 Безопасность

4.1.1 Условия труда

На своём рабочем месте сотрудник может подвергаться влиянию различных факторов, например, природно-климатическими, или же связанными с профессиональной деятельностью, которые не всегда положительно влияют на здоровье. Факторы, которые способны при определенных условиях вызывать острое нарушение здоровья и гибель организма называют опасными. Факторы, которые отрицательно влияют на работоспособность или вызывают профессиональные заболевания и другие неблагоприятные последствия называют вредными.

Вредные и опасные факторы можно разделить на:

– химические;

– физические;

– биологические.

Вредные факторы можно разделить на:

– физические;

– физиологические;

– нервно-психические.

Во время рабочего процесса в кабинетах Правительства оказывают влияние вредные факторы. У сотрудников нередки случаи возникновения физических перегрузок из-за неудобного положения тела во время работы за ПК.

Случаются нервно-психические перегрузки, так как в основном, сотрудники работают за компьютером с поступающей к ним информацией, то есть занимаются умственным трудом.

Организация работы с ПЭВМ осуществляется в зависимости от вида и категории трудовой деятельности. Виды трудовой деятельности разделяются на 3 группы (Таблица 1): группа А – работа по считыванию информации с экрана ВДТ с предварительным запросом; группа Б – работа по вводу информации; группа В – творческая работа в режиме диалога с ПЭВМ.

При выполнении в течение рабочей смены работ, относящихся к разным видам трудовой деятельности, за основную работу с ПЭВМ следует принимать такую, которая занимает не менее 50 % времени в течение рабочей смены или рабочего дня.

Для предупреждения преждевременной утомляемости пользователей ПЭВМ рекомендуется организовывать рабочую смену путем чередования работ с использованием ПЭВМ и без него.

Таблица 1 – Суммарное время регламентированных перерывов в зависимости от продолжительности работы, вида и категории трудовой деятельности с ПЭВМ

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работ с ПЭВМ			Суммарное время регламентированных перерывов, мин.	
	группа А, количество знаков	группа Б, количество знаков	группа В, ч	при 8-часовой смене	при 12-часовой смене
I	до 20 000	до 15 000	до 2	50	80
II	до 40 000	до 30 000	до 4	70	110
III	до 60 000	до 40 000	до 6	90	140

Когда характер работы требует постоянного взаимодействия с ВДТ (набор текстов или ввод данных и т.п.) с напряжением внимания и сосредоточенности, при исключении возможности периодического переключения на другие виды трудовой деятельности, не связанные с ПЭВМ, рекомендуется организация перерывов на (10-15) минут через каждый час работы.

Продолжительность непрерывной работы с ВДТ без регламентированного перерыва не должна превышать 1 часа.

В Правительстве Амурской области уровень нагрузки за рабочую смену относится к группе А, категории I.

4.1.2 Требования к помещениям для работы с ПЭВМ и организация рабочего места

К помещениям офиса предприятия предъявляются следующие требования.

Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток. Оконные проемы должны быть оборудованы регулируемыми устройствами, например, жалюзи, занавесей, внешних козырьков и др.

Площадь на одно рабочее место пользователей ПК должна составлять не менее 4,5 $м^2$.

Помещения, где размещаются рабочие места с ПК, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.

Не следует размещать рабочие места с ПК вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПК.

Для исследования был взят один из кабинетов Правительства площадью 19 $м^2$ (Рисунок 8) В помещении находится два рабочих места с ПЭВМ, содержащих ЖК-монитор, клавиатуру, принтер и мышь. Данное помещение полностью соответствует требованиям, поскольку на одно рабочее место приходится более 9 $м^2$. Мебель удобная и соответствует всем требованиям. Рабочие места размещены около оконных проёмов, что обеспечивает нормальный уровень естественного освещения. Для поддержания оптимальной температуры воздуха установлен кондиционер.

4.1.3 Требования к микроклимату помещений.

В Правительстве Амурской области, работа с использованием ПК является основной и связана с нервно-эмоциональным напряжением, должны обеспечиваться оптимальные параметры микроклимата для категории работ 1а и 1б в

соответствии с действующими санитарно-эпидемиологическими нормативами. На других рабочих местах следует поддерживать параметры микроклимата на допустимом уровне, соответствующем требованиям указанных выше нормативов.

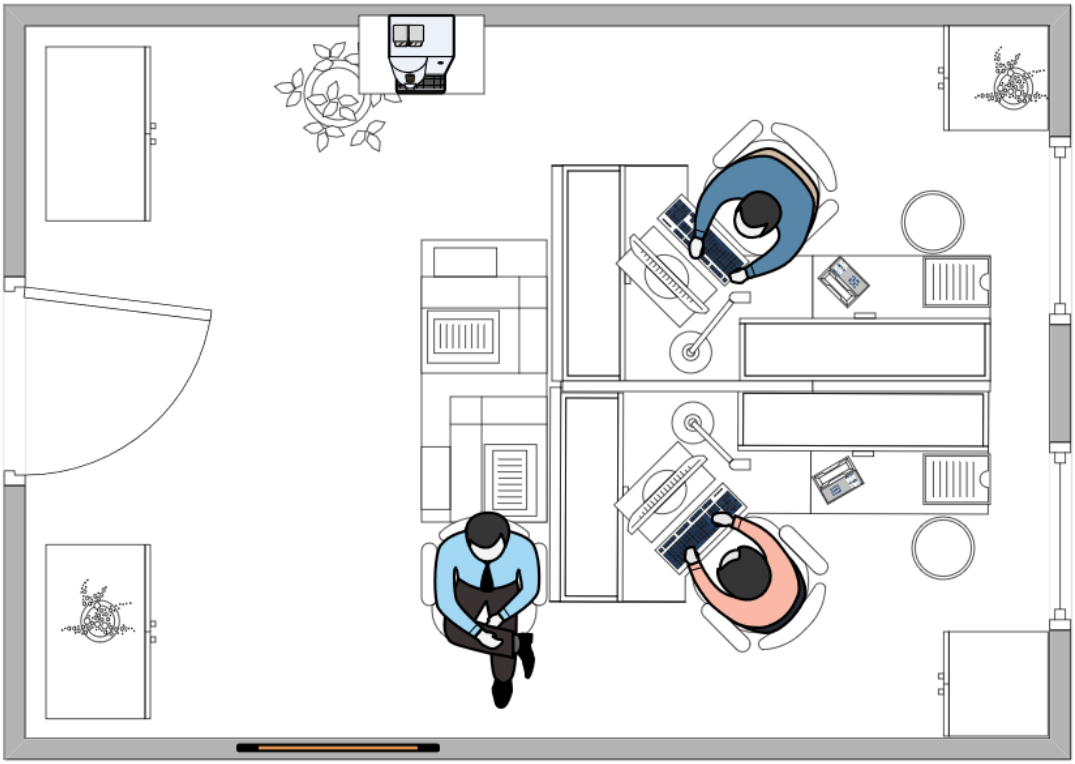

Рисунок 8 – Планировка исследуемого помещения

Содержание вредных химических веществ в офисных помещениях, в которых работа с использованием ПК является основной, не должно превышать предельно допустимых концентраций загрязняющих веществ в атмосферном воздухе населенных мест в соответствии с действующими гигиеническими нормативами.

В Правительстве Амурской области выполняются все вышеперечисленные требования. Также в Правительстве проводятся мероприятия по озеленению в кабинетах и коридорах. Это имеет большое санитарно-гигиеническое и эстетическое значение, т.к. улучшает состав воздуха, снижает температуру в

жаркое время года, повышает влажность. Во всех кабинетах сотрудников предусмотрены кондиционеры.

4.1.4 Требования к уровням шума и вибрации на рабочих местах, оборудованных ПЭВМ.

В производственных помещениях при выполнении основных или вспомогательных работ с использованием ПЭВМ уровни шума на рабочих местах не должны превышать предельно допустимых значений, установленных для данных видов работ в соответствии с действующими нормативами.

При выполнении работ с использованием ПЭВМ в производственных помещениях уровень вибрации не должен превышать допустимых значений вибрации для рабочих мест в соответствии с действующими санитарно-эпидемиологическими нормативами.

Шумящее оборудование (печатающие устройства, серверы и т.п.), уровни шума которого превышают нормативные, должно размещаться вне помещений с ПЭВМ.

Уровень шума и вибраций на предприятии соответствуют стандарту и не превышают нормы.

4.1.5 Освещение помещений

Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В офисных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения.

Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном

расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

В Правительстве Амурской области выполняются все требования к освещению помещений. Каждое рабочее место пользователя дополнительно оснащено настольными лампами. Общее освещение выполнено в виде прерывистой линии светильников, равноудалённо расположенных на потолке в центре каждого кабинета.

4.1.6 Требования к организации рабочих мест пользователей ПЭВМ.

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора) должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м.

Экран видеомонитора должен находиться от глаз пользователя на расстоянии (600-700) мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения от 0,5 до 0,7.

Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

В каждом кабинете Правительстве Амурской области находится от одного до четырёх рабочих мест (в соответствии со стандартами и нормативными актами) и каждое из них имеет необходимое количество оборудования для комфортной работы пользователя.

4.1.7 Организация графического интерфейса

Графический интерфейс разработанного приложения для защиты информации на мониторе ПК для правительства Амурской области разработан по требованиям эргономики программного обеспечения.

Разработанная форма имеет интуитивно понятный минималистичный интерфейс – работа с приложением не вызовет никаких трудностей даже у необученного пользователя.

Интерфейс не противоречит требованиям и в нём нет избыточной информации или кнопок. В окне настроек расположен минимум всех необходимых настроек, которые понятны и пользователю, и администратору, так как нет загромождения, и они вводят только минимальную информацию, необходимую для работы.

Цветовое оформление в пастельных тонах не режет глаз, размер шрифта оптимален для чтения.

4.2 Экологичность

Персональный компьютер, на котором установлена программа, оказывает влияние на окружающую среду. Если, по какой-то причине он выйдет из строя и починить его будет невозможно, то ПК необходимо утилизировать особым образом, так как в его составе находятся вредные вещества.

По законодательству РФ оргтехника должна быть утилизирована специальной организацией с действующей лицензией на работу с отходами разных классов опасности, т.к. простой вывоз к ближайшей свалке запрещен законом.

На предприятии ведется журнал учета количества эксплуатируемых, замененных и утилизированных светильников, мониторов, системных блоков и другой орг. техники. Не работающие приборы и лампы – источник загрязняющих веществ, поэтому должны утилизироваться безопасными способами. В

случае необходимости их утилизации предприятие обращается к компаниям, имеющим лицензию на соответствующий вид работ.

4.3 Чрезвычайные ситуации

Чрезвычайная ситуация (ЧС) – это обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которая может повлечь или повлекла за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери или нарушения условий жизнедеятельности людей.

В офисе предприятия может возникнуть такая чрезвычайная ситуация, как пожар.

Пожар – это неконтролируемый процесс горения вне специального очага, возникший непроизвольно или по злому умыслу, в ходе которого выделяются тепло и дым, а также который сопровождается материальным ущербом и угрожает здоровью или жизни людей. Источниками возгорания могут служить случайные искры различного происхождения, нагретые тела, перегрев электрических контактов и др.

Основные причины пожаров в офисе:

- неисправное электрооборудование;
- плохая подготовка оборудования к ремонту;
- самовозгорание различных материалов;
- несоблюдение правил пожарной безопасности;
- захламление помещений и др.

Для тушения пожара используют огнегасительные вещества, которые при введении в зону сгорания прекращают горение. Основные огнегасящие вещества и материалы – вода и водяной пар, химическая и воздушно-механическая пены, водные растворы солей, негорючие газы, сухие огнетушащие порошки. Наиболее распространенным веществом, применяемым для тушения пожара, является вода. Под первичными средствами пожаротушения понимают передвижные и ручные огнетушители, переносные огнегасительные установки,

внутренние пожарные краны, ящики с песком, асбестовые покрывала, противопожарные щиты с набором инвентаря и др.

В Правительстве Амурской области имеются такие средства пожаротушения, как:

– ручные углекислотные огнетушители;

– система автоматического пожаротушения;

– ящики с песком;

– пожарные датчики и пожарные кнопки;

– схемы путей эвакуации (схема эвакуации находится в начале и в конце каждого коридора).

Все сотрудники регулярно проходят инструктажи по технике пожарной безопасности и правилам эвакуации.

4.4 Техника безопасности для офисных работников

4.4.1 Общие требования безопасности

Офисный работник обязан соблюдать действующие на предприятии правила внутреннего трудового распорядка и графики работы, которыми предусматривается: время начала и окончания работы (смены), перерывы для отдыха и питания, порядок предоставления дней отдыха, чередование смен и другие вопросы использования рабочего времени.

Офисный работник обязан:

– пользоваться исправными выключателями, розетками, вилками, патронами и другой электроарматурой;

– не оставлять без присмотра включенное оборудование и электроприборы, отключать электрическое освещение (кроме аварийного) по окончании работы;

– курить только в специально отведенных и оборудованных местах;

– при использовании в работе горючих и легковоспламеняющихся веществ убирать их в безопасное в пожарном отношении место, не оставлять использованный обтирочный материал в помещении по окончании работы;

– соблюдать действующие Правила противопожарного режима в Российской Федерации.

Офисный работник обязан соблюдать правила личной гигиены:

– приходить на работу в чистой одежде и обуви;

– постоянно следить за чистотой тела, рук, волос;

– мыть руки с мылом после посещения туалета, соприкосновения с загрязненными предметами, по окончании работы.

За нарушение (невыполнение) требований нормативных актов об охране труда офисный работник привлекается к дисциплинарной, а в соответствующих случаях - материальной и уголовной ответственности в порядке, установленном законодательством РФ, локальными нормативными актами.

На рабочем месте офисный работник получает первичный инструктаж по безопасности труда и проходит:

– стажировку;

– обучение устройству и правилам эксплуатации используемого оборудования;

– проверку знаний по электробезопасности (при использовании оборудования, работающего от электрической сети), теоретических знаний и приобретенных навыков безопасных способов работы.

Во время работы офисный работник проходит повторный инструктаж по безопасности труда на рабочем месте - один раз в полгода.

4.4.2 Требования безопасности перед началом работы

Офисный работник обязан подготовить рабочую зону для безопасной работы:

– проверить оснащенность рабочего места;

– проверить путем внешнего осмотра достаточность освещенности и исправность выключателей и розеток;

– осуществить осмотр электрооборудования (проверку комплектности и надежности крепления деталей; проверку путем внешнего осмотра ис-

правности кабеля (шнура); проверку четкости работы выключателя; использовать только штатные приспособления).

Офисный работник обязан доложить руководителю при обнаружении дефектов в электрооборудовании и не эксплуатировать неисправное электрооборудование.

Включение электрооборудования производить вставкой исправной вилки в исправную розетку для бытовых приборов.

Офисный работник во время работы с электрооборудованием обязан поддерживать порядок на рабочем месте.

При работе с электрооборудованием запрещается:

– оставлять включенное электрооборудование без надзора;

– передавать электрооборудование лицам, не имеющим права работать с ним;

– снимать средства защиты;

– дергать за подводящий провод для отключения;

– держать палец на выключателе при переносе электрооборудования;

– натягивать, перекручивать и перегибать подводящий кабель;

– ставить на кабель (шнур) посторонние предметы;

– допускать касание кабеля (шнура) с горячими или теплыми предметами.

Офисный работник обязан выполнять с электрооборудованием только ту работу, для которой предназначено электрооборудование.

Если во время работы обнаружится неисправность электрооборудования или работающий с ним почувствует хотя бы слабое действие тока, работа должна быть немедленно прекращена и неисправное электрооборудование должно быть сдано на проверку или в ремонт.

Отключение электрооборудования необходимо производить:

– при перерыве в работе;

– при окончании рабочего процесса.

4.4.3 Требования безопасности во время работы

Офисный работник должен выполнять только ту работу, по которой прошел обучение, инструктаж по охране труда и к которой допущен работником, ответственным за безопасное выполнение работ.

Не поручать свою работу посторонним лицам.

Во время нахождения на рабочем месте офисный работник не должен совершать действий, которые могут повлечь за собой наступление несчастного случая:

– не качаться на стуле;

– не касаться оголенных проводов;

– не работать на оборудовании мокрыми руками;

– не размахивать острыми и режущими предметами.

Соблюдать правила перемещения в помещении и на территории организации, пользоваться только установленными проходами. Не загромождать установленные проходы и проезды.

Хранить документацию в шкафах в специально оборудованном кабинете.

Вследствие того, что большая часть времени посвящена работе на компьютере, необходимо каждые два часа делать перерыв на 15 минут для снижения утомляемости общефизического характера.

Офисному работнику во время работы запрещается:

– допускать захламленность рабочего места бумагой в целях недопущения накапливания органической пыли;

– производить отключение питания во время выполнения активной задачи;

– производить частые переключения питания;

– включать сильно охлажденное (принесенное с улицы в зимнее время) оборудование;

– производить самостоятельно вскрытие и ремонт оборудования.

4.4.4 Требования безопасности в аварийных ситуациях

В аварийной обстановке следует оповестить об опасности окружающих людей и действовать в соответствии с планом ликвидации аварий.

В случае возникновения возгорания или пожара необходимо немедленно сообщить об этом в пожарную часть, окриком предупредить окружающих людей и принять меры для тушения пожара.

При травмировании, отравлении или внезапном заболевании прекратить работу и обратиться за помощью к медицинскому работнику, а в случае его отсутствия оказать себе или другим пострадавшим первую доврачебную медицинскую помощь и сообщить о случившемся непосредственному руководителю, далее действовать по его указанию.

В ситуациях, угрожающих жизни и здоровью, покинуть опасный участок.

4.4.5 Требования безопасности по окончании работы

По окончании работы офисный работник должен произвести уборку рабочего места.

Офисный работник должен:

– отключить электрооборудование;
– проверить противопожарное состояние кабинета;
– закрыть окна, выключить свет, закрыть двери.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы был проведен анализ предметной области, построена организационная структура Правительства Амурской области, построены диаграммы внешнего и внутреннего документооборота.

Приведено описание программных модулей, выбраны средства разработки, разработана модель нарушителя, а также политики безопасности.

Проведен анализ безопасности и экологичности предприятия и разработанного продукта.

Главным результатом выполнения работы стал программный продукт, разработанный в PyCharm на языке Python для Правительства Амурской области.

Созданное приложение «Faseblock» позволяет защитить данные на экране монитора пользователя от несанкционированного доступа к ним, что позволяет безопасней работать с информацией различной степени секретности.

Таким образом, можно считать, что цель работы достигнута, и поставленные задачи решены.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Безопасность жизнедеятельности. Учебник для бакалавров / Э. А. Арустамов [и др.]; под ред. Э. А. Арустамова. – 21-е изд. – М.: Дашков и К, 2018. – 446 с.

2 Безопасность жизнедеятельности. Учебное пособие / Г. В. Тягунов [и др.]; под ред. В.С. Цепелева. – Екатеринбург: Уральский федеральный университет, 2016. – 236 с.

3 Безопасность жизнедеятельности. Учебное пособие / Л. А. Муравей [и др.]; под ред. Л. А. Муравья. – 2-е изд. – М.: ЮНИТИ-ДАНА, 2017. – 431 с.

4 Васильев, А.Н. Python на примерах. Практический курс по программированию. – М.: Наука и техника, 2016. – 432 с.

5 Волкова, А.А. Безопасность жизнедеятельности в примерах и задачах: учеб. пособие / А.А. Волкова, В.Г. Шишкунов, А.О. Хоменко, Г.В. Тягунов; под общ. ред. канд. техн. наук, доц. А.О. Хоменко. — Екатеринбург: Изд-во Урал. ун-та, - 2018. - 120 с.

6 Кардаш, Т. А. Эргономика рабочих мест служащих и инженерно-технических работников, оснащенных ПЭВМ. Учебное пособие / Т. А. Кардаш. – Благовещенск: Изд-во Амур. гос. ун-та, 2018. – 60 с.

7 Кармановский, Н.С. Организационно- правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2019. − 148 с.

8 Методологии функционального моделирования. Диаграммы потоков данных (DFD) и методология IDEF0 [Электронный ресурс] – Режим доступа: http://www.mstu.edu.ru/study/materials/zelenkov/ch_5_3.html. – 02.03.2021.

9 О персональных данных [Электронный ресурс]: федеральный закон: [принят Государственной Думой 8 июля 2006 г.: одобрено Советом Федерации 14 июля 2006 г.]. – Режим доступа: http://www.consultant.ru/document/Cons_doc_LAW_61801/ − 25.05.2022.

Оформление выпускных квалификационных и курсовых работ (проектов) [Текст] стандарт Амур. Гос. ун-та / АмГУ; АмГУ. – Благовещенск: Изд-во Амур. Гос. ун-та, 2018. – 75. Прилож.: с.50-71

10 Порядок утилизации старой оргтехники на предприятии [Электронный ресурс] – Режим доступа: https://stop-othod.ru/recycling/utilizaciya-orgtekhniki.html – 12.06.2022.

11 СанПиН 1.2.3685-21. Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания. – Введ. 2021-28-01. – М: Минюст России, 2021. – 469 с.

12 Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации [Электронный ресурс]:Утверждены приказом ФСТЭК России от 25 декабря 2017 г. N 239 – Режим доступа: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 − 25.05.2022.

13 Трещев, И.А. О классификации угроз безопасности конфиденциальной информации предприятия // Мир Науки №3, 2018. − 6 с.

14 Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. − М.: ИД «ФОРУМ»: ИНФРА-М, 2019. − 416 с.

15 Шумилин, В. К. Пособие по безопасной работе на персональных компьютерах / В. К. Шумилин. – М.: НЦ ЭНАС, 2015. – 28 с.

16 Эргономика программного обеспечения [Электронный ресурс] – Режим доступа: https://studwood.net/1589590/informatika/ergonomika_programmnogo _obespecheniya. – 13.06.2022.

17 Ян Эрик Солем. Программирование компьютерного зрения на Python. – М.: ДМК Пресс, 2016. – 312 с.

18 digital.amurobl.ru: Министерство Цифрового развития [Электронный ресурс] – Режим доступа: https://digital.amurobl.ru/ -24.06.2022

19 fstec.ru: Дальневосточный федеральный округ ФСТЭК России [Электронный ресурс] – Режим доступа: https://fstec.ru/territorialnye-organy/dalnevostochnyj-federalnyj-okrug -25.05.2021

20 Hough P. V. C.Hough P. V. C. Methods, Means for Recognizing Complex Patterns / U.S., Patent 3069654, 1962. [188]

21 moodle.kstu.ru: Основные понятия делопроизводства и документооборота [Электронный ресурс] – Режим доступа: https://moodle.kstu.ru/mod/book/tool/print/index.php?id=16664 -27.05.2022

ПРИЛОЖЕНИЕ А
Техническое задание на проектирование

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование приложения

Приложение для защиты данных от несанкционированного доступа «Faseblock» для Правительства Амурской области.

1.2 Область применения

Информационные системы Правительства Амурской области

1.3 Наименование предприятий разработчика и заказчика системы

Разработчик: студент группы 855-об, факультета математики и информатики, Амурского государственного университета Барсук Алёна Алексеевна.

Заказчик: Правительство Амурской области

Фактический адрес: 675000, Амурская область, г. Благовещенск, ул. Ленина 135

1.4 Перечень документов

Документы, на основании которых создается МИС предприятия:

– ГОСТ 34.601-90 – техническое задание на проектирование автоматизированной системы управления;

– ГОСТ 19.201-78 – техническое задание.

1.5 Плановые сроки начала и окончания работы

Срок начала работ: - 01.01.2022

Срок окончания работ: - 01.10.2022

1.6 Сведения об источниках и порядке финансирования работ

Данный проект является учебным и выполняется без привлечения каких-либо финансовых средств.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение системы

ПРОДОЛЖЕНИЕ ПРИЛОЖЕНИЯ А

Разрабатываемое приложение предназначено для защиты данных разной степени секретности, а также персональных данных на экране компьютера.

2.2. Цели создания системы

Целью разработки является защита данных на персональном компьютере от несанкционированного доступа к ним.

3 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ПРОДУКТУ

3.1 Требования к приложению

3.1.1 Требования к структуре и функционированию

В приложении можно выделить следующие функции:

Возможность регистрации пользователя.

Возможность распознавания лица пользователя и лица нарушителя.

Возможность блокировки экрана после окончания действия таймера.

Возможность выбора картинки для экрана блокировки.

3.1.2 Требования к графическому дизайну приложения

Все элементы интерфейса должны быть четко различимы и выполнены в одной цветовой гамме для наилучшего восприятия.

3.1.3. Требования к квалификации и численности персонала, режиму его работы

Для обеспечения работы приложения нужно два пользователя. Предположительно – пользователь, который будет работать с самим приложением и администратор (уполномоченное лицо), который будет отвечать за выдачу и периодическую смену пароля.

Система должна содержать идентификацию пользователя.

Надежное хранение данных;

Система должна обладать таким свойством, как предотвращение некорректных данных.

ПРОДОЛЖЕНИЕ ПРИЛОЖЕНИЯ А

3.1.5 Требования к интерфейсу пользователя

Система должна иметь человеко-машинный интерфейс, удовлетворяющий следующим требованиям:

– взаимодействие системы и пользователя должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;

– допустима видимость предоставляемой информации на экране;

– допустимая цветопередача.

3.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению.

Пользователи обязаны быть проинформированы о правилах использования технических средств и работы с программой и с оборудованием, на котором используется данная программа.

Устройство хранения должно быть защищено от внешних физических воздействий, в качестве переноса и хранения может быть любой диск для хранения данных.

3.2 Требования к видам обеспечения

3.2.1 Требования к информационному обеспечению и программной документации.

Данные, обрабатываемые в приложении, должны храниться во внутренней памяти компьютера.

Состав программной документации, предъявляемой на испытании:

- ГОСТ 19.402-78 – описание программы;

- ГОСТ 19.301-79 – программа и методика испытаний;

- ГОСТ 19.401-78 – тестирование программы.

3.2.2 Требования к лингвистическому обеспечению

Для создания данной программы необходимы знания языка программи-

рования Python.

3.2.3 Требования к программному обеспечению

Для реализации и эксплуатации симулятора пользователь должен иметь установленную операционную систему Windows 7/8/8.1/10 или Ubuntu.

3.2.4 Требования к техническому обеспечению

Минимальные требования для работы на персональных компьютерах, имеющих следующие минимальные характеристики:

– тактовая частота процессора – 2.1 ГГц;
– ОЗУ - 512 Мб или более;
– объем жесткого диска должен быть не менее 500 Гбайт;

К дополнительным требованиям относятся:

– устройство ввода информации: клавиатура, мышь;
– монитор;
– устройство для работы с USB Flash носителями;
– устройство захвата и записи видео.

4 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Этапы, которые необходимо выполнить по созданию приложения:

1 этап – Изучение предметной области, анализ процессов деятельности организации. В конце этого этапа будут разработаны диаграммы внешнего и внутреннего документооборота;

2 этап – анализ защищенности предприятия, на основании которого будет вестись разработка безопасности приложения.

2 этап – Разработка программного продукта с использованием языка Python.

3 этап – Программная реализация приложения

4 этап – Согласование программной реализации образовательного прило-

жения с требованиями заказчика с учетом всех замечаний и пожеланий.

5 этап – Внедрение и сопровождение приложения: установка и настройка программного средства, обучение пользователей работе с приложением, выявление и устранение неполадок.

5 ТРЕБОВАНИЯ К ПРИЕМКЕ-СДАЧЕ ПРОЕКТА

В рамках работ по данному проекту исполнитель разрабатывает приложение, необходимое заказчику.

Приемка готового программного продукта в соответствии со следующим планом:

1 этап – анализ готового проекта;

2 этап – сравнение готового проекта с техническим заданием для определения степени соответствия поставленным задачам и требованиям;

3 этап – внесение коррективов и дополнений в систему по результатам предыдущих этапов;

4 этап – составление списка преимуществ и недостатков разработанного программного продукта.

6 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

Перед вводом в эксплуатацию готового симулятора разработчик должен договорится с руководителем организации о временном промежутке, в течение которого он обязан внедрить разработанный программный продукт. Под внедрением понимается комплекс мероприятий, включающий обучение персонала (пользователь и администратор), настройку системы для дальнейшего использования, предоставление им необходимой документации для системы, ознакомление инструктора с его обязанностями.

ПРОДОЛЖЕНИЕ ПРИЛОЖЕНИЯ А

7 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

При вводе программы в эксплуатацию пакет сопроводительных документов должен включать:

– техническое задание;

– описание программного продукта;

– руководство пользователя;

8 ПОРЯДОК ПЕРЕНОСА СИМУЛЯТОРА НА ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАКАЗЧИКА

После завершения сдачи-приемки программы, в рамках гарантийной поддержки исполнителем производится однократный перенос разработанного программного обеспечения на аппаратные средства Заказчика.

ПРИЛОЖЕНИЕ Б

Блок-схема алгоритма работы программного продукта