Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Кибернетики
Направление подготовки 09.04.01 Информатика и вычислительная техника
Кафедра Автоматики и Компьютерных Систем

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Использование средств биометрической идентификации для доступа к КИС

УДК 004.056.523:57.087.1

Студент

Группа	ФИО	Подпись	Дата
8ВМ5Г	Шипицина Варвара Павловна		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент кафедры АиКС	Пономарев А.А.	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент кафедры менеджмента	Конотопский В.Ю.	к.э.н		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент кафедры ЭБЖ	Извеков В. Н.	к.т.н.		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
АиКС	Суходоев М.С.	к.т.н.		

Томск – 2017 г.

Планируемые результаты обучения

Код результата	Результат обучения (выпускник должен быть готов)
	Общепрофессиональные компетенции
Р1	Воспринимать и самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.
Р2	Владеть и применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.
Р3	Демонстрировать культуру мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных, анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.
Р4	Анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности. Владеть, по крайней мере, одним из иностранных языков на уровне социального и профессионального общения, применять специальную лексику и профессиональную терминологию языка.
	Профессиональные компетенции
Р5	Выполнять инновационные инженерные проекты по разработке аппаратных и программных средств автоматизированных систем различного назначения с использованием современных методов проектирования, систем автоматизированного проектирования, передового опыта разработки конкурентно способных изделий.
Р6	Планировать и проводить теоретические и экспериментальные исследования в

Код результата	Результат обучения (выпускник должен быть готов)
	области проектирования аппаратных и программных средств автоматизированных систем с использованием новейших достижений науки и техники, передового отечественного и зарубежного опыта. Критически оценивать полученные данные и делать выводы.
Р7	Осуществлять авторское сопровождение процессов проектирования, внедрения и эксплуатации аппаратных и программных средств автоматизированных систем различного назначения.
	Общекультурные компетенции
Р8	Использовать на практике умения и навыки в организации исследовательских, проектных работ и профессиональной эксплуатации современного оборудования и приборов, в управлении коллективом.
Р9	Осуществлять коммуникации в профессиональной среде и в обществе в целом, активно владеть иностранным языком, разрабатывать документацию, презентовать и защищать результаты инновационной инженерной деятельности, в том числе на иностранном языке.
Р10	Совершенствовать и развивать свой интеллектуальный и общекультурный уровень. Проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности.
Р11	Демонстрировать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности, способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, способность к педагогической деятельности.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки (специальность) 09.04.01 Информатика и вычислительная техника
Кафедра Автоматики и Компьютерных Систем

УТВЕРЖДАЮ:

Зав. кафедрой

_____ _____ _____

(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

магистерской диссертации

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	**ФИО**
8ВМ5Г	Шипицина Варвара Павловна

Тема работы:

Использование средств биометрической идентификации для доступа к КИС	
Утверждена приказом директора (дата, номер)	

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе *(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).*	

Перечень подлежащих исследованию, проектированию и разработке вопросов *(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).*	— Обзор литературы — Объект и методы исследования; — Расчеты и аналитика; — Результаты проведенного исследования; — Финансовый менеджмент, ресурсоэффективность и ресурсосбережение; — Социальная ответственность; — Заключение по работе.
Перечень графического материала *(с точным указанием обязательных чертежей)*	

Консультанты по разделам выпускной квалификационной работы

(с указанием разделов)

Раздел	Консультант
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Конотопский Владимир Юрьевич
Социальная ответственность	Извеков Владимир Николаевич

Названия разделов, которые должны быть написаны на русском и иностранном языках:

Обзор литературы

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент кафедры АиКС	Пономарев Алексей Анатольевич	к.т.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ5Г	Шипицина Варвара Павловна		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8ВМ5Г	Шипицина Варвара Павловна

Институт	**Кибернетики**	**Кафедра**	**Автоматики и компьютерных систем**
Уровень образования	Магистр	**Направление/специальность**	09.04.01 Информатика и вычислительная техника

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих*	
2. *Нормы и нормативы расходования ресурсов*	
3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого потенциала, перспективности и альтернатив проведения НИ с позиции ресурсоэффективности и ресурсосбережения*	
2. *Планирование и формирование бюджета научных исследований*	
3. *Определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования*	
Перечень графического материала *(с точным указанием обязательных чертежей)***:**	
1. *Оценка конкурентоспособности технических решений* 2. *Альтернативы проведения НИ* 3. *График проведения и бюджет НИ* 4. *Оценка ресурсной, финансовой и экономической эффективности НИ*	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Конотопский В.Ю.	к.э.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ5Г	Шипицина Варвара Павловна		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	**ФИО**
8ВМ5Г	Шипицина Варвара Павловна

Институт	Кибернетики	**Кафедра**	ОСУ
Уровень образования	Магистр	**Направление/специальность**	09.04.01 Информатика и вычислительная техника

Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения	*В данной работе рассматривается возможность доработки системы мониторинга состояния здоровья «ЮМС Диагностический шлюз» в плане измерения температуры.*
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Производственная безопасность 1.1. Анализ выявленных вредных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности. 1.2. Анализ выявленных опасных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности. 1.3. Рекомендации по минимизации влияний	*В качестве вредных факторов выделены: шум и электромагнитное излучение. В качестве опасных: возможность поражения током и возникновение пожара, электромагнитного излучения. Приведены рекомендации по улучшению микроклимата в офисном помещении, а также рекомендации по минимизации влияния шума, электромагнитного излучения и освещения, меры по обеспечению пожарной безопасности, способы защиты отиэлектричекого тока.*
2. Экологическая безопасность:	*Деятельность организации не связана с производством, поэтому влияние на окружающую среду минимально. Рассмотрена утилизация бумажных отходов.*
3. Безопасность в чрезвычайных ситуациях:	*Наиболее типичной ЧС в офисном помещении является возникновение пожара. При хранении конфиденциальных данных в электронных таблицах можно говорить о возможности возникновения кибертерроризма. Приведены способы защиты от кибератак.*
4. Правовые и организационные вопросы обеспечения безопасности:	*Рассмотрены психофизиологические факторы, организационные мероприятия при компоновке рабочей зоны, обеспечение гарантий защиты конфиденциальных данных граждан с помощью комплекса технических и юридических мер.*

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент	Извеков Владимир Николаевич	к.т.н		

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
8ВМ5Г	Шипицина Варвара Павловна		

РЕФЕРАТ

Выпускная квалификационная работа 112 с., 18 рис., 22 табл., 50 источников, 3 прил.

Ключевые слова: биометрия, отпечатки пальцев.

Объектом исследования является разработка алгоритма для идентификации сотрудников в корпоративной информационной системе прохождения предсменного или послесменного осмотра с использованием системы мониторинга состояния здоровья «ЮМС Диагностический шлюз».

Цель работы – разработать алгоритм идентификации сотрудников в КИС.

В процессе исследования проводились:

1) Обзор аппаратного обеспечения;

2) Выбрано аппаратное обеспечение для решения задачи идентификации;

3) Рассмотрена существующая архитектура программно-аппаратного комплекса.

В результате исследования было выполнено:

1) Подготовлено решение по интеграции;

2) Разработано программное обеспечение обеспечивающее исполнение предложенного способа на АРМ и ПАК, представленных оконным приложением реализованного с применением технологии WPF и веб-решением реализованное с применением фреймворка ASP.Net MVC соответственно;

3) Подготовлено предложение по изменению бизнес-процесса по прохождению медицинских осмотров;

4) Выполнена работа по тестированию и отладке.

Основные конструктивные, технологические и технико-эксплуатационные характеристики: программа разработана на языке программирования C# для платформы WPF и ASP MVC, имеет модульную структуру. Предназначена для работы под управлением ОС Windows 10.

Степень внедрения: разработанный алгоритм внедрен в итоговую сборку программного обеспечения «ЮМС Диагностический шлюз».

Область применения: идентификация сотрудников для прохождения предсменного или послесменного осмотра.

Экономическую эффективность работы вычислить затруднительно, эффект косвенный.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ, НОРМАТИВНЫЕ ССЫЛКИ

В данной работе применены следующие термины с соответствующими определениями:

Биометрические системы аутентификации — системы аутентификации, применяемые для идентификации личности человека по биометрическим данным.

Биометрическая аутентификация — процесс подтверждения пользователя путей проверки биометрического образа посредствам применения методов и протоколов индентификации.

Папилярный узор – рельефные линии на ладонных и подошвенных поверхностях пальцев человека.

Минуации – пункты определяющие изменения линии паппилярных узоров.

Глобальные признаки — признаки, которые можно увидеть невооружённым глазом.

Сегментация — это процесс разделения цифрового изображения на несколько сегментов.

В данной работе применены следующие сокращения:

FAR — коэффициент ложного пропуска, вероятность ложной идентификации, то есть вероятность того, что система биоидентификации по ошибке признает подлинность (например, по отпечатку пальца) пользователя, не зарегистрированного в системе.

FMR — вероятность, что система неверно сравнивает входной образец с несоответствующим шаблоном в базе данных.

АРМ – автоматизированное рабочее место.

ДИ – Дактилоскопическое изображение.

КИС – корпоративная информационная система.

ОП – отпечаток пальца.

ПАК – программно-аппаратный комплекс.

ПДн – Персональные данные.

ЭЦП – электронно-цифровая подпись.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

С введением в действие Федерального закона 152-ФЗ (ред. от 03.07.2016) "О персональных данных" все большее внимание разработчиков занимают вопросы организации программных средств защиты данных и организации доступа к ним. В работе рассматриваются возможности современного оборудования для организации доступа к корпоративной информационной системе (КИС) с использованием биометрических данных.

Задачами данной магистерской диссертации являются:

— изучение типов биометрических параметров;

— изучение способов идентификации с применением отпечатков пальцев;

— рассмотрение достоинств и недостатков применения отпечатков при идентификации сотрудников;

— формирование предложений о внесении изменений в бизнес-процесс прохождения осмотра;

— внедрение нового способа идентификации по биометрическим параметрам.

Актуальность темы заключается в том, что на сегодняшний день кибербезопасность является основной задачей любой Компании являющейся оператором ПДн.

Аутентификация в любой КИС требует наличия идентификационных параметров.

Такие способы идентификации как логин/пароли, использование ЭЦП, карт доступа может быть сфальсифицирован. Применение биометрических параметров для идентификации человека снижает возможность подлога и кражи личности, т.к. биометрические параметры человека являются индивидуальными.

Основываясь на ФЗ 152 оператор ПДн обязан обеспечить безопасность располагаемых ПДн.

Объектом исследования является процесс сканирования, сохранения и распознавания отпечатка пальца человека.

Предметом является разработка алгоритма идентификации сотрудников в КИС.

1 ОБЗОР ЛИТЕРАТУРЫ

1.1 Биометрическая аутентификация

Актуальность вопросов биометрической аутентификации возрастает с каждым днём. Ежедневно ведётся разработка новых информационных систем, данные содержащиеся в которых требуют защиты. В связи с динамическим ростом рынка IT возрастает вопрос кибербезопасности и обеспечения доступа. Применение средств биометрической идентификации способствует повышению уровня безопасности, поскольку биометрические параметры являются уникальными для каждого человека, поэтому применение подобных средств защиты являются более безопасным чем системы использующие пароли.

Существующие методы аутентификации по биометрическим параметрам делятся на два основных класса:

— статические;

— динамические.

Статистические методы основываются на характеристиках присутствующих от рождения и до самой смерти. Данные характеристики нельзя украсть, передать или потерять, они неизменны на протяжении всей жизни человека.

Динамические методы основываются на поведенческих характеристиках человека, то есть основаны на характерных для подсознательных движений в процессе воспроизведения или повторения какого-либо обыденного действия [2].

Критерии для биометрических параметров. Они обязаны соответствовать следующим пунктам [3]:

1) всеобщность: данный признак должен присутствовать у всех людей без исключения;

2) уникальность: биометрия отрицает существование двух людей с одинаковыми физическими и поведенческими параметрами;

3) постоянство: для корректной аутентификации необходимо постоянство во времени;

4) измеряемость: специалисты должны иметь возможность измерить признак каким-либо устройством для дальнейшего занесения в базу данных;

5) приемлемость: общество не должно быть против сбора и измерения биометрического параметра.

1.2 Типы биометрических параметров, применяемых для аутентификации

1.2.1 Метод аутентификации по отпечатку пальца

Самой распространённой биометрической технологией аутентификации пользователей является идентификация по отпечатку пальца.

Основой метода является использование уникального рисунка папиллярных узоров на пальцах людей. Сканер считывает папиллярный узор, преобразует его в цифровую модель и затем производит сравнение с ранее введённым рисунком отпечатка, который принято считать эталонным.

Основным преимуществом данного метода является лёгкость в применении и внедрении.

Так же стоит отметить универсальность данного метода, заключающуюся в возможности применения метода в решении задач идентификации любого уровня и любого рода деятельности.

Отпечаток пальца можно получить, применяя сканер отпечатков пальцев. В связи с тем, что отпечаток пальца достаточно мал, необходимо применение узконаправленных методов.

Все сканеры отпечатков пальцев можно разделить на 3 основных типа:

— ёмкостные;

— прокатные;

— оптические.

Самыми распространёнными являются оптические сканеры.

По физическим принципам сканеры отпечатков пальцев можно разделить на 3 класса:

— оптические;

— кремниевые;

— ультразвуковые [3].

В отпечатке выделяются 2 типа признаков – глобальные и локальные.

Локальные признаки — признаки описывающие точки изменения структуры линий папиллярного узора (окончание, раздвоение, разрыв и т. д.).

Папиллярный узор состоит из:

— область узора – область отпечатка пальца, содержащая все глобальные признаки;

— ядро (центр) – участок середины отпечатка или области рисунка;

— дельта – начальная точка соединения или разветвления линий папиллярного узора или короткая линия, вырожденная в точку;

— тип линии – начинающиеся как параллельные две линии огибающие всю область отпечатка;

— счётчик линий – число линий между ядром и дельтой и областью образа.

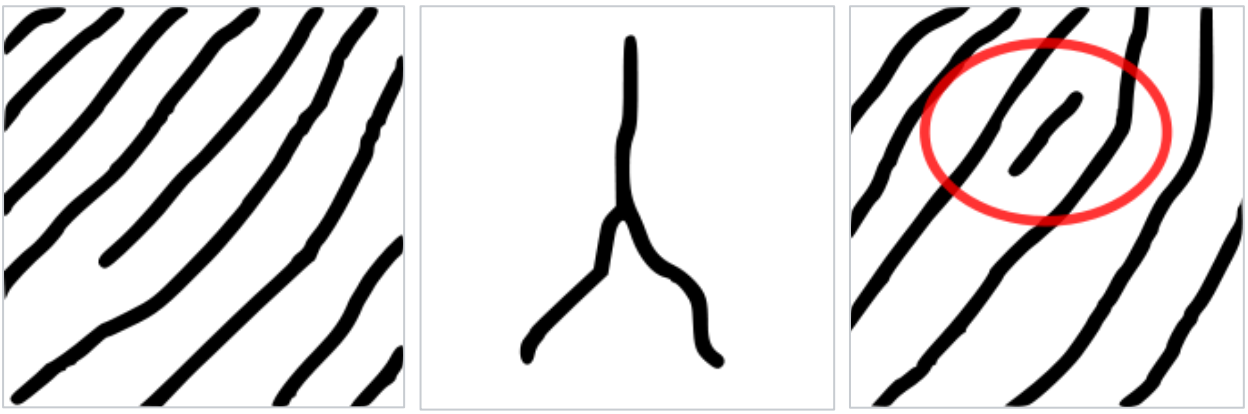


Рисунок 1 – Типы минуаций слева направо (окончание, разветвление, островок)

Основные типы папиллярных узоров:

— петля;

— дельта или дуга;

— спираль.

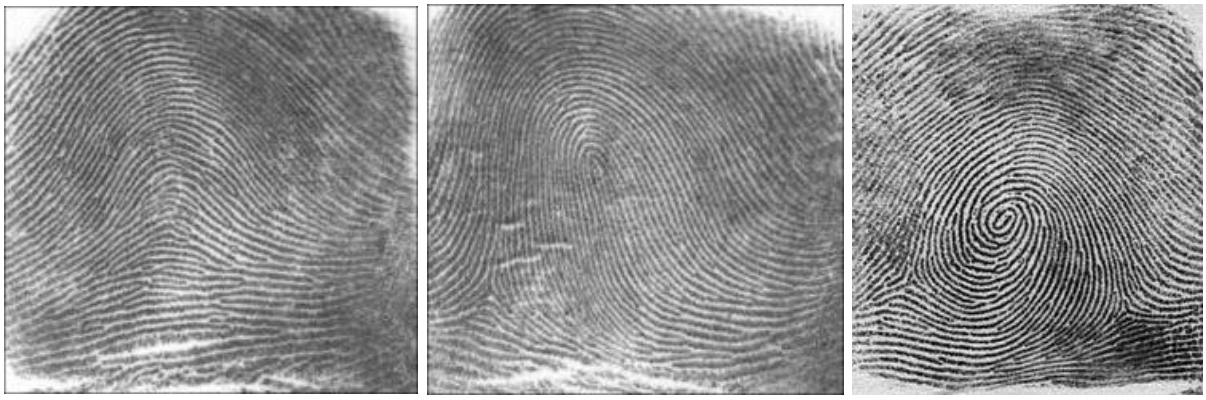


Рисунок 2 – Типы папиллярных узоров (арка, петля, завиток)

Практика показывает, что отпечатки пальцев разных людей могут иметь одинаковые глобальные признаки, но совершенно невозможно наличие одинаковых микроузоров минуций. Поэтому глобальные признаки используют для разделения базы данных на классы и на этапе аутентификации. На втором этапе распознавания используют уже локальные признаки.

1.2.2Стандарты на отпечатки пальцев в России

В России биометрические стандарты регламентируются по ГОСТ Р ИСО/МЭК 19794-4-2006 [4].

Изображение отпечатка пальцев должно быть представлено в виде точек либо квадратных областей одинаковой высоты и ширины.

На рисунке отпечатка пальца чёрному цвету соответствуют минимальный уровень яркости равный нулю, максимальный уровень яркости соответствует белому цвету и уровень яркости равняется единице. Полутона соответствуют серому цвету обеспечивает 256 уровней градации серого.

В записи должна содержаться информация о точках исходного изображения. На кодирование каждой точки отводится один байт, значения серых точек должны храниться в двоичном коде.

Разрешение полученного со сканера изображения должно совпадать с изображением, полученным со сканера. Разрешение изображения может быть изменено, но должно сохранят исходную структуру отпечатка.

Для наибольшей эффективности получения отпечатка пальца необходимо располагать отпечаток в центре окна сканера. Для получения изображения четырех пальцев необходимо располагать половину пальцев слева от центра, а вторую половину справа.

1.2.3 Метод аутентификации по радужной оболочке глаза

Радужная оболочка представляет собой тонкую подвижную диафрагму со ответвим в центре. Располагается за роговицей, перед хрусталиком между передней и задней камерами глаз. Радужная оболочка не меняется на протяжении всей жизни человека. По текстуре она похожа на сеть с большим количеством рисунков и кругов. Рисунок радужной оболочки может быть обработан компьютером и на ней могут выделяться порядка 200 точек, применяемых в процессе идентификации [5].

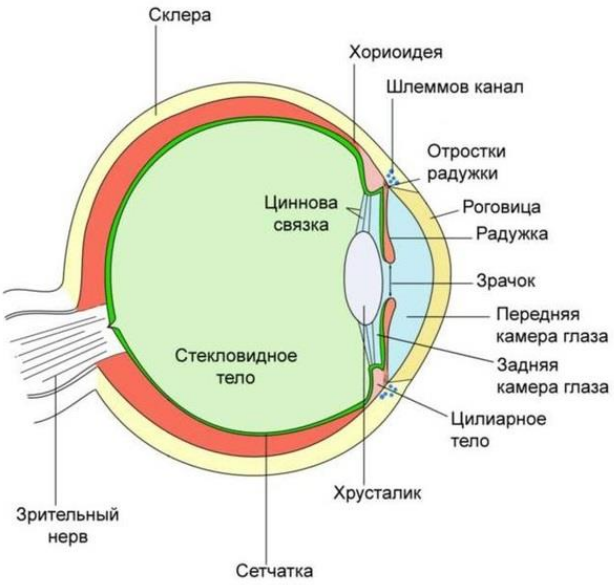


Рисунок 3 – Строение человеческого глаза

Радужная оболочка состоит из трабекулярной сети. Это эластична материя, представленная в виде сетчатого образования состоящая из углублений, гребенчатых стяжек, борозд, колец, морщин, веснушек, сосудов и других черт. Совокупность этих признаков образует радужную оболочку, благодаря этому рисунок на радужной оболочке получается уникальным [6].

Узор траберкулярной сети остаётся неизменным в течение всей жизни человека, изменение цвета глаз не влияет на строение траберкулярной сети.

Узор траберкулярной сети может быть изменен путем хирургического вмешательства [6].

Метод идентификации с применением радужной оболочке глаза можно разделить на 3 основных этапа:

— получение изображения глаза человека;

— сегментация;

— выделение контрольной области.

В итоге получается шаблон радужной оболочки глаза, который применяется для дальнейшей идентификации[7].

В ходе аутентификации имеющийся шаблон побитово сравнивается с новым шаблоном. Мерой, с помощью которой определяется степень различия двух радужных оболочек, является расстояние Хэмминга [8].

1.2.4 Метод аутентификации по сетчатке глаза

Сетчатка – внутренняя оболочка глазного яблока, воспринимающая свет. Сетчатка является периферическим отделом зрительного анализатора; содержит фоторецепторные клетки, обеспечивающие восприятие и преобразование электромагнитного излучения видимой части спектра в нервные импульсы, а также обеспечивает их первичную обработку образов.

Сетчатка глаза у взрослого человека покрывает около 72 % площади внутренней поверхности глазного яблока и имеет диаметральный размер 22 мм [9].

Толщина сетчатки неодинакова, самый толстый участок составляет не более 0,5мм.

Для получения изображения сетчатки глаза используются сканеры, основанные на инфракрасном излучении низкой интенсивности. Луч сканера направляется через зрачок к кровеносным сосудам на задней стенке глаза. Полученный сигнал преобразуется в цифровой шаблон.

Недостатком данного метода является высокие требования к качеству изображения [9].

1.2.5Метод аутентификации по геометрии руки

В данном методе для идентификации используются параметры форма кисти руки.

Не все параметры руки являются уникальными, поэтому требуется использовать дополнительных характеристик таких как как изгибы пальцев, их

длина и толщина, ширина и толщина тыльной стороны руки, расстояние между суставами и структура кости, морщины на коже.

Сканер в данном случает состоит из камеры и подсвечивающих диодов, на основе полученных снимков строится трехмерная модель [2].

Основным из недостатков метода является, то что рука может подвергаться изменению, травмам, заболеваем суставов.

1.2.6Метод аутентификации по геометрии лица

Метод идентификации по геометрии лица получил обширное использование поскольку изображения полученного с камеры видеонаблюдения достаточно для построения трехмерной модели человеческого лица. При построении модели выделяют контуры глаз, бровей, губ, носа, и других различных элементов лица, затем вычисляют расстояние между ними. Требуется выделить 12-40 характерных элементов, соответствующих одному человеку.

Недостатком является потребность решения сложной математической задачи по сравнению новой и имеющейся модели [2].

1.2.7Метод аутентификации по голосу

Метод основан на создании шаблона с применением комбинации частотных и статических характеристик голоса, также могут рассматриваться такие характеристики как интонация, высота тона и т.д.

Для реализации метода достаточно иметь микрофон.

Основным недостатком является низкая точность метода. При возрастном изменении голоса или изменения тона и тембра голоса, наличии шума метод может не давать ожидаемый результат [9].

1.2.8Метод аутентификации по рукописному почерку

Шаблон для метода формируется на основе подписи выполняемой специальным пером.

Метод может применяться в двух вариация.

Анализ подписи и сверки, существующий подписи и полученной.

Анализ дополнительных характеристик таких как нажатие на перо, скорость и т.д. [10]

2 ОБЪЕКТЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

2.1 Способы аутентификации с применением отпечатков

2.1.1Способы аутентификации с применением отпечатков

Идентификация по отпечаткам пальцев наиболее распространенная на сегодняшний день технология, применяемая в биометрических системах контроля доступа. В основе технологии - уникальность рисунка папиллярных узоров на пальцах людей [11].

После получения отпечатка его папиллярный узор преобразовывается в цифровой код, который и хранится в базе данных, а затем сравнивается с ранее введенными и преобразованными «кодами отпечатков пальцев».

Преимущества биометрического контроля доступа по отпечаткам пальцев - легкость в использовании, удобство и надежность, высокая достоверность и низкая стоимость устройств, сканирующих изображение отпечатка пальца.

Среди недостатков: нарушение папиллярного узора мелкими царапинами, порезами, химическими реактивами; невозможность считывания отпечатка некоторыми сканерами при чрезмерно сухой коже.

Среднее значение показателя FAR контроля доступа по отпечаткам пальцев – 0.001%. Стабильная работа системы идентификации при FAR=0.001% возможна при численности персонала N≈300.

На сегодняшний день системы идентификации по отпечаткам пальцев составляют более половины рынка биометрии.

2.1.2Методы аутентификации по отпечаткам пальцев

Технология Match-on-Host является отраслевым стандартом. Система состоит из датчика отпечатков пальцев, считывающего биометрические данные с отправкой на центральный внешний процессор. Вся обработка и поиск совпадающих отпечатков осуществляется на внешнем сервере.

Такая система аутентификации по отпечаткам пальцев доступна, экономична, может быть довольно просто и быстро интегрирована в любую уже существующую СКУД.

Популярность Match-on-Host технологии привела к инновациям в смежных областях, таких как Fast Identity Online (FIDO) сформированной Universal Authentication Framework (UAF).

Технология Match-in-Sensor имеет архитектуру, замкнутую на самом чипе (system-on-a-chip или SoC). Считывание отпечатка пальца и вся последующая обработка биометрических данных осуществляется непосредственно в IC-датчике. Такая архитектура является более безопасной, ведь шаблоны посещаемости зашифрованы и подписаны с помощью датчика, а вся информация хранится в частной флэш-памяти.

В докладе Electronic Design, Synaptics' VP of marketing Anthony Gioeli делается однозначный выбор в пользу последнего метода аутентификации по отпечаткам пальцев, поскольку такая замкнутая система становится гораздо менее доступной для взлома и кражи хакерами уникальной информации о биометрических данных пользователя [12].

2.1.3Стандартизация шаблонов для аутентификации по отпечатку пальца

Существование стандартного шаблона отпечатка пальца INCITS 378 дает возможность разработки полностью совместимых приложений, позволяющих осуществлять быстрый и точный обмен компактными биометрическими шаблонами и последующую обработку данных. На практике, биометрические данные, сгенерированные различными производителями могут, обрабатываться с меньшей скоростью и точностью, увеличивая количество отказов системы [13].

Программа тестирования шаблонов отпечатка пальца и алгоритмов их обработки MINEX III (Minutiae Interoperability Exchange Test) позволяет осуществить измерения производительности и совместимости кодирования

шаблонов ядра (включая ограничения на скорость работы алгоритма, потребление памяти, время выполнения и т.д.), что помогает оценить соответствующие возможности для пользователей, поставщиков и заинтересованных сторон.

Сегодня сервис по тестированию шаблонов для выяснения уровня их стандартизации MINEX III вводит более высокие требования. Новый уровень соответствия PIV Level 2 восходит к большей точности обработки шаблонов одного отпечатка пальца: теперь с FNMR меньшим или равным 0,02 и FMR меньшим или равным 0,0001. При этом, разработчики MINEX III обещают существенно увеличить набор генерируемых данных (до 2 миллионов одиночных шаблонов) и масштаб тестирования (до 3 миллионов операции по тестовой идентификации отпечатка пальца). А результаты тестирования планируется предоставлять с подробными статистическими данными и их графической визуализацией [13].

2.1.4Технологии «живого пальца»

На рынке представлены различные запатентованные технологии обнаружения поддельных отпечатков пальцев.

Одна их них под наименованием fake-finger-detection (FFD), известная также как Liveness Detection SDK, является разработкой NexID Biometrics LLC. Компания имеет свою собственную лабораторию, а также сотрудничает с биометрическими лабораториями в Университете Кларксона и в Университете Западной Вирджинии [14].

Версия 2.0 SDK NextID демонстрирует диапазон точности обнаружения мошеннических попыток идентификации от 96,5% до 99,5%, в зависимости от механизмов создания фальшивого отпечатка.

Кроме работы по увеличению точности работы систем и изучения постоянно изменяющихся методов спуфинга, существует fake-finger-detection также уделяют большое внимание усовершенствованию технических

характеристик программного обеспечения. Стараясь снизить требования к вычислительной производительности и свободным ресурсам, сохранив при этом полный набор функций анализа и защиты от фальсификации отпечатков, NexID добилась успешной интеграции ПО с SoC-системами ("match-on-chip").

Благодаря минимальным системным требованиям, технология распознавания живых отпечатков пальцев SDK может быть успешно интегрирована в любые системы контроля учета доступа, в том числе в банкоматы, кассовые терминалы и т.п. Fake-finger-detection может применяться как самостоятельно, так и в качестве составной части многофакторной системы аутентификации (например, в дополнение к паролю или распознаванию лица). Кроме того, существует решение, специально созданное NexID для мобильных устройств с датчиками отпечатков пальцев, в частности смартфонов от Apple и Samsung.

Вне зависимости от того, считать ли технологии создания фальшивых отпечатков пальца для верификации в биометрических системах простыми или сложными, целесообразными или нет - нельзя не признавать, что такая угроза существует. Еще в 2014 году Chaos Computer Club опубликовал информацию о возможности получения исходных данных для создания подделки не только контактным способом (если человек прикоснулся к любому объекту с полированной поверхностью, будь то стакан или экран смартфона), но и при помощи обычного фотоаппарата.

2.2 Виды сканеров

Все сканеры отпечатков пальцев можно разделить на три типа:

— оптические;

— полупроводниковые;

— ультразвуковые.

2.2.1Оптические сканеры

Оптические сканеры — основаны на применении оптических методов получения изображения [15]. Существует несколько основных способов реализации оптического метода:

- оптический метод на отражение;
- оптический метод на просвет;
- оптические бесконтактные сканеры;
- полупроводниковые сканеры;
- емкостные сканеры;
- радиочастотные сканеры;
- сканеры, использующие метод давления;
- термосканеры;
- ультразвуковой метод.

2.2.1.1 Оптический метод на отражение

Основой метода является эффект нарушенного полного внутреннего отражения [15].

Эффект нарушенного полного внутреннего отражения основывается на разделении световой энергии. Одна часть отражается от границы, вторая проникает через границу во вторую среду. Доля отраженной энергии зависит от угла падения светового потока.

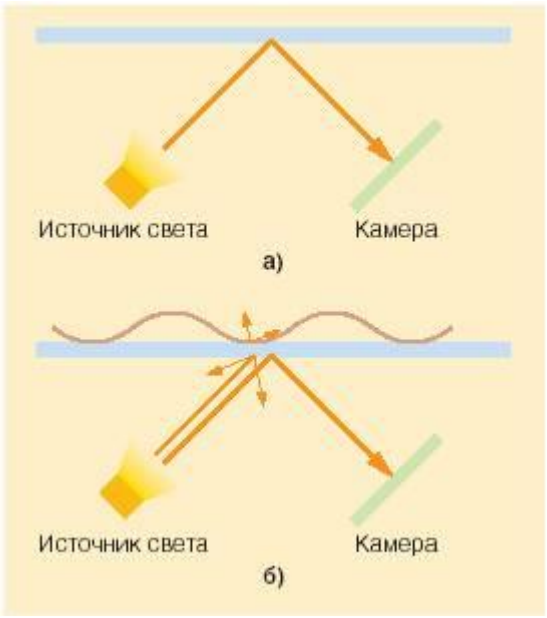


Рисунок 4 – Принцип FTIR-сканеров

Этот эффект называется полным внутренним отражением.

При контакте более плотной оптической среды с менее плотной в точке полного внутреннего отражения пучок света проходит через эту границу. Поэтому, от границы отразятся только пучки света, попавшие в определенные точки полного внутреннего отражения, к которым не был приложен папиллярный узор.

Недостатки метода:

— неэффективная защита от муляжей;

— чувствительность к загрязнениям.

Ведущими производителями подобных сканеров являются компании:

— BioLink;

— Digital Persona;

— Identix.

2.2.1.2 Оптический метод на просвет

Сканеры данного типа представляют собой фотодатчики, которые соединены с оптоволоконной матрицей [15].

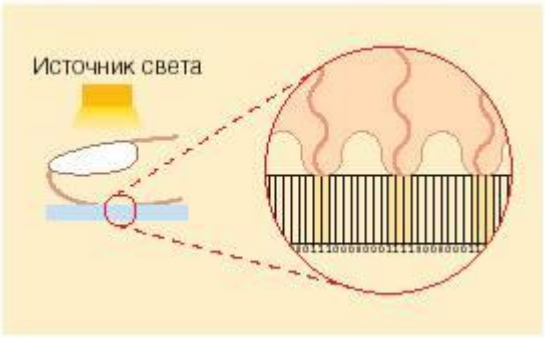


Рисунок 5 – Принцип работы оптоволоконных сканеров

Каждый датчик позволяет фиксировать остаточный свет, который проходит через палец, в точке соприкосновения пальца с поверхность матрицы.

Изображение всего отпечатка формируется по данным, полученным с каждого фотодатчика.

Достоинства метода:

— высокая надежность считывания;

— устойчивость к обману.

Существенным недостатком метода является – сложность реализации метода.

Данный тип сканеров выпускается компанией Security First Corp.

2.2.1.3 Оптические бесконтактные сканеры

Оптические бесконтактные сканеры не требуют непосредственного контактирования пальца и поверхности сканирующего устройства.

Для сканирования отпечатка, палец прикладывается к окну сканирования, несколько источников света направленных на палец подсвечивают палец снизу

под разным углом, в центре сканера находится линза, через которую, собранная информация проецируется на камеру, которая преобразует полученные данные в изображение отпечатка пальца [15].

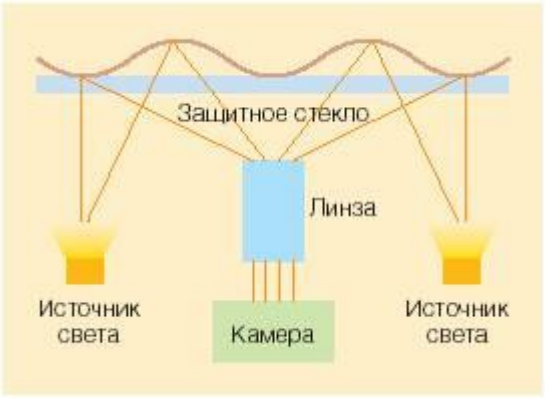


Рисунок 6 – Обобщенная схема работы бесконтактного сканера

Ведущим производителем сканеров данного типа является Touchless Sensor Technology.

2.2.2Полупроводниковые сканеры

В полупроводниковых сканерах изображение поверхности пальцев получается путем применения свойств полупроводников, изменяющихся в местах контакта гребней папиллярного узора с поверхностью сканера [15].

2.2.2.1 Емкостные сканеры

Работа данного типа сканеров основана на эффекте изменения емкости p-n-перехода полупроводника при соприкосновении гребня папиллярного узора с элементом полупроводниковой матрицы [15].

Достоинствами емкостных сканеров является:

— низкая себестоимость;

— надежность.

Недостатком емкостных сканеров является неэффективная защита от муляжей.

Ведущими производителями сканеров данного типа являются компании:

— Infineon;

— STMicroelectronics;

— Veridicom.

2.2.2.2 Радиочастотные сканеры

Сканеры основаны на принципе работы миниатюрных антенн. На сканируемую поверхность пальца направляется сигнал низкой интенсивности. Отраженный от папиллярного узора сигнал принимается чувствительной матрицей. Таким образом получается матрица напряжений, преобразуемая в цифровую модель отпечатка пальцев [15].

Достоинством радиочастотных сканеров является низкая вероятность обмана сканера, недостатком является неустойчивая работа.

Производителем радиочастотных сканеров является компания Authentec.

2.2.2.3 Сканеры, использующие метод давления

Чувствительные к давлению сканеры основан на матрице пьезоэлектрических элементов, чувствительных к нажатию. При прикладывании пальца к сканеру элементы папиллярного узора оказывают давление на матрицу сканера.

Совокупность полученных с пьезоэлектрических элементов напряжений преобразуется в изображение отпечатка пальца.

Недостатки данного метода:

— низкая чувствительность;

— неэффективная защита от муляжей;

— подверженность к повреждениям при чрезмерно прилагаемых усилиях.

Производством чувствительных к давлению сканеров занимается компания BMF.

2.2.2.4 Термосканеры

Термосканеры основаны на пироэлектрических элементах, которые позволяют фиксировать разницу температуры.

При сканировании отпечатка строится температурная карта, которая формируется на основании температуры на гребнях и впадинах папиллярного узора, далее полученный рисунок преобразуется в цифровую модель отпечатка.

Метод на основании применения термосканеров имеет следующие преимущества:

— высокая устойчивость к электростатическому разряду;

— устойчивая работа в широком температурном диапазоне;

— эффективная защита от муляжей.

Недостатком является быстрое исчезновение изображения отпечатка.

2.2.3Ультразвуковой метод

Метод основывается на сканировании поверхности пальца утрозвуковыми волнами. Фиксируется расстояние между источником волн и впадинами папиллярного узора [15].

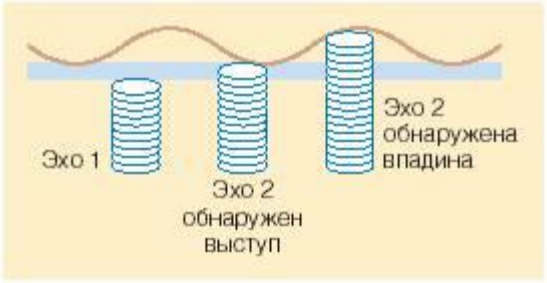


Рисунок 7 – Схема работы утразвукового сканера

Достоинства:

— высокое качество получаемого изображения;

— защита от муляжей;

— позволяет получить информацию о пульсе.

Основным недостатком данного метода является высокая стоимость.

Ведущим производителем сканеров данного типа является компания Ultra-Scan Corporation.

2.3 Сравнение и выбор сканера

Были рассмотрены следующие сканеры:

— BioLink U-Match BI USB. Компактный оптичческий сканер BioLink U-Match BI USB легко интегрируется с оборудованием самых различных типов. В комплект поставки входит крышка для крепления сканера к внешней поверхности и облегчения процесса приложения пальца к окну сканирования [16];

— BioLink S-Match 4F. Специализированный USB-сканер отпечатков пальцев BioLink S-Match 4F применяется в системах массовой биометрической идентификации, предназначенных для выпуска электронных документов, удостоверяющих личность (биометрические паспорта, идентификационные карты и т.п.) и поддержки деятельности правоохранительных органов [17];

— BioLink S-Match 2F. Сканер отпечатков BioLink S-Match 2F разработан специально для работы с системой биометрической идентификации клиентов банка BioLink CI (Client Identification) [18];

— BioLink CI. BioLink CI (Client Identification) – новейшее отраслевое решение от компании BioLink, специально созданное для минимизации

банковских рисков и борьбы с фальсификацией документов в финансовых организациях [19];

— BioLink S-Match 1F. Оптический USB-сканер BioLink S-Match 1F специально разработан для компаний и организаций, заинтересованных в надежной защите своих информационных ресурсов при одновременной минимизации требований, предъявляемых к сотрудникам [20];

— BioLink U-Match BI Ethernet. Сканер BioLink U-Match BI Ethernet активно применяется в корпоративных сетях. С помощью этого устройства осуществляется сканирование отпечатков пальцев на удалении от компьютера, где функционирует программное обеспечение биометрической идентификации. В комплект поставки входит крышка для крепления сканера к внешней поверхности и облегчения процесса приложения пальца к окну сканирования [21];

— Синергет STS-715 (Ethernet). Сканер отпечатка пальца STS-715 конструктивно выполнен в виде встраиваемого модуля для монтажа в стену или панель и представляет собой полноценное решение для организации проходной. Сканер отпечатка пальца STS-715 предназначен для работы с ПО «Стилпост», «Синергет», производства ЗАО «Stilsoft» [22];

— Futronic FS-84. Futronic FS-84 — модуль аутентификации отпечатков пальцев с интерфейсом связи Ethernet, комбинирует в себе оптический сканер отпечатков пальцев и механизм распознавания отпечатков пальцев. Модуль Futronic FS-84 имеет внутренняя память, которая хранит до 2500 шаблонов отпечатков пальцев [23];

— Futronic FS88 OEM module (FS 89). FS88 OEM module является модулем сканера FS88H. Модуль предназначен для интеграции в сторонние ПАК и переносные станции. Сканер имеет уникальный номер, определяющийся при каждом считывании отпечатка [24];

— Futronic FS88H. Сканер отпечатков применяется для массовой идентификации. Исполнен в виде корпусного устройства, подключаемого по UBS. Сканер оснащён системой защиты от муляжей [25];

— Futronic FS26. Устройство представляет собой сканер отпечатков пальцев и считывания карт доступа в одном устройстве. Шаблон отпечатка пальца хранится на карте, и можно сравнить с отпечатком пальца сканируемого с помощью сканера отпечатков пальцев [26].

Данные об отпечатках пальцев сотрудников должны сохраняться в базу данных предприятия, вся вязи с данным ограничением сканеры, которые хранят модели отпечатков в устройстве не подходят для решения задачи идентификации.

Основываясь на проведённом анализе сканеров были отобраны сканеры приведенные в таблице № 1

Таблица 1 – Сравнительные характеристики сканеров BioLink U-MatchEthernet и Futronic FS88 OEM.

Характеристики	**BioLink U-MatchEthernet**	**FS88 OEM**
Тип сканера	оптический	Оптический
Способ исполнения	Встраиваемый	Встраиваемый
Вес	450 г.	80 г.
Размер окна сканирования пальцев	28x20 мм	16 x 24 мм
Разрешение (точек на дюйм)	508	500
Интерфейс	Ethernet 10 MBit	USB 2.0
Размер устройства	79 * 106 * 46 мм	55 x 45 x 20 мм
Напряжение	12В	4.5-5.5 В
Рабочая температура	от 0°С до +55°С	-10 °С до + 55 ° С
Страна производитель	Россия	Китай

2.4 Подходы к защите от муляжей

Одной из самых сложных как для всей области, так и в первую очередь для технологии распознавания отпечатков пальцев является защита от муляжей биометрических идентификаторов.

Данный вопрос является актуальным т.к. отпечатки пальцев относительно легко получить по сравнению и изготовление муляжа отпечатка пальца выглядит также сравнительно более простой задачей [27].

Условно методы можно разделить на две группы:

1) Организационные основываются на организации процессов аутентификации, таким образом, чтобы затруднить или исключить возможность использования муляжа. Можно выделить следующие подметоды:

— усложнение аутентификации. метод заключается в использовании нескольких разных пальцев для проведения идентификации;

— мультибиометрия. метод использует сочетанием нескольких биометрических параметров таких как отпечатки, геометрия лица, голос и т.д.;

— многофакторная аутентификация. метод использует сочетание биометрического метода и других методов.

2. Технические методы реализуются на уровне считывающего устройства или на уровне программного обеспечения. Можно выделить следующие подметоды:

— защита на уровне считывающего устройства;

— защита по дополнительной характеристике. Получение дополнительной информации такой как наличие пульса частиц пота, получение капиллярной сетки;

— защита по предыдущим данным. Производится сравнение не одного, а нескольких последних изображений.

2.5 Плюсы и минусы использования биометрии

В каждом из метод идентификации есть свои достоинства и недостатки, как и в система биометрической идентификации [28].

Преимуществом биометрической идентификации являются:

— безопасность. возможность идентифицировать личность человека;

— удобство. отсутствие дополнительного аппаратного идентификатора;

— экономия времени, как время на идентификацию, так и время на поиск средства идентификации.

Недостатками биометрической идентификации являются:

— нестабильность распознавания. большое количество ошибок второго рода;

— увеличение вычислительных мощностей;

— стоимость разработки и внедрения.

3 ПРАВОВОЙ ВОПРОС

Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным [29].

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну [29].

3.1 Категории персональных данных

Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» определяет следующие категории персональных данных:

1) общедоступные ПДн;
2) специальные категории ПДн;

3) категории ПДн, обрабатываемые в информационных системах персональных данных (далее ИСПДн);

4) биометрические ПДн и другие.

3.2 Общедоступные ПДн

Общедоступные ПДн – данные предоставляемые с согласия субъекта ПДн неограниченному кругу лиц. На этот тип данных не распространяются требования соблюдения конфиденциальности.

К общедоступным ПДн относятся: фамиляю, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн.

3.2.1Специальные категории ПДн

Специальные ПДн – данные о расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Обработка таких данных допускается только в следующих случаях:

— субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;

— персональные данные являются общедоступными;

— персональные данные относятся к состоянию здоровья субъекта ПДн и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

— обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПДн;

— обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

3.2.2Категории персональных данных, обрабатываемых в ИСПДн

Определяются следующие категории ИСПДн:

1) Персональные данные, касающиеся национальной принадлежности, расовой, религиозных и философских убеждений, политических взглядов, состояния здоровья, интимной жизни;

2) Персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

3) Персональные данные, позволяющие идентифицировать субъекта ПДн;

4) Обезличенные и (или) общедоступные персональные данные.

Категорирование персональных данных при обработке в ИСПДн может также проводиться по параметру «объем обрабатываемых персональных данных». Под этим подразумевается количество субъектов, данные которых обрабатываются в информационной системе.

Категорирование персональных данных необходимо для определения класса ИСПДн, от которого зависят меры по обеспечению безопасности ПДн при обработке в информационных системах.

3.3 Биометрические персональные данные

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых

можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Основываясь на определении биометрических ПДн, к ним относятся фотографии и видеоизображения субъектов ПДн.

3.4 Оператор персональных данных

Согласно Закону №152-ФЗ операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных [29].

Под обработкой ПДн понимаются действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Все организации, хранящие у себя данные сотрудников, являются операторами персональных данных.

Помимо этого, многие компании по роду своей деятельности обрабатывают сведения о своих клиентах, партнерах, поставщиках и субподрядчиках, которые им необходимы для выполнения функций в соответствии с их назначением.

3.5 Уведомление Роскомнадзор при обработке ПДн

Оператор ПДн имеет право не уведомлять Роскомнадзор об обработке персональных данных в случаях:

— относящихся к субъектам ПДн, которых с оператором связывают трудовые отношения;

— полученных оператором в связи с заключением договора, стороной которого является субъект ПДн, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;

— относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПДн;

— являющихся общедоступными персональными данными;

— включающих в себя только фамилии, имена и отчества субъектов персональных данных;

— необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;

— включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем (далее ИС), а также в государственные ИСПДн, созданные в целях защиты безопасности государства и общественного порядка;

— обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов ПДн.

При этом бытует ошибочное мнение о том, что в случае, если нет необходимости регистрироваться как оператор ПДн в Роскомнадзоре (а законом такие случаи предусмотрены), то компания не является оператором ПДн и на нее не распространяются обязанности, предусмотренные законодательством. Более того, таким образом компании пытаются оправдать свое бездействие в области обеспечения безопасности ПДн. Если компания не предпринимает никаких усилий по защите персональных данных, это однозначно расценивается как «невыполнение требований российского законодательства».

3.6 Обязанности оператора ПДн

Российское законодательство возлагает на операторов ПДн определенные обязанности, основными из которых являются:

1) Обеспечение безопасности обработки персональных данных, что означает обязанность «принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий»;

2) Уведомительный характер обработки персональных данных. В соответствии со статьей 22 Закона оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) о своем намерении осуществлять обработку персональных данных;

3) Роскомнадзор вносит сведения об операторе в реестр операторов. Информация, содержащаяся в реестре, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, является общедоступной;

4) При получении персональных данных (в том числе от третьих лиц) оператор ПДн до начала обработки обязан получить у субъекта этих ПДн письменное разрешение на их обработку (за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если они являются общедоступными);

5) Оператор обязан предоставить субъекту ПДн по требованию все имеющиеся сведения о нем, целях и условиях обработки, способах защиты его персональных данных. Оператор также должен уничтожить или блокировать соответствующие персональные данные, внести в них необходимые изменения по предоставлении субъектом ПДн или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

6) Более того, оператор ПДн обязан предоставить доказательство получения согласия субъекта ПДн на обработку его персональных данных, а в случае обработки общедоступных персональных данных на него возлагается обязанность доказать, что обрабатываемые ПДн являются общедоступными;

7) Подконтрольность и поднадзорность деятельности операторов персональных данных государственным органам. Это означает обязанность оператора сообщать в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа. Функциями контроля и надзора государство наделило Роскомнадзор, ФСТЭК и ФСБ3.

3.7 Неисполнение требований законодательства

Законом предусмотрена гражданская, уголовная, административная, дисциплинарная и иная ответственность за нарушение его требований. Так, Кодекс об административных правонарушениях предусматривает максимальный штраф в 500000 рублей за невыполнение законного предписания Роскомнадзора (ст. 19.5 КоАП). Тот же Кодекс предусматривает приостановку деятельности организации на срок до 90 суток при осуществлении деятельности по защите персональных данных без лицензии (ст. 19.20 КоАП).

В уголовном кодексе говорится о штрафе в 300000 руб., обязательных работах на срок до 1-го года, аресте до 6-ти месяцев и лишении права занимать должность на срок до 5-ти лет в случае осуществления защиты персональных данных без лицензии в случаях, если это деяние причинило крупный ущерб гражданам (ст. 171 УК).

При систематических и грубых нарушениях Роскомнадзор имеет право ходатайствовать об отзыве лицензий на основной вид деятельности.

4 РАСЧЕТ И АНАЛИТИКА

4.1 Алгоритм распознавания отпечатков пальцев по ключевым точкам

Алгоритм распознавания отпечатков пальцев по ключевым точкам базируется на трех основных этапах: обработка изображения, центрирование и распознавание [30].

На первом этапе линии папиллярного узора изображения отпечатка утончаются до одного пикселя, устраняются шумы и ложные пропечаток, определяется контур отпечатка, определяются граничные точки, выделяются контрольные точки.

Центрирование применяется для ускорения процесса сравнения. Центрирование базируется на двух основных подходах: определение центра информативной области отпечатка пальцев и нахождение пиксельного центра тяжести [31].

Выделение контрольных точек и определение координат этих точек выполняется я в первичной системе координат.

Сопоставление двух отпечатков пальцев базируется на сравнении контрольных точек. Алгоритм сопоставления применяется к цифровым моделям отпечатков пальца T_1 и T_2. На рисунке 8 представлены варианты блока, который вычисляет степень сходства и который принято называть мэтчером.

Рисунок 8 – Основной вариант мэтчеров

Сравнение контрольных точек производится каждая с каждой. В окрестности каждой контрольной точки производится сравнение ближайших точек, если точка располагается на допустимом удалении, то эти точки

считаются совпавшими. Смещение контрольных точек может достигать до 10% от длины рамки изображения отпечатка пальца. Перед каждым сопоставлением отпечатков пальцев вычисляется мера близости двух отпечатков пальцев. Для определения меры близости вносится небольшой угол поворота отпечатка и смещение его центра. Сопоставления выполняются до тех пор, пока не будут перебраны все возможные углы поворота одного отпечатка и возможные сочетания пикселов центральной области [32].

Решение об идентификации принимается по наибольшему значению меры близости из всех вариантов сопоставлений, если оно не меньше заданного порога.

Число сравнений контрольных точек двух отпечатков необходимое для принятия решения об идентификации равно

$$N_{\text{ср}} = N_d N_{\text{ЦО}} N_{\text{КТ}}^2 \quad (1)$$

где N_d — число шагов поворота одного из ОП; $N_{\text{ЦО}}$ — число пикселов центральной области; $N_{\text{КТ}}$ — число контрольных точек в одном из ОП.

Данный алгоритм позволяет распараллелить сопоставление отпечатков, а также снизить зависимость вероятности распознавания отпечатка пальцев от поворотов, смещений. Скорость распознавания отпечатка увеличивается благодаря дополнительному этапу поиска наиболее достоверных пар базовых отрезков.

Центрирование обеспечивает переход от декартовой системы координат к полярной, центром для которой принимается центр достоверного базового отрезка. Из рассмотрения исключаются контрольные точки, расположенные вблизи центра отпечатка и границы информационной области.

Базовые отрезки формируются из внутренних точек разветвлений и окончаний папиллярного рисунка.

При формирование базовых отрезков радиус-вектор вращается по часовой стрелке относительно первичной системы координат, последовательно

отрезками прямых соединяются встречающиеся контрольные точки. Если несколько контрольных точек встречаются в одном направлении радиуса-вектора, то предыдущая точка соединяется с самой удаленной от центра. Оставшиеся контрольные точки соединяются по мере приближения к центру. По завершению обхода контрольных точек базовый отрезок представляется замкнутым контуром в виде ломаной линии с вершинами в контрольных точках

Близкие по длине и взаимной ориентации базовые отрезки выделяются на обоих отпечатках пальцев. Взаимная ориентация определяется значением углов с четырьмя соседними базовыми отрезками.

Достоверная пара базовых отрезков выделяется следующим образом. Необходимо определить отпечаток пальца, который имеет меньшее число базовых отрезков, входящих в ломаные. Этот отпечаток *A* используется для минимизации числа проверяемых пар базового отрезка. Для каждого базового отрезка отпечатка *A* необходимо выбрать такой парный ему базовый отрезок из второго отпечатка *B*, для которого будет минимальной мера *C:*

$$\begin{gathered} \mathrm{C}_1 = \frac{l_A - l_B}{L} + \frac{a_{A_1} - a_{B_1}}{\Lambda}, \\ \mathrm{C}_2 = \frac{l_A - l_B}{L} + \frac{a_{A_2} - a_{B_2}}{\Lambda}, \\ \mathrm{C}_3 = \frac{l_A - l_B}{L} + \frac{a_{A_3} - a_{B_3}}{\Lambda}, \\ \mathrm{C}_4 = \frac{l_A - l_B}{L} + \frac{a_{A_4} - a_{B_4}}{\Lambda}, \\ C = \min\{C_1, C_2, C_3, C_4\} \end{gathered} \qquad (2)$$

где l — длина базового отрезка; α — угол с соседним базовыми отрезками в пределах одного и того же отпечатка пальца; L — максимальная длина базового отрезка в обоих базовых отрезках; Λ — максимально возможная величина угла, равная 2π. В качестве центра *O* новой полярной системы координат в одном из отпечатков пальцев принимается центр достоверного базового отрезка той пары базового отрезка, для которой будет значение *C* наименьшим. Достоверная пара базового отрезка выбирается по следующей формуле:

$$C_{min} = \min_i \left\{ \min_j \left\{ \max_K \{C\}_{K=1}^{K=4} \right\}_{j=1}^{j=N_B} \right\}_{i=1}^{i=N_A} \quad (3)$$

где N_A, N_B — число базовых отрезков в отпечатках A и B соответственно; K — число соседних базовых отрезков, используемых при нахождении меры C (1), где $K = 4$.

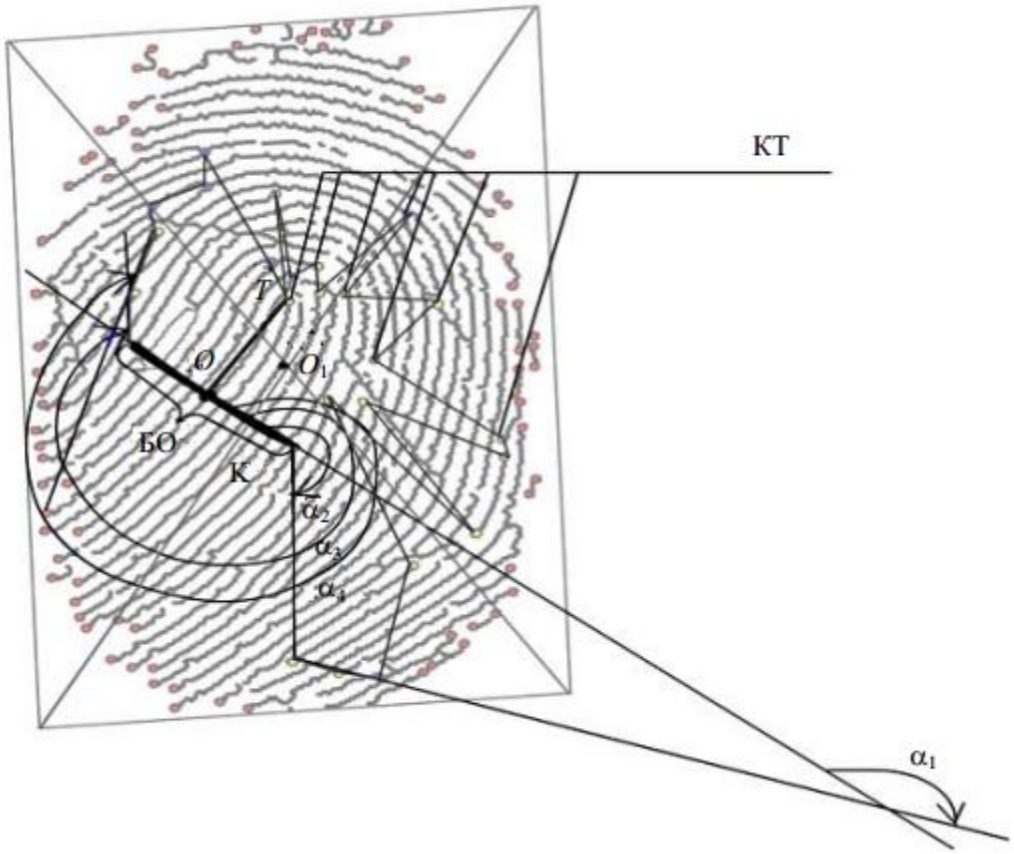


Рисунок 9 – Выделение особых точек на отпечатке пальца

В полярной системе координат формируется векторное описание множеств контрольных точек с учетом до контрольной точки от центра

Перевод из первичной в новую полярную систему координат осуществляется по следующим формулам:

$$L = \sqrt{(X_T - X_O)^2 + (Y_T - Y_O)^2},$$

$$\alpha = arccos \frac{(X_T - X_O)^2 + (Y_T - Y_O)^2 + (X_K - X_O)^2 + (Y_K - Y_O)^2 - (X_K - X_T)^2 - (Y_K - Y_T)^2}{2\sqrt{(X_T - X_O)^2 + (Y_T - Y_O)^2}\sqrt{(X_K - X_O)^2 + (Y_K - Y_O)^2}} \quad (4)$$

где $X_т$, $Y_т$ — абсцисса и ордината данной контрольной точки в первичной системе координат; X_0, Y_0 — абсцисса и ордината центра достоверного базового отрезка в первичной системе координат.

Для каждого элемента множеств контрольных точек соответствующим отпечаткам пальцев A и B, необходимо вычислить минимальное расстояние от всех элементов другого множества:

$$e_k^A = min_t\{d\left((\alpha_k^A, l_k^A), (\alpha_t^B, l_t^B)\right)\}_{t=1}^{t=N_B}, k = 1, \dots, N_A,$$
$$e_k^B = min_k\{d\left((\alpha_t^B, l_t^B), (\alpha_k^A, l_k^A)\right)\}_{k=1}^{k=N_A}, t = 1, \dots, N_B \quad (5)$$

где $d(x, y)$ — расстояние между элементами множеств x и y; t, k — номер контрольной точки в множествах A и B соответственно. После этого необходимо вычислить максимальные значения из множеств полученных минимумов:

$$e_{max}^A = min_k\{e_k^A\}$$
$$e_{max}^B = min_t\{e_t^B\} \quad (6)$$

Затем вычисляются максимум и минимум из двух полученных величин (6):

$$e_{\max i,j} = \max(e_{max}^A, e_{max}^B)$$
$$e_{\mathrm{mix}\, i,j} = \mathrm{mix}(e_{max}^A, e_{max}^B) \quad (7)$$

где i, j — номер выбранного достоверного базового отрезка в A и B соответственно. Определение минимума необходимо для определения степени включения одного множества в другое, это позволяет численно определить идентичность фрагментов пары отпечатков пальцев. Вывод о совпадении отпечатков пальцев принимается на основе анализа $e_{max,ij}$ и $e_{min,ij}$

Если $e_{max,ij} \leq h$ и $e_{min,ij} \leq h$, то отпечатки признаются идентичными. Если $e_{max,ij} > h$ и $e_{min,ij} \leq h$, то отпечатки принадлежат разным людям. Значение h выбирается пропорционально значению C сопоставляемых отпечатков пальцев.

4.2 Структура формата записи контрольных точек

В таблице 2 приведены структура и поля формата записи контрольных точек отпечатка пальца. Форматы блоков дополнительных данных числа гребней, ядра, дельты и локального качества указаны в сокращенном виде [31].

Таблица 2 – Форма записи контрольных точек

	Поле	**Размер**	**Значение**	**Примечание**
Один заголовок на всю запись	Идентификатор формата	4 байта	0X464D5200 (‘F’ ’M’ ’R’ 0x0)	“FMR” (Finger minutiae record) запись контрольных точек
	Номер версии стандарта	4 байта	n n n 0x0	“XX”, где XX=20 и более
	Длина записи	4 байта	от 24 до 4294967295	Значение может быть от 0x0018 д о OxOOOOFFFFFFFF
	Сертфикаты сканера	4 бита		Совместимы со стандартами ИСО в области био метрии
	Идентификационный номер типа сканера	12 битов		
	Размер изображения по горизонтали	2 байта		
	Размер изображения по вертикали	2 байта		
	Разрешение изображения по горизонтали	2 байта		
	Разрешение изображения по вертикали	2 байта		

	Поле	Размер	Значение	Примечание
	Число представлений пальцев	1 байт		
	Зарезервированное поле	1байт		
Один заголовок на каждое представление пальца	Локализация пальца	4 бита	От 0 до 10	
	Номер представления	4 бита	От 0 до 10	
	Тип отпечатка пальца	4 бита	От 0 до 15	
	Качество изображения отпечатка пальцев	1 байт	0, 1, 2, 3, 8	
	Число контрольных точек отпечатка пальца	1 байт	От 0 до 100	Должно быть в диапазоне от 0 до 100
Один заголовок на каждую точку	Координата X расположения контрольной точки (тип контрольной точки указывается в двух старших битах)	2 байта		Указывают в элементах изображения
Один заголовок на каждое представление пальца	Длина области дополнительных данных	2 байта		0 0000 означает отсутствие блока дополнительных данных
Ноль и более заголовков на каждое представление пальца	Код типа блока дополнительных данных	2 байта		Присутствует в случае, если длина блока дополнительных данных не равна 0
	Длина блока дополнительных данных	2 байта		Присутствует в случае, если длина блока дополнительных данных не равна 0
	Дополнительные данные	Указывается в предыдущем поле		Присутствует в случае, если длина блока дополнительных данных не равна 0

Определяются следующие типы форматов контрольных точек отпечатка пальца:

— формат нормального размера;

— формат компактного размера.

В формате нормального размера каждая контрольная точка кодируется пятью байтами согласно таблице 3:

— тип / контрольной точки (2 бита):

00 — другая контрольная точка,

01 — окончание гребня, установленное через точку бифуркации основы впадин, или окончание основы гребней,

10 — бифуркация гребня, определенная через точку бифуркации основы гребней,

11 — зарезервировано для дальнейшего использования;

— координата X (14 битов) с размерами элемента изображения, равным 10"2 мм;

— зарезервировано 2 бита; значение по умолчанию — 00;

— координата Y (14 битов); с размерами элемента изображения, равным 1СГ2 мм;

— ориентация контрольной точки θ (8 битов) с шагом 2я/256 рад.

Таблица 3 – Формат нормального размера контрольной точки

Тип 1	Координата X	Зарезервировано	Координата Y	Ориентация θ
2 байта		2 байта		1 байт

В формате компактного размера каждая контрольная точка кодируется тремя байтами согласно таблице 4.

Таблица 4 – Формат компактного размера контрольной точки

Координата X	Координата Y	Тип1	Ориентация θ
1 байт	1 байт	1 байт	

а) координата X (8 битов) с размерами элемента изображения, равными 10-1 мм;

б) координата Y (8 битов) с размерами элемента изображения, равными 10-1 мм;

в) тип контрольной точки (2 бита), аналогичный формату нормального размера;

г) ориентация контрольной точки 0 (6 бит) с шагом 2я/64 рад.

Примечание — Максимальное значение для координат X и Y в компактном формате должно составлять 25,5 мм.

4.3 Порядок следования контрольных точек

Упорядочивание последовательности контрольных точек производится в соответствии с таблицей 5.

Таблица 5 – значение объекта данных «Упорядочение последовательности контрольных точек»

Биты данных								Значение
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	Упорядочение не требуется (по умолчанию)
						0	1	Упорядочение по требованию
						1	0	Упорядочение по убыванию
			0	0	1			Упорядочивание в декартовой системе координат XY*
			0	1	0			Упорядочивание в декартовой системе координат YX
			0	1	1			Упорядочение по значению угла**

Биты данных								Значение
b8	b7	b6	b5	b4	b3	b2	b1	
			1	0	0			Упорядочение в полярной системе координат
		1	0	0	0	0	0	Упорядочение с расширением координат X или Y в формате компактного размера
x	x	x						000, значение зарезервированы
* Упорядочение по возрастанию/убыванию координат X, а если координаты X равны — по возрастанию/убыванию координаты У(сначала X, затем — Y). ** По значению угла определяют ориентацию контрольной точки.								

Упорядочивание производится в соответствии со следующими процедурами:

— упорядочение последовательности контрольных точек по возрастанию;

— упорядочение по убыванию;

— упорядочение в декартовой системе координат ху;

— упорядочение в декартовой системе координат ух;

— упорядочение по значению угла;

— упорядочение в полярной системе координат: допускается упорядочение по убыванию и по возрастанию значения угла полярной системы координат.

$$X_{cm} = (X_1 + X_2 +, \dots, +X_n)/n,$$

$$Y_{cm} = \frac{Y_1 + Y_2 +, \dots, +Y_n}{n} \quad (8)$$

где n – число контрольных точек;

Xi, Yi – координаты контрольной точки;

cm – центр масс.

— упорядочение с расширением координат X и Y в формате компактного размера.

4.4 Регистрация отпечатка пальца в базе данных

Для возможности идентификации сотрудника или клиента по отпечаткам пальцев сначала необходимо зарегистрировать его отпечатки пальцев в системе. Процесс регистрации отпечатка каждого пальца сотрудника в базе данных осуществляется в следующие этапы:

— сканирование отпечатка пальца;

— распознавание и выделение папиллярных линий в снимке отпечатка пальца;

— выделение папиллярных узоров;

— создание шаблона (модели) отпечатка пальца;

— преобразование шаблона в цифровое представление;

— сохранение шаблона в базе данных.

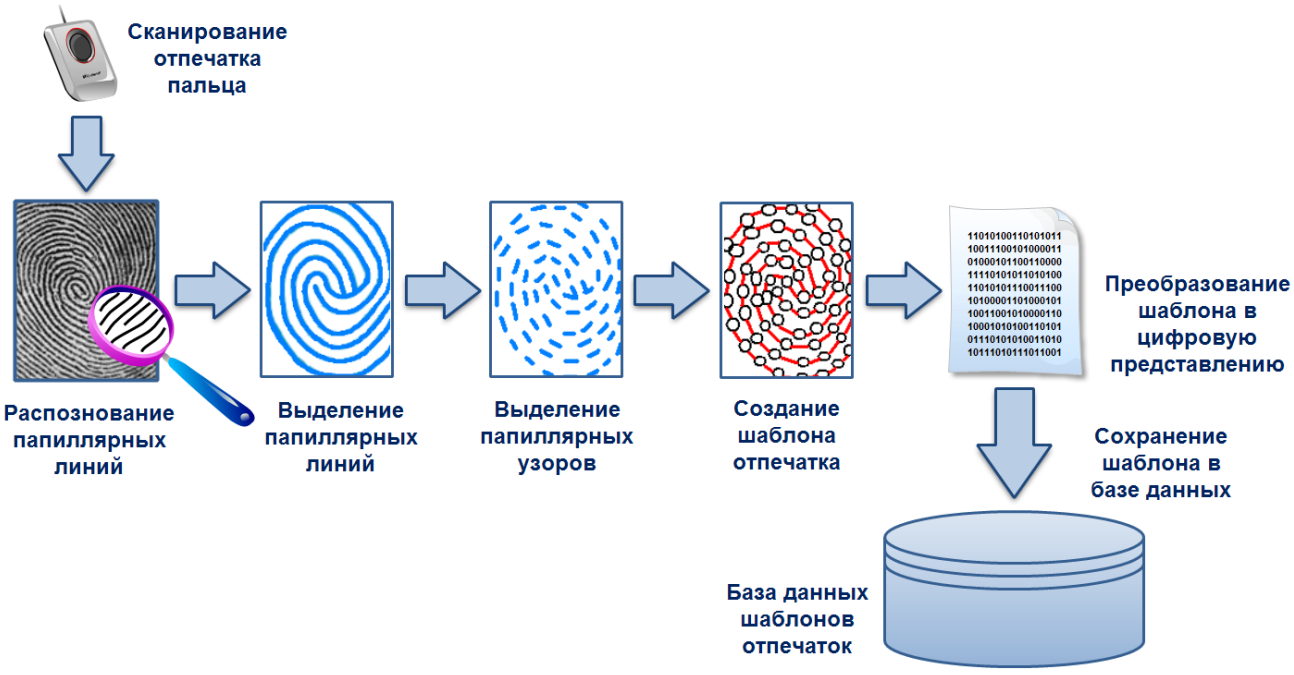


Рисунок 10 – Иллюстрация процесса регистрации отпечатка пальца в базе данных

Как видно из рисунка, в базе данных сохраняется не графический образ отпечатка пальца, полученный со сканера, а его цифровая модель. Цифровая модель отпечатка, сохранённая в базе данных, называется шаблоном.

4.5 Идентификация личности и аутентификация по отпечатку пальца

Процесс идентификации личности по отпечатку пальца осуществляется в следующие этапы:

— сканирование отпечатка пальца;

— распознавание и выделение папиллярных линий в снимке отпечатка пальца;

— выделение папиллярных узоров;

— считывание базы данных шаблонов отпечаток пальцев в оперативную память;

— поочередное сравнение отпечатка пальца с шаблонами отпечаток из базы данных до нахождения подходящего шаблона;

— идентификация или аутентификация сотрудника успешна, если найден подходящий отпечатку шаблон;

— клиент или сотрудник не идентифицирован, если не найден подходящий отпечатку шаблон.

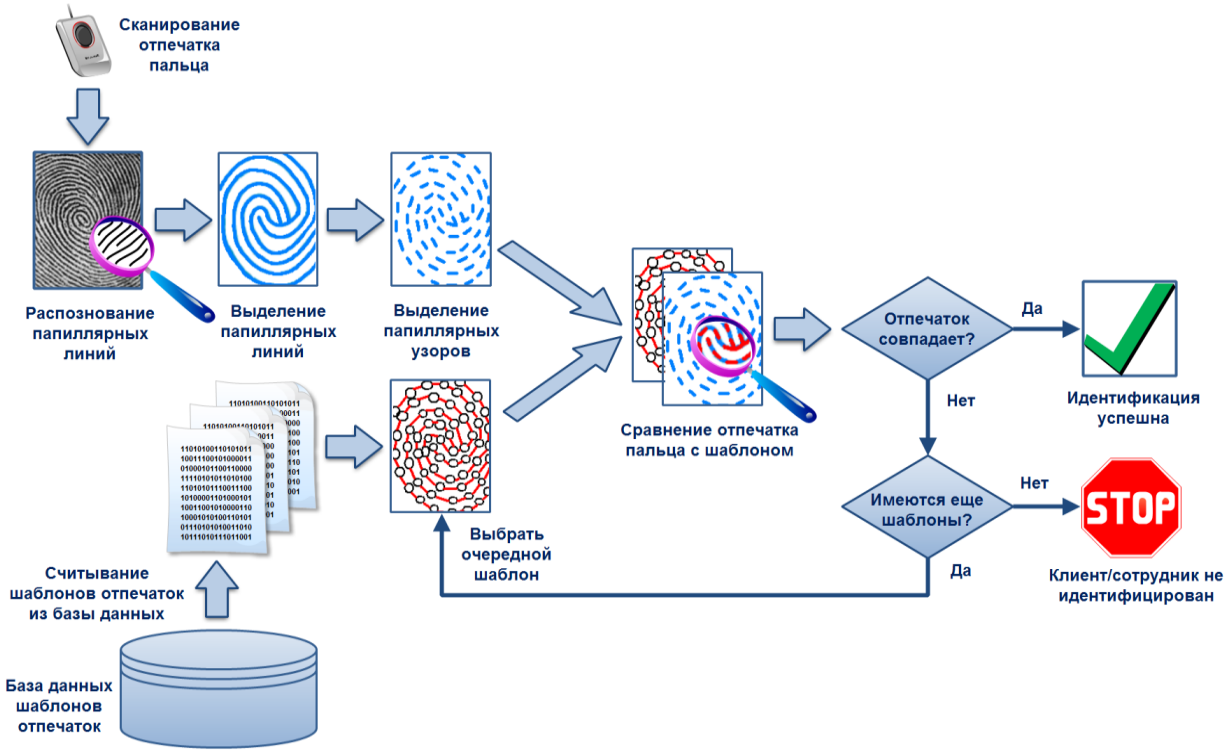


Рисунок 11 – Иллюстрация идентификации клиента или сотрудника по отпечатку пальца

Как видно из рисунка, в процессе идентификации модель отсканированного отпечатка клиента или сотрудника будет поочерёдно сравниваться с шаблонами отпечатков из базы данных, пока не будет найден шаблон отпечатка идентифицируемого сотрудника или клиента, отсканированного ранее в процессе регистрации.

Процесс аутентификации сотрудника или клиента схож с процессом идентификации. Единственным отличием является то, что в случае аутентификации поиск подходящего отпечатка осуществляется не по всей базе данных, а только в подмножестве шаблонов отпечатков пальцев, принадлежащих авторизуемому сотруднику.

4.6 Алгоритм распознавания отпечатков пальцев.

После получения картинки отпечатка пальца с помощью сканера, она преобразуется в цифровую модель.

Из графического изображения выделяются ключевые характерные точки из которых формируется цифровая модель отпечатка. В современных системах берется от 12- 24 ключевых точек. При выборе большего количества ключевых точек, современных вычислительных ресурсов не хватит для нормальной эксплуатации системы в связи с низкой скоростью идентификации. При выборе меньшего количества точек, существует большая вероятность допуска чужого отпечатка пальца. Поэтому необходимо брать некое среднее значение для удовлетворения обоих требований.

В связи с этим алгоритм распознавания отпечатков имеет 2 важных параметра: FAR – ошибка предоставления допуска чужому пользователю; FRR – ошибка недопуска своего пользователя. Эти величины взаимопропорциональны. На сегодняшний день значения данных параметров FRR-0.01%, FAR-0.000001%. Биометрические устройства имеют функцию изменения этих значений, таким образом Вы можете для каждого конкретного случая выбирать или высокую скорость распознавания, или высокую безопасность системы.

4.7 Программная реализация

4.7.1Объект License

BioLink SDK защищен лицензией.

Лицензия BioLink SDK может быть следующих типов для получения дополнительной информации о типах лицензий BSDK):

— встроенный в USB-ключ Rainbow Sentinel (только для операционной системы Windows системы);

— встроенный в сканер BioLink U-Match 3.5;

— программного обеспечения.

Чтобы начать работу с BSDK, необходимо создать объект License. Любая защищенная BSDK вызов метода (сравнение, сканирование, идентификация)

завершится с ошибкой «No License», если нет успешно созданной и все еще существует объект лицензии.

Защищаются следующие операции:

— сравнение шаблонов (объект Matcher);

— сканирование (объект сканера);

— перечисление устройств (объект DeviceList);

— создание шаблона (объект ImageProcessor).

Во время создания объекта лицензии лицензия не проверяется, т. е. Объект лицензии конструктор вернет Success независимо от наличия лицензии.

4.7.2Сканирование изображения отпечатков пальцев

Чтобы создать объект лицензии, который должен существовать все время использования BSDK. Затем вы должны получить список всех устройств, подключенных к компьютеру (используя DeviceList объект). Выбирается первое найденное устройство из списка подключенных устройств, передавая 0 в метод deviceList.DeviceDescriptor. Возвращаемая ссылка на подключенное устройство затем используется для создания объекта Scanner. Изображение отпечатка пальца затем извлекается со сканера с помощью сканера. AcquireImage метод.

4.7.3Создание, сохранение и загрузка шаблона

Объект ImageProcessor используется для создания шаблонов отпечатков пальцев из изображений. Чтобы создать шаблон, необходимо передать объект ImageSet (содержащий полученные изображения с помощью объекта Scanner и добавлен в ImageSet с определенным FingerCode) в качестве параметр метода ImageProcessor.CreateTemplate.

Чтобы сохранить шаблон в байтовом массиве, необходимо вызвать метод Save объекта Template. Загрузить шаблон из массива буферов, использовать метод Load, определяющий получателя как параметр.

4.7.4 Сравнение двух шаблонов

Чтобы сравнить два шаблона, необходимо создать экземпляр объекта Matcher. Метод Matcher.Compare возвращает целочисленное значение представляя порог между двумя шаблонами.

Однако рекомендуется использовать метод Matcher.Identify для сравнения шаблонов. При работе в больших базах данных для него используются все доступные ядра процессоров для ускорения процесса сравнения.

4.7.5Идентификация один ко многим

Удобный способ выполнения идентификации (согласование 1 к N) обеспечивается объект TemplateSet BioLink SDK и метод Matcher.Identify.

Объект TemplateSet представляет набор зарегистрированных шаблонов, среди которых идентификация будет выполнено. Построение набора шаблонов состоит из создания объекта TemplateSet и добавление шаблонов путем вызова метода TemplateSet.Add. Параметры переданы для добавления - это сам шаблон, идентификационный номер, используемый для уникальной идентификации.

Шаблон в наборе и связан с записью во внешнем хранилище, например, базы данных и строкового значения, которое не может быть уникальным.

Метод Matcher.Identify ищет шаблон TemplateSet для сопоставления, фактически, набор Matcher.Identify принимает в качестве входных данных следующие параметры: шаблон отпечатка пальца для поиска, TemplateSet, где искать, порог совпадения и максимальный количество совпадений для возврата (topN) (если последний параметр опущен, все совпадения, который больше

установленного порога, будет возвращен). Однажды вызванный, Identify сравнивает искомый шаблон с каждым шаблоном в наборе, формирующем список идентификационных номеров шаблонов и совпадений. Затем этот список сортируется в по убыванию, совпадение результатов меньше порогового значения, и topN записей. Список возвращается как объект IdentifyInfoSet.

Объект IdentifyInfoSet содержит коллекцию объектов IdentifyInfo. Обратившись к объекту IdentifyInfo в IdentifyInfoSet можно получить доступ передав метод IndentifyInfoSet.GetItem в качестве параметра. Каждый Объект IdentifyInfo возвращает информацию о шаблоне отпечатка пальца в наборе TemplateSet и результат его сравнения с идентифицируемым шаблоном отпечатка пальца.

Основное преимущество метода Matcher.Identify заключается в его способности использовать все доступные ядра процессора для выполнения сопоставления 1 к N в больших базах данных. Вот почему не рекомендуется использовать метод Matcher.Compare, поскольку в нем используется только одно ядро и может быть узким местом для общей производительности системы.

4.8 Архитектура программно-аппаратного комплекса «ЮМС Диагностический шлюз»

4.8.1Существующая архитектура программно-аппаратного комплекса

Диаграмма развертывания программно-аппаратного комплекса «ЮМС Диагностический шлюз» представлена на рисунке 12.

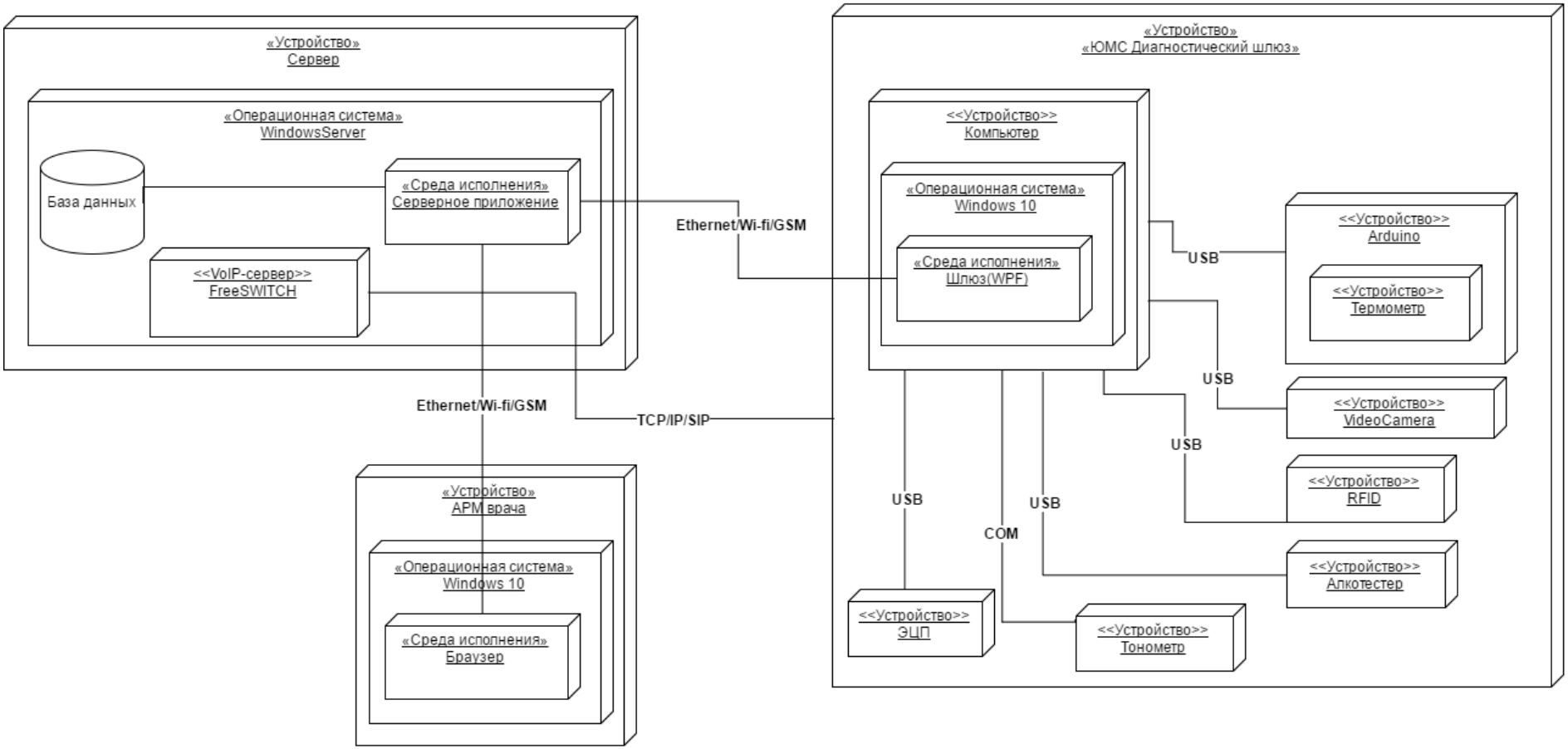


Рисунок 12 – Диаграмма развертывания программно-аппаратного комплекса «ЮМС Диагностический шлюз»

ЮМС Диагностический шлюз состоит из следующих элементов:

— устройство «ЮМС диагностический шлюз» представленный в виде установки для прохождения предсменного и послесменного осмотра;

— устройство «Компьютер» под управлением Windows 10;

— среда исполнения «Шлюз», реализующий работу программного обеспечения «ЮМС диагностический шлюз»;

— устройство «Arduino» осуществляет взаимодействие с датчиками, размещенными на диагностическом шлюзе;

— устройство «Сервер» под управлением операционной системы WindowsServer;

— среда исполнения «Серверное приложение» обеспечивающее взаимосвязь всех шлюзов с базой данных;

— база данных содержащая данные о сотрудниках предприятия и результатах исследования;

— устройство «АРМ врача» под управлением операционной системы Windows 10;

— среда исполнения «Браузер» обеспечивает взаимодействие сотрудников отдела кадров с серверным приложением;

— VoIP-сервер «FreeSWITCH» обеспечивает фиксацию звонков.

4.8.2Модификация программно-аппаратного комплекса

Диаграмма развертывания программно-аппаратного комплекса «ЮМС Диагностический шлюз» после внедрения модуля идентификации по отпечаткам пальцев представлена на рисунке 13.

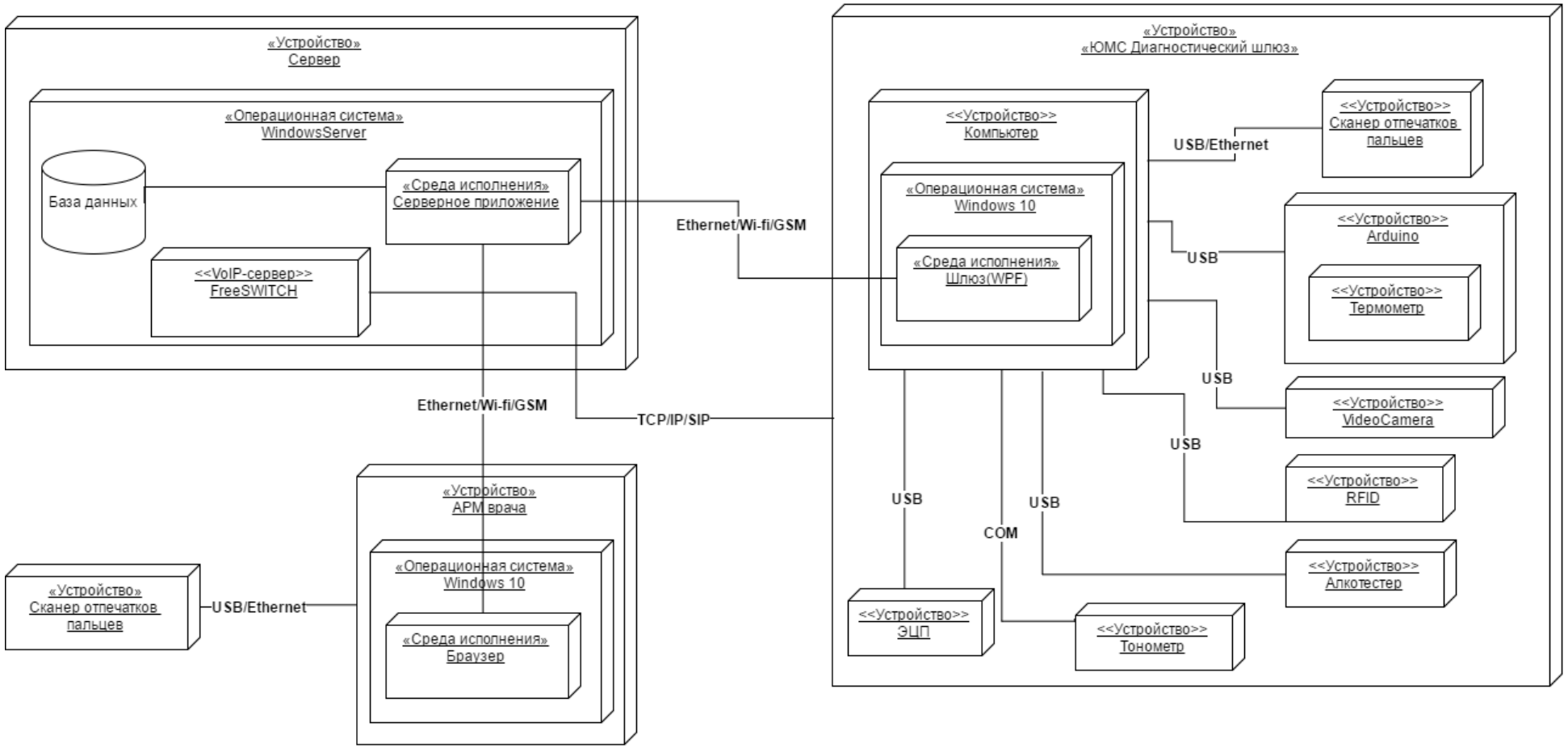


Рисунок 13 – Диаграмма развертывания программно-аппаратного комплекса «ЮМС Диагностический шлюз»

В состав программно-аппаратного комплекса были включены следующие компоненты:

— устройство «ЮМС Диагностический шлюз» дополняется устройством «Сканер отпечатков пальцев», который подключается при помощи кабеля USB или Ethernet;

— устройство «АРМ врача» расширяется возможностью взаимодействия с устройством «Сканер отпечатков пальцев», который подключается при помощи кабеля USB.

4.9 Предложения по изменению бизнес-процесса по прохождению медицинского осмотра

4.9.1Регистрация сотрудника в базе данных

Процесс регистрации сотрудника представлен на диаграмме деятельности.

Рисунок 14 – Регистрация сотрудника и внесение его биометрических данных в базу данных

1) Каждый сотрудник должен пройти в отделе кадров регистрацию в системе.

2) Сотрудники должны подписать согласие на обработку персональных данных.

3) Сотрудник отдела кадров должен внести отпечаток пальца сотрудника посредствам считывания со сканера отпечатков пальцев.

4.9.2Прохождение идентификации в системе

Процесс идентификации сотрудника представлен на диаграмме деятельности.

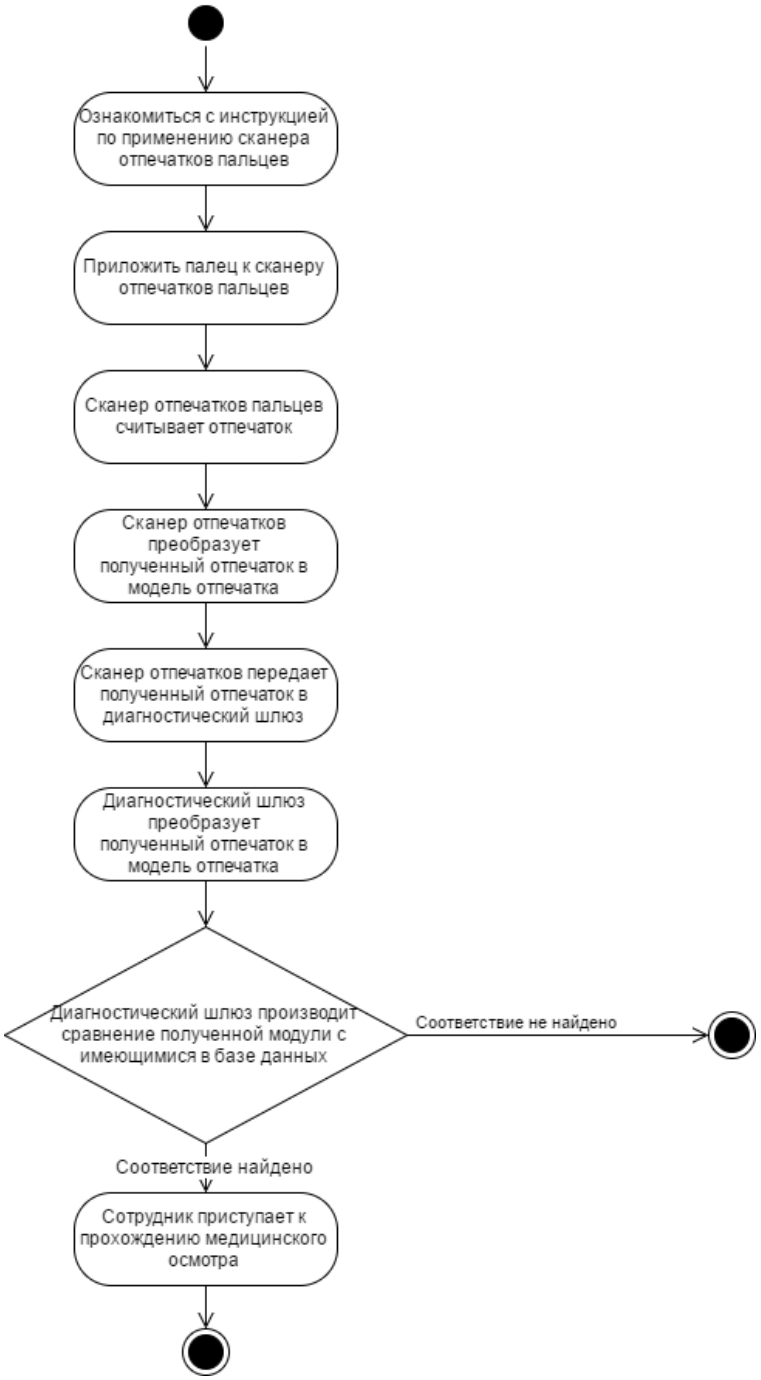


Рисунок 15 – Диаграмма деятельности описывающая процесс идентификации сотрудника

1) Ознакомиться с инструкцией по применению сканера отпечатков пальцев (Приложение Б).

2) Приложить палец к сканеру отпечатков пальцев.

3) Сканер отпечатков пальцев считывает отпечаток

4) Сканер передает рисунок отпечатка диагностическому шлюзу.

5) Диагностический шлюз преобразует полученный отпечаток в цифровую. модель отпечатка.

6) Программное обеспечение диагностического шлюза производит сравнение полученной модули отпечатка с имеющимися моделями отпечатков в базе данных.

7) При нахождении соответствия сотруднику предоставляется доступ к прохождению медицинского осмотра.

8) При несоответствии предоставленного отпечатка пальцев и пальца в базе данных на экране диагностического шлюза сотрудник увидит сообщение об отказе в доступе.

При отказе в доступе пользователю необходимо повторить попытку идентификации.

5 РЕЗУЛЬТАТЫ ПРОВЕДЕННОГО ИССЛЕДОВАНИЯ

В ходе проведения исследования было выполнено:

Обзор аппаратного обеспечения, обеспечивающего идентификацию по биометрическим параметрам.

Выбрано аппаратное обеспечение для решения задачи идентификации на основе отпечатка пальцев.

Рассмотрена существующая архитектура программно-аппаратного комплекса «ЮМС Диагностический шлюз».

Подготовлено решение по интеграции.

Разработано программное обеспечение обеспечивающее исполнение предложенного способа на АРМ сотрудника отдела кадров, производящего регистрацию сотрудников в системе медицинских осмотров, а также разработано решение для обеспечения работы диагностического шлюза по идентификации сотрудников.

Подготовлено предложение по изменению бизнес-процесса по прохождению медицинского осмотра.

Была подготовлена конфигурация программно-аппаратного комплекса для использования идентификации сотрудника с использованием средств биометрической идентификации.

Проведены работы по тестированию и отладке.

6 ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ

Целью настоящего раздела магистерской диссертации является финансовая и технико-экономическая оценка показателей разрабатываемого алгоритма идентификации сотрудников по биометрическим параметрам. В данное обоснование включается оценка денежных затрат на исследование и разработку проекта, экономических результатов ее внедрения, а также научно-технического уровня разработки.

6.1 Организация и планирование работ

При организации процесса разработки алгоритма необходимо распределять уровень занятости каждого из его участников и сроки проведения отдельных этапов. Целью работы на данном этапе будет составление линейного графика проведения работ. Составим хронологическую таблицу этапов работ для исполнителя (И) и научного руководителя (НР) (таблица 6).

Таблица 6 – Перечень работ и продолжительность их выполнения

Этап разработки	Исполнители	Загрузка исполнителя
Постановка целей и задач, сбор первоначальной информации	НР, И	НР – 70%, И – 100%
Планирование и технико-экономическое обоснование ВКР	И	И – 100%
Анализ опасных и вредных производственных факторов	И	И – 100%
Составление и согласование технического задания	НР, И	НР – 30%, И – 70%
Анализ предметной области и сбор необходимой информации	И	И-100%
Анализ существующих разработок	И	И – 100%
Анализ существующих сканеров отпечатков	И	И – 100%
Выбор сканера отпечатков	НР, И	НР – 30%, И – 100%
Проектирование модели	НР, И	НР – 20%, И – 100%
Разработка модели	НР, И	НР – 10%, И – 100%
Тестирование модели	И	И – 100%
Составление и оформление пояснительной записки	И	И – 100%

6.1.1Продолжительность этапов работ

Определим ожидаемые значения продолжительности выполняемых работ ($t_{ож}$) экспертным путем с учетом загруженности исполнителей, которые приведены в таблице 1, в рабочих днях (раб. дн.) по следующей формуле:

$$t_{ож} = \frac{3*t_{min}+2*t_{max}}{5} \quad (9)$$

где tmin – минимальная продолжительность работы, дн.;

tmax – максимальная продолжительность работы, дн.;

Для построения линейного графика необходимо рассчитать длительность этапов в рабочих днях, а затем перевести ее в календарные дни. Расчет продолжительности выполнения каждого этапа в рабочих днях ($T_{РД}$) ведется по формуле:

$$T_{РД} = \frac{t_{ож}}{K_{ВН}} \cdot K_{Д} \quad (10)$$

где $t_{ож}$ – продолжительность работы, дн.;

$K_{вн}$ – коэффициент выполнения работ, учитывающий влияние внешних факторов на соблюдение предварительно определенных длительностей, в частности, возможно $K_{вн} = 1$;

$K_{Д}$ – коэффициент, учитывающий дополнительное время на компенсацию непредвиденных задержек и согласование работ ($K_{Д}$ = 1–1,2; в этих границах конкретное значение принимает сам исполнитель).

Расчет продолжительности этапа в календарных днях ведется по формуле:

$$Т_{КД} = Т_{РД} * Т_{К} \quad (11)$$

где $Т_{КД}$ – продолжительность выполнения этапа в календарных днях; $Т_{К}$ – коэффициент календарности, позволяющий перейти от длительности работ в рабочих днях к их аналогам в календарных днях, и рассчитываемый по формуле 12

$$Т_{к} = \frac{Т_{КАЛ}}{Т_{КАЛ} - Т_{ВД} - Т_{ПД}} \quad (12)$$

где $Т_{КАЛ}$ – календарные дни (ТКАЛ = 365);

$Т_{ВД}$ – выходные дни (ТВД = 50);

$Т_{ПД}$ – праздничные дни (ТПД = 17).

$$Т_{К} = \frac{365}{365 - 50 - 17} = 1{,}22$$

В таблице 7 приведены длительность этапов работ и число исполнителей, занятых на каждом этапе.

Таблица 7 – Длительность этапов работ и число исполнителей, занятых на каждом этапе.

Этап разработки	**Исполнители**	**Загрузка исполнителя**	**Продолжительность работ, дни**			**Трудоемкость, чел/дн**			
						Трд		**Ткд**	
			tmin	**tmax**	**tож**	**Р**	**И**	**Р**	**И**
Постановка целей и задач, сбор первоначальной информации	НР, И	НР – 70%, И – 100%	2,0	4,0	2,8	3,1	3,1	3,6	3,6
Планирование и технико-экономическое обоснование ВКР	И	И – 100%	2,0	4,0	2,8		3,1		3,6
Анализ опасных и вредных производственных факторов	И	И – 100%	1,0	2,0	1,4		1,5		1,8
Составление и согласование технического задания	НР, И	НР – 30%, И – 70%	3,0	5,0	3,8	2,3	4,2	2,76	5,0
Анализ предметной области и сбор необходимой информации	И	И-100%	7,0	9,0	7,8		8,6		10,3
Анализ существующих разработок	И	И – 80%	1,0	3,0	1,8		2,0		2,3
Анализ существующих сканеров отпечатков	И	И – 100%	10,0	12,0	10,8		11,9		14,3
Выбор сканера отпечатков	НР, И	НР – 30%, И – 100%	20	30	24	19,6	26,4	23,52	31,8
Проектирование модели	НР, И	НР – 20%, И – 100%	10	20	14	11,5	15,4	13,8	18,5
Разработка модели	НР, И	НР – 10%, И – 100%	7	15	10,2	8,1	11,22	9,72	13,5
Тестирование модели	И	И – 100%	2	6	3,6		3,9		4,7
Составление и оформление пояснительной записки	НР, И	НР - 20%,И – 100%	12	15	13,2	9,9	4,52	11,88	17,4
Итого					96,2	54,5	95,84	65,28	126,8

Таблица 8 – Линейный график работ

Этап	**НР**	**И**	Февраль			Март			Апрель			Май		
			10	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**	**110**	**120**
1	3,6	3,6												
2		3,6												
3		1,8												
4	2,76	5,0												
5		10,3												
6		2,3												
7		14,3												
8	23,52	31,8												
9	13,8	18,5												
10	9,72	13,5												
11		4,7												
12	11,88	17,4												

6.1.2Расчет накопления готовности проекта

В данном пункте оценивается текущее состояние (результаты) над проектом. Данный показатель позволяет точно знать, на каком уровне выполнения находится определенный этап или работа.

Введем следующие обозначения:

— ТРобщ. – общая трудоемкость проекта;

— ТРi (ТРk) − трудоемкость i-го (k-го) этапа проекта;

— ТРiН − накопленная трудоемкость i-го этапа проекта по его завершении;

— ТРij (ТРkj) − трудоемкость работ, выполняемых j-м участником на i-м этапе, здесь $j = \overline{1,m}$ − индекс исполнителя (m = 2).

Степень готовности определяется формулой (13)

$$СГ_i = \frac{ТР_i^Н}{ТР_{общ.}} = \frac{\sum_{k=1}^{i} ТР_k}{ТР_{общ.}} = \frac{\sum_{k=1}^{i}\sum_{j=1}^{m} ТР_{km}}{\sum_{k=1}^{I}\sum_{j=1}^{m} ТР_{km}} \quad (13)$$

Таблица 9 – Нарастание технической готовности работы и удельный вес каждого этапа.

Этап разработки	$ТР_i$, р.д.	$СГ_i$, %
Постановка целей и задач, сбор первоначальной информации	6,2	3,35695
Планирование и технико-экономическое обоснование ВКР	3,1	1,67847
Анализ опасных и вредных производственных факторов	1,5	0,83924
Составление и согласование технического задания	6,5	3,53134
Анализ предметной области и сбор необходимой информации	8,6	4,67575
Анализ существующих разработок	2	1,07902
Анализ существующих сканеров отпечатков	11,9	6,47411

Этап разработки	$ТР_i$, р.д.	$СГ_i$, %
Выбор сканера отпечатков	46	25,0681
Проектирование модели	26,9	14,6594
Разработка модели	30,9	16,8501
Тестирование модели	15,5	8,47956
Составление и оформление пояснительной записки	24,4	13,3079
Итого	183,5	100

6.2 Расчет сметы затрат на выполнение проекта

В состав затрат на создание проекта включается стоимость всех расходов, необходимых для реализации проекта. Расчет сметной стоимости на выполнение данной разработки производится по следующим статьям затрат:

— заработная плата;
— социальный налог;
— расходы на электроэнергию (без освещения);
— амортизационные отчисления;
— командировочные расходы;
— оплата услуг связи;
— арендная плата за пользование имуществом;
— прочие услуги (сторонних организаций);
— прочие (накладные расходы) расходы.

6.2.1Расчет заработной платы

Данная статья расходов включает заработную плату руководителя и исполнителя. Расчет основной заработной платы выполняется на основе трудоемкости выполнения каждого этапа и величины месячного оклада исполнителя, а также премии, входящие в фонд заработной платы. Расчет

основной заработной платы выполняется на основе трудоемкости выполнения каждого этапа и величины месячного оклада исполнителя.

Среднедневная тарифная заработная плата ($ЗП_{дн-т}$) рассчитывается по формуле:

$$ЗП_{дн-т} = МО/24,83 \quad (14)$$

где МО – месячный оклад.

Расчеты затрат на полную заработную плату приведены в таблице 5. Для учета в ее составе премий, дополнительной зарплаты и районной надбавки используется следующий ряд коэффициентов: $К_{ПР} = 1,1$; $К_{доп.ЗП} = 1,188$; $К_р = 1,3$. Таким образом, для перехода от тарифной (базовой) суммы заработка исполнителя, связанной с участием в проекте, к соответствующему полному заработку (зарплатной части сметы) необходимо первую умножить на интегральный коэффициент $К_и$ = 1,1* 1,188*1,3 = 1,699. Вышеуказанное значение $К_{доп.ЗП}$ применяется при шестидневной рабочей неделе, при пятидневной оно равно 1,113, соответственно в этом случае $К_и = 1,62$.

Таблица 10 – Затраты на заработную плату

Исполнитель	Оклад, руб./мес.	Среднедневная ставка,руб./раб.день	Затраты времени,раб.дни	Коэффициент	Фонд з/платы, руб.
НР	23 264,86	936,9657672	67,7	1,699	107 771,96
И	14 874	684,81	115,8	1,62	128 466,98
Итого:					236 238,94

6.2.2Расчет затрат на социальный налог

Затраты на единый социальный налог (ЕСН), включающий в себя отчисления в пенсионный фонд, на социальное и медицинское страхование, составляют 30 % от полной заработной платы по проекту, т.е. $С_{соц.} = С_{зп}$*0,3. Итак, в нашем случае $С_{соц.}$ = 220 151,63* 0,3 = 66045,489 руб.

6.2.3Расчет затрат на электроэнергию

Данный вид расходов включает в себя затраты на электроэнергию, потраченную в ходе выполнения проекта на работу используемого оборудования, рассчитываемые по формуле:

$$C_{эл.об.} = P_{об} t_{об} Ц_Э \quad (15)$$

где $P_{ОБ}$ – мощность, потребляемая оборудованием, кВт;

$Ц_Э$ – тариф на 1 кВт·час;

$t_{об}$ – время работы оборудования, час.

Для ТПУ $Ц_Э$ = 5,782 руб./квт·час (с НДС).

Время работы оборудования вычисляется на основе итоговых данных таблицы 6 для инженера ($T_{РД}$) из расчета, что продолжительность рабочего дня равна 8 часов.

$$t_{об} = T_{РД} * К_t, \quad (16)$$

где $К_t \leq 1$– коэффициент использования оборудования по времени, равный отношению времени его работы в процессе выполнения проекта к $T_{РД}$, определяется исполнителем самостоятельно. В ряде случаев возможно определение $t_{об}$ путем прямого учета, особенно при ограниченном использовании соответствующего оборудования.

Мощность, потребляемая оборудованием, определяется по формуле:

$$P_{ОБ} = P_{ном.} * К_С \quad (17)$$

где $P_{ном.}$ – номинальная мощность оборудования, кВт;

$K_С \leq 1$ – коэффициент загрузки, зависящий от средней степени использования номинальной мощности. Для технологического оборудования малой мощности $K_С = 1$.

Пример расчета затраты на электроэнергию для технологических целей приведен в таблице 11.

Таблица 11 – Затраты на электроэнергию технологическую

Наименование оборудования	Время работы оборудования tОБ, час	Потребляемая мощность РОБ, кВт	Затраты ЭОБ, руб.
Персональный компьютер	Трд*Кт = (115,8+67,7)*8*0,6=878,4	0,3	1527,84
Сетевое оборудование		0,1	509,28
Итого			2037,11

6.2.4Расчет амортизационных расходов

В главе «Расчет амортизационных расходов» рассчитывается амортизация используемого оборудования за время выполнения проекта.

Амортизационные отчисления рассчитываются на время использования ЭВМ по формуле:

$$C_{\text{АМ}} = \frac{\text{Н}_\text{А} \cdot \text{Ц}_\text{ОБ}}{F_\text{Д}} \cdot t_{\text{ВТ}} \cdot n, \quad (18)$$

где $\text{Н}_\text{А}$ – годовая норма амортизации, $\text{Н}_\text{А}$ = 40%;

$\text{Ц}_\text{ОБ}$ – цена оборудования, $\text{Ц}_\text{ОБ}$ = 45000 руб.;

$F_\text{Д}$ – действительный годовой фонд рабочего времени, $F_\text{Д}$ = 298 * 8 = 2384 часа;

Срок реализации программного проекта – 4 месяца (февраль, март, апрель, май) или 99 день. Количество рабочих дней, согласно календарю, на 2017 год: февраль – 23, март – 26, апрель – 25, май – 25.

$t_{\text{ВТ}}$ – время работы вычислительной техники при создании программного продукта, $t_{\text{ВТ}}$ =99*8=792 часа;

n – число задействованных ПЭВМ, n = 1.

Итак, затраты на амортизационные отчисления составили:

$$\text{Сам} = \frac{0{,}4 * 45000}{2384} * 792 * 1 = 5979{,}9$$

6.2.5Расчет прочих расходов

В статье «Прочие расходы» отражены расходы на выполнение проекта, которые не учтены в предыдущих статьях, их следует принять равными 10% от суммы всех предыдущих расходов, т.е.

$C_{проч.} = (C_{мат} + C_{зп} + C_{соц} + C_{эл.об.} + C_{ам} + C_{нп})*0,1$

Для нашего примера это

$C_{проч.} = (220\ 151,63+66045,489 +1850,13 + 5979,9)*0,1 = 35313$ руб.

6.2.6Расчет общей себестоимости разработки

Таким образом, на основании проведенных ранее подсчетов по отдельным статьям затрат вычислим общую плановую себестоимость разработки алгоритма идентификации по биометрическим параметрам.

Таблица 12 – Смета затрат на разработку проекта

Статья затрат	Условное обозначение	Сумма, руб.
Основная заработная плата	$C_{зп}$	220 151,63
Отчисления в социальные фонды	$C_{соц}$	66045,489
Расходы на электроэнергию	$C_{эл.}$	1850,13
Амортизационные отчисления	$C_{ам}$	5979,9
Прочие расходы	$C_{проч}$	35313
Итого:		329 340,15

Таким образом, затраты на разработку составили C = 329 340,15 руб.

6.2.7Расчет прибыли

Прибыль от реализации проекта в зависимости от конкретной ситуации (масштаб и характер получаемого результата, степень его определенности и коммерциализации, специфика целевого сегмента рынка и т.д.) может определяться различными способами. Если исполнитель работы не располагает данными для применения «сложных» методов, то прибыль следует принять в

размере 5 ÷ 20 % от полной себестоимости проекта. В нашем примере она составляет 65868,03 руб. (20 %) от расходов на разработку проекта.

6.2.8Расчет НДС

НДС составляет 18% от суммы затрат на разработку и прибыли. В нашем случае это (329340,15 + 65868,03) * 0,18 = 71137,5руб.

6.2.9Цена разработки НИР

Цена равна сумме полной себестоимости, прибыли и НДС, в нашем случае

$Ц_{НИР(КР)}$ = 329340,15 + 65868,03+ 71137,5=466345,68 руб.

6.3 Оценка экономической эффективности проекта

Разработка алгоритма идентификации сотрудника по биометрическим параметрам при прохождении предсменного и послесменного осмотра с использованием системы мониторинга состояния здоровья «ЮМС Диагностический шлюз» от компании ООО «ЮМССофт» была необходима для расширения возможности идентификации сотрудников. Оценка экономической эффективности данного проекта затруднительна, так как численно посчитать экономический эффект не предоставляется возможным в рамках данной магистерской диссертации. Экономический эффект является косвенным, так как добавление нового способа идентификации не повлияет на работу диагностического шлюза. Данный метод идентификации позволит уйти от идинтификационных кодов и медицинских карт, тем самым сократит время прохождения идентификации в системе.

6.4 Оценка научно-технического уровня НИР

Научно-технический уровень характеризует влияние проекта на уровень и динамику обеспечения научно-технического прогресса в данной области. Для оценки научной ценности, технической значимости и эффективности, планируемых и выполняемых НИР, используется метод балльных оценок. Балльная оценка заключается в том, что каждому фактору по принятой шкале присваивается определенное количество баллов. Обобщенную оценку проводят по сумме баллов по всем показателям. На ее основе делается вывод о целесообразности НИР.

Сущность метода заключается в том, что на основе оценок признаков работы определяется интегральный показатель (индекс) ее научно-технического уровня по формуле:

$$K_{\text{НТУ}} = \sum_{i=1}^{3} R_i \cdot n_i, \qquad (19)$$

где $I_{\text{НТУ}}$ – интегральный индекс научно-технического уровня;

R_i – весовой коэффициент i-го признака научно-технического эффекта;

n_i – количественная оценка i-го признака научно-технического эффекта, в баллах.

Таблица 13 – Весовые коэффициенты признаков НТУ

Признаки научно-технического эффекта НИР	Характеристика признака НИР	Ri
Уровень новизны	Систематизируются и обобщаются сведения, определяются пути дальнейших исследований	00,4
Теоретический уровень	Разработка способа (алгоритм, программа мероприятий, устройство, вещество и т.п.)	00,1
Возможность реализации	Время реализации в течение первых лет	00,5

Таблица 14 – Баллы для оценки уровня новизны

Уровень новизны	Характеристика уровня новизны – n_1	Баллы
Принципиально новая	Новое направление в науке и технике, новые факты и закономерности, новая теория, вещество, способ	8 – 10
Новая	По-новому объясняются те же факты, закономерности, новые понятия дополняют ранее полученные результаты	5 – 7
Относительно новая	Систематизируются, обобщаются имеющиеся сведения, новые связи между известными факторами	2 – 4
Не обладает новизной	Результат, который ранее был известен	0

Таблица 15 – Баллы значимости теоретических уровней

Теоретический уровень полученных результатов – n_2	Баллы
Установка закона, разработка новой теории	10
Глубокая разработка проблемы, многоспектральный анализ взаимодействия между факторами с наличием объяснений	8
Разработка способа (алгоритм, программа и т. д.)	6
Элементарный анализ связей между фактами (наличие гипотезы, объяснения версии, практических рекомендаций)	2
Описание отдельных элементарных факторов, изложение наблюдений, опыта, результатов измерений	0,5

Таблица 16 – Возможность реализации результатов по времени

Время реализации – n_3	Баллы
В течение первых лет	10
От 5 до 10 лет	4
Свыше 10 лет	2

Так как все частные признаки научно-технического уровня оцениваются по 10-балльной шкале, а сумма весов Ri равна единице, то величина интегрального показателя также принадлежит интервалу [0, 10]. В таблице 17 указано соответствие качественных уровней НИР значениям показателя.

Таблица 17 – Соответствие качественных уровней НИР значениям показателя

Уровень НТЭ	Показатель НТЭ
Низкий	1-4
Средний	4-7
Высокий	8-10

Частные оценки уровня n_i и их краткое обоснование даны в таблице 18.

Таблица 18 – Оценки научно-технического уровня НИР

Значимость	Фактор НТУ	Уровень фактора	Выбранный балл	Обоснование выбранного балла
0,4	Уровень новизны	Относительно новая	4	Увеличение эффективности работы алгоритма
0,1	Теоретический уровень	Разработка способа	6	Идентификация по биометрическим параметрам
0,5	Возможность реализации	В течение первых лет	10	Лёгкое внедрение

Отсюда интегральный показатель научно-технического уровня для нашего проекта составляет:

$$I_{нту} = 0,4*4 + 0,1*6 + 0,5*10 = 1,6 + 0,1 + 5 = 7,2$$

Таким образом, исходя из данных таблицы 18, данный проект имеет средний уровень научно-технического эффекта.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8ВМ5Г	Шипицина Варвара Павловна

Институт	Кибернетики	**Кафедра**	ОСУ
Уровень образования	Магистр	**Направление/специальность**	09.04.01 Информатика и вычислительная техника

Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения	*В данной работе рассматривается возможность доработки системы мониторинга состояния здоровья «ЮМС Диагностический шлюз» в плане измерения температуры.*
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Производственная безопасность 1.1. Анализ выявленных вредных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности. 1.2. Анализ выявленных опасных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности. 1.3. Рекомендации по минимизации влияний	*В качестве вредных факторов выделены: шум и электромагнитное излучение. В качестве опасных: возможность поражения током и возникновение пожара, электромагнитного излучения. Приведены рекомендации по улучшению микроклимата в офисном помещении, а также рекомендации по минимизации влияния шума, электромагнитного излучения и освещения, меры по обеспечению пожарной безопасности, способы защиты отиэлектричекого тока.*
2. Экологическая безопасность:	*Деятельность организации не связана с производством, поэтому влияние на окружающую среду минимально. Рассмотрена утилизация бумажных отходов.*
3. Безопасность в чрезвычайных ситуациях:	*Наиболее типичной ЧС в офисном помещении является возникновение пожара. При хранении конфиденциальных данных в электронных таблицах можно говорить о возможности возникновения кибертерроризма. Приведены способы защиты от кибератак.*
4. Правовые и организационные вопросы обеспечения безопасности:	*Рассмотрены психофизиологические факторы, организационные мероприятия при компоновке рабочей зоны, обеспечение гарантий защиты конфиденциальных данных граждан с помощью комплекса технических и юридических мер.*

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Извеков Владимир Николаевич	к.т.н		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ5Г	Шипицина Варвара Павловна		

7 СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

Аннотация

Представление понятия «Социальная ответственность» сформулировано в международном стандарте (МС) IC CSR-08260008000: 2011 «Социальная ответственность организации».

В соответствии с МС - Социальная ответственность - ответственность организации за воздействие ее решений и деятельности на общество и окружающую среду через прозрачное и этичное поведение, которое:

— содействует устойчивому развитию, включая здоровье и благосостояние общества;

— учитывает ожидания заинтересованных сторон;

— соответствует применяемому законодательству и согласуется с международными нормами поведения (включая промышленную безопасность и условия труда, экологическую безопасность);

— интегрировано в деятельность всей организации и применяется во всех ее взаимоотношениях (включая промышленную безопасность и условия труда, экологическую безопасность).

Введение

Система мониторинга состояния здоровья ЮМС Диагностический шлюз в составе (далее по тексту - система), предназначенная для экспресс – оценки показателей здоровья и позволяющую производить бесконтактное измерение температуры тела, содержание алкоголя в парах выдыхаемого воздуха, а также частоты пульса и артериального давления, проводимые в лечебно – профилактических учреждениях, лабораториях или бытовых условиях.

Система может быть размещена преимущественно в кабинете или в кабине для диагностики или рядом с ней и работает в режиме компьютерного автоматизированного управления, ручного управления самим пациентом, или с помощью или под контролем медработника, оператора, рабочее место которого расположено вне кабины (удаленно).

В зависимости от потенциального риска применения стимулятор, в соответствии с Приказом Минздрава России № 4н от 06.06.2012 г. «Об утверждении номенклатурной классификации медицинских изделий», относится к классу **2а.**

По климатическому исполнению, система относится к группе УХЛ 4.2 по ГОСТ 15150.

Класс безопасности программного обеспечения А по ГОСТ Р МЭК 62304.

Пример условного обозначения системы при заказе: «Система мониторинга состояния здоровья «ЮМС Диагностический шлюз» по ТУ 9441-001-97579107-2016 в составе».

7.1 Описание рабочего места

Правила и порядок безопасной работы с ЭВМ описаны санитарными правилами и нормами СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [33].

Рабочий кабинет, располагается на первом этаже здания. Кабинет представляет собой комнату длиной – 6 м, шириной – 5 м и высотой – 3 м. Естественное освещение кабинета осуществляется посредством двух окон размерами 2 м х 1 м каждое. Дверь – деревянная, коричневая. Высота двери – 2 м, ширина - 1 м. Стены комнаты окрашены водоэмульсионной краской. Цвет стен – бежевый. Потолок подвесной открытого кассетного типа со встроенными светильниками. Пол покрывает линолеум светло -коричневого цвета. Площадь кабинета составляет 30 м^2, объем – 90 м^3.

Помещение оборудовано на десять рабочих мест. Пункт 3.4 СанПиН 2.2.2/2.4.1340-03[33]. определяет требования к минимальной площади и объему на одно рабочее место. Согласно СанПиН 2.2.2/2.4.1340-03 при периметральном расположении рабочих мест площадь одного рабочего места должна составлять не менее 4,0 кв.м. Для данного помещения эти требования выполнены.

Согласно п.9.1 СанПиН 2.2.2/2.4.1340-03 [33], расстояние между столами с видеомониторами (во фронтальной плоскости) должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов должно быть не менее 1,2 м. Расстояние между столами 3 м, между боковыми поверхностями видеомониторов 1,5 м. Требования пункта 9.1 СанПиН 2.2.2/2.4.1340-03 выполняются.

7.2 Производственная безопасность

В данном пункте анализируются вредные и опасные факторы, которые могут возникать при разработке или эксплуатации проектируемого решения.

Для выбора факторов необходимо использовать ГОСТ 12.0.003-74 «Опасные и вредные производственные факторы. Классификация». Перечень опасных и вредных факторов, характерных для проектируемой производственной среды необходимо представить в виде таблицы. Таблица составляется индивидуально для каждой ВКР с соответствующим диплому заголовком, например:

Таблица 19 – Основные элементы производственного процесса, формирующие опасные и вредные факторы согласно ГОСТ 12.0.003-74 ССБТ [34].

Наименование видов работ и параметров производственного процесса	Факторы	
	Вредные	Опасные
Разработка программного обеспечения	Недостаточная освещенность рабочей зоны. Превышение уровней шума. Отклонение показателей микроклимата в помещении. Электромагнитное излучение.	Поражение электрическим током

7.2.1Анализ вредных и опасных факторов, которые может создать объект исследования

Данная разработка может повлечь способствовать появление такого опасного фактора как поражение электрическим током.

Электрические установки, к которым относятся оборудования ЭВМ, представляет потенциальную опасность для человека [35].

В рабочих кабинетах выполняются такие защитные меры как защитное заземление, зануление, защитное отключение, электрическая изоляция токоведущих частей, малое напряжение. Защитные меры должны обеспечивать напряжение прикосновения не выше 42В – в помещении без повышенной опасности и с повышенной опасностью. Рабочее место относятся к помещениям без повышенной опасности, согласно ПУЭ [35].

Питание оборудования осуществляется от сети напряжением 220В при частоте 50Гц. Сопротивление изоляции должно быть не менее 0.5мОм.

Токи статического электричества возникают при прикосновении персонала к любому из элементов ЭВМ. Также статическое электричество существует вблизи экрана дисплея, но электроопасности не несет.

Создание прочих вредных и опасных факторов объектом исследования исключено.

7.2.2Анализ вредных и опасных факторов, которые могут возникнуть при проведении исследований

7.2.2.1 Освещение

Освещение – получение, распределение и использование световой энергии для обеспечения благоприятных условий видения предметов и объектов [36].

Правильное освещение является основным фактором, соблюдение которого требуется для снижения развития профессиональных болезней при работе с ПЭВМ и увеличения работоспособности. Условия деятельности операторов в системе «человек – машина» связаны с явным преобладанием зрительной информации – до 90% общего объема.

В рабочем помещении используется система комбинированного освещения. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения [36].

Естественное освещение должно осуществляться через боковые светопроемы ориентированные преимущественно на север и северо-восток. Величина коэффициента естественной освещенности (КЕО) должна соответствовать нормативным уровням по СНиП 23-05-95 "Естественное и искусственное освещение" [36] и создавать КЕО не ниже 1,2% в зонах с устойчивым снежным покровом и не ниже 1,5% на остальной территории.

Схема расположения светильников представлена на рисунке 16.

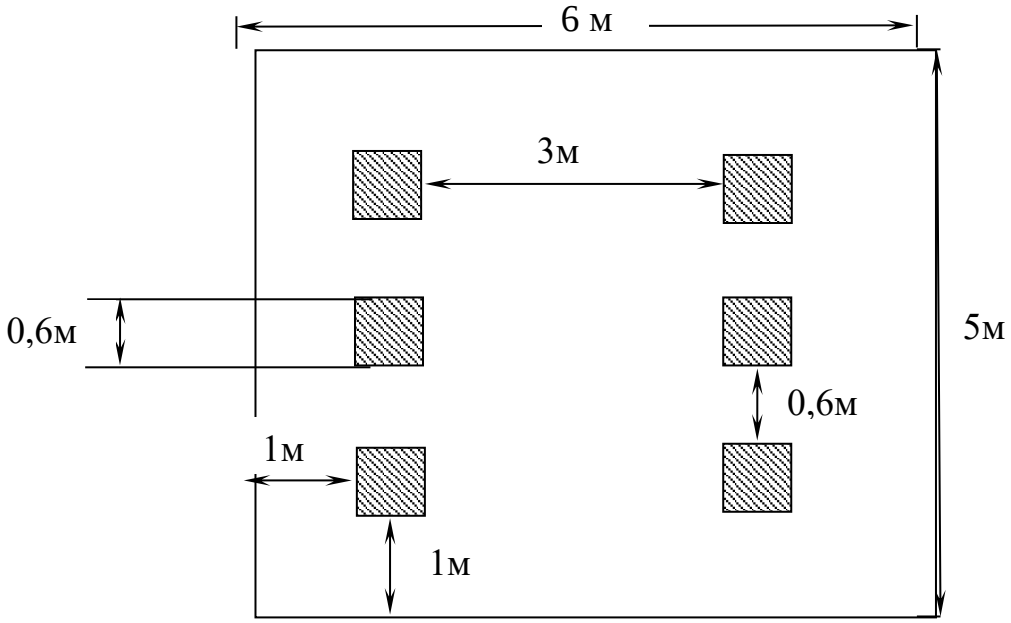


Рисунок 16 — Схема освещения

В помещении установлены светильники типа ARS/R 418, укомплектованные четырьмя люминесцентными лампами мощностью 20 Вт. Геометрические размеры светильников 595х595х36 мм, $\lambda = 1,4$. Учитывая, что в каждом светильники установлено по 4 лампы, количество ламп составит N = 24.

Согласно СНиП 23-05-95 [37] норма освещённости рабочих поверхностей в помещениях для работы с дисплеями и видеотерминалами принимается $E_н$ = 200лк.

Фактическая освещенность определяется по формуле:

$$E_ф = (N \cdot n \cdot Ф_{ст} \cdot \eta) / (S \cdot K_з \cdot Z) \quad (20)$$

где S – площадь освещаемого помещения, м^2;

$K_з$ – коэффициент запаса, учитывающий загрязнение светильника;

$Ф_{ст}$ - световой поток люминесцентных ламп, лм;

Z – коэффициент неравномерности освещения, отношение $E_{ср.}/E_{min}$.

N – число светильников;

n – число ламп в светильнике;

η - коэффициент использования светового потока, %.

Для определения коэффициента использования светового потока необходимо найти индекс помещения. Индекс помещения определяется по формуле:

$$i = S/h*(A+B) \quad (21)$$

где h - высота помещения;

S - площадь помещения;

A – ширина помещения;

B – длина помещения.

Длина помещения B составляет 6 метров, ширина A – 5 м, высота h – 3 м.

Находим индекс помещения по формуле 21:

$$i = 30/3 *(6+5) = 0,91$$

Зная индекс помещения i, коэффициент отражения светлых стен $\rho_c = 50\%$ и светлого потолка $\rho_п=70\%$, определим коэффициент использования светового потока из таблицы, взятой из СНиП 23-05-95, $\eta = 0,49$ [37].

Коэффициент неравномерности освещения *Z* принимается в пределах 1.1-1.2, в данной работе примем $Z = 1.1$. Коэффициент запаса определяется по таблице из СНиП 23-05-95 [36]. в зависимости от характеристик помещения, в нашем случае $K = 1.5$. Световой поток люминесцентных ламп типа ЛБ с мощностью 20 Вт согласно таблицы из СНиП 23-05-95 [36] составляет 1060 лк.

Фактическая освещенность:

$$E_ф = \frac{6*4*1060*0,49}{30*1,5*1,1} = 251,83 \text{ лк.}$$

Отклонение от нормы ΔE рассчитываются по формуле:

$$\Delta E = ((E_ф - E_н) / E_н)*100 \quad (22)$$

$\Delta E = ((251,83 - 200) / 200)*100 = 25.9\%$

Фактическое значение освещенности выше нормативного. Установка местного освещения не требуется.

7.2.2.2 Шум

Шум - звук, мешающий разговорной речи и негативно влияющий на здоровье человека [38].

Шум ухудшает условия труда, что сказывается на качестве работы. Оказывает вредное действие на организм человека, вызывая раздражительность, головные боли, головокружение, ухудшение памяти, повышенную утомляемость, понижение аппетита, боли в ушах и т. д.

В офисах источниками шума являются печатающие устройства, множительная техника и кондиционеры. Сами ПЭВМ также производят шум, а именно вентиляторы систем охлаждения.

В производственных помещениях при выполнении основных или вспомогательных работ с использованием ПЭВМ уровни шума на рабочих местах не должны превышать предельно допустимых значений, установленных соответствующими нормами СНиП 2.2.4/2.1.8.562-96 [39].

В таблице 20 указаны допустимые уровни звука для работы программиста, являющиеся безопасными в отношении сохранения здоровья и работоспособности.

Таблица 20 – Допустимые уровни звука, дБ, на рабочих местах

Вид трудовой деятельности, рабочее место	Уровни звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц									Уровни звука и эквивалентного звука (в дБА)
	1,5	3	25	50	00	000	000	000	000	
Конструкторские бюро, программисты, лаборатории	6	1	1	4	9	5	2	0	8	5 0

7.2.2.3 Микроклимат

Микроклимат производственных помещений – климат внутренней среды этих помещений, который определяется действующими на организм человека сочетаниями температуры, влажности и скорости движения воздуха, а также интенсивности теплового излучения от нагретых поверхностей [39].

Необходимо определим следующие параметры: температура, относительная влажность и скорость движения воздуха. Оптимальные значения характеристик микроклимата согласно, СанПиН 2.2.4.548-96 [40] устанавливаются в соответствии с категорией работ (программист – легкая, 1а и 1б) и приведены в таблице 21.

Таблица 21 – Оптимальные значения характеристик микроклимата

Сезон года	Температура воздуха, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	22 - 24	40 - 60	до 0,1
Теплый	23 - 25	40 - 60	до 0,2

7.2.2.4 Электромагнитное излучение

Повышенный уровень электромагнитного излучения обусловлен большим количеством компьютерной техники в помещении. Источниками электромагнитного излучения являются электрические сигналы цепей при работе компьютера. Электромагнитные излучения очень низкой и сверхнизкой частоты, создаваемые ПЭВМ и другой оргтехникой, негативно влияют на здоровье человека. Наибольшее воздействие на программиста оказывает дисплей ПЭВМ. Малые дозы облучения могут привести к раковым заболеваниям, нарушениям нервной, эндокринной и сердечно-сосудистых систем. Временные допустимые уровни электромагнитных полей, создаваемых ПВЭМ указаны в таблице 22 [34].

Таблица 22 – Временные допустимые уровни ЭМП, создаваемых ПЭВМ на рабочих местах

Наименование параметров		ВДУ
Напряженность электрического поля	в диапазоне частот 5 Гц - 2 кГц	25 В/м
	в диапазоне частот 2 кГц - 400 кГц	2,5 В/м
Плотность магнитного потока	в диапазоне частот 5 Гц - 2 кГц	250 нТл
	в диапазоне частот 2 кГц - 400 кГц	25 нТл
Напряженность электростатического поля		15 кВ/м

7.2.3Обоснование мероприятий по защите исследователя от действия опасных и вредных факторов

Для обеспечения электробезопасности при эксплуатации ЭВМ с ВДТ и ЧП необходимо соблюдать следующие требования:

— в помещении, где одновременно эксплуатируются более пяти ЭВМ с ВДТ и ЧП, на видном и доступном месте устанавливается аварийный резервный выключатель, который может полностью отключить электропитание помещения, кроме освещения;

— ЭВМ с ВДТ и ПП должны подключаться к электросети только с помощью исправных штепсельных соединений и электророзеток заводского изготовления;

— не допускается подключать ЭВМ с ВДТ и ЧП к обычной двухпроводной электросети, в том числе - с использованием переходных устройств;

— электросети штепсельных соединений и электророзеток для питания ЭВМ с ВДТ и ЧП нужно выполнять по магистральной схеме, по 3-6 соединений или электророзеток в одном круге [41].

Для уменьшения уровня шума нужно производить регулярный осмотр и чистку вентиляторов в ПЭВМ, закрывать системный блок (это также

способствует соблюдению техники безопасности). Помещение может быть отделано с применением звукопоглощающих материалов.

Микроклимат помещения поддерживается на оптимальном уровне системой водяного центрального отопления, естественной вентиляцией, а также искусственным кондиционированием в теплое время года и дополнительным прогревом в холодное время года. В помещениях также должно проводиться систематическое проветривание после каждого часа работы на ПЭВМ.

7.3 Экологическая безопасность

Общие требования к хозяйственной и иной деятельности, оказывающей вредное воздействие на атмосферный воздух регламентированы Федеральным законом "Об охране атмосферного воздуха" статья 15 [42].

Требования охраны атмосферного воздуха при проектировании, размещении, строительстве, реконструкции и эксплуатации объектов хозяйственной и иной деятельности указаны в статье 16 СанПиН 2.2.1/2.1.1.1200-03 [43].

В качестве промышленных отходов выступают: бумага, картон. Предприятие решает проблему отходов, в основной массе это бумага, путем сдачи их в пункты сбора вторичного сырья для дальнейшей переработки.

Потребляемая производством вода используется в качестве источника питьевого и хозяйственно-бытового водопользования согласно СанПиН 2.1.5.980-00 2.1.5 [44], поэтому дополнительной очистки перед отводом в канализацию не требуется. Сточные воды поступают на комплексные очистные сооружения, где очищаются и сбрасываются в водоём.

В случае выхода из строя компьютера происходит его списание и отправка на специальный склад, который при необходимости принимает меры по утилизации списанной техники и комплектующих.

Современные энергосберегающие лампочки, также как и другие люминесцентные лампы при разрушении представляют серьезную угрозу для

окружающей среды и человека. Пары ртути очень ядовиты и вызывают тяжелое отравление организма, поражают клетки центральной нервной системы, другие органы и приводят к тяжелым заболеваниям [44].

Люминесцентные лампы должны быть подвергнуты особому процессу транспортирования и утилизации, согласно ГОСТ 6825-91 [45]. Для этого организуется их прием специальными организациями, и производятся централизованная утилизация люминесцентных ламп на отведенных для этого полигонах [44].

7.4 Безопасность в чрезвычайных ситуациях

Чрезвычайная ситуация (ЧС) – обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей [46].

Чрезвычайные ситуации, которые могут возникнуть при работе на предприятии, классифицируются на [47]:

— техногенные: взрывы, пожары, обрушение помещений, аварии на системах жизнеобеспечения;

— природные: наводнения, ураганы, бури, природные пожары;

— экологические: разрушение озонового слоя, кислотные дожди;

— биологические: эпидемии, пандемии;

— антропогенные: война, терроризм.

7.4.1Анализ вероятных ЧС, которые могут возникнуть при исследовании объекта

Рассмотрим пожар, как наиболее вероятную чрезвычайную ситуацию техногенного характера на производстве.

Пожарная безопасность представляет собой единый комплекс организационных, технических, режимных и эксплуатационных мероприятий по предупреждению пожаров и взрывов. Так как пожар является одним из наиболее вероятных чрезвычайных ситуаций, то помещения должны быть обеспечены всем необходимым для быстрой локализации и/или уничтожения очага.

Согласно ППБ-105-03, помещение, в котором ведется работа, по степени пожарной опасности относится к категории Д - помещения, в которых находятся негорючие вещества и материалы в холодном состоянии [48].

Возможными источниками и причинами пожара в помещении являются:

— короткое замыкание в электропроводке вследствие неисправности самой проводки или электрораспределительных щитов;

— неисправная аппаратура;

— нарушение правил пожарной безопасности работниками.

7.4.2Обоснование мероприятий по предотвращению ЧС и разработка порядка действия в случае возникновения ЧС

Профилактические методы борьбы с пожарами в помещении предусматривают:

— организационные: обучение и разработка планов эвакуации, содержание помещений в должном состоянии и другое;

— технические: современные автоматические средства сигнализации, методы и устройства ограничения распространения огня, автоматические стационарные системы тушения пожаров, огнетушители.

Помещение оснащено пороговой пожарной сигнализацией и знаками пожарной безопасности, согласно ГОСТ Р 12.4.026-2001 [49]. Общие требования

к знакам пожарной безопасности регламентированы нормами пожарной безопасности [18].

На рисунке 17 показан план эвакуации этажа с размещенными средствами пожаротушения.

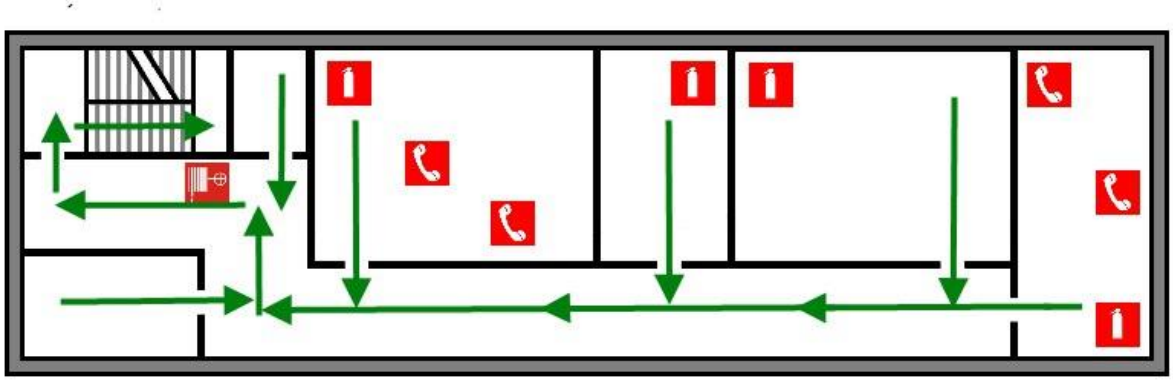


Рисунок 17 — План эвакуации ООО «ЮМССофт»

Основные способы пожаротушения:

— охлаждение очага горения или горящего материала ниже определенных температур;

— изоляция очага горения от воздуха или снижение концентрации кислорода в воздухе путем разбавления негорючими газами;

— механический срыв пламени сильной струей воды или газа; торможение (ингибирование) скорости реакции окисления;

— создание условий огнепреграждения, при которых пламя распространяется через узкие каналы, сечение которых ниже установленного диаметра.

К средствам тушения относятся огнетушащие вещества и составы. В качестве средств тушения используют воду, пены (воздушно-механические различной кратности и химические), представляющие собой коллоидные системы, состоящие из пузырьков воздуха или диоксида углерода; инертные газовые разбавители (диоксид углерода, азот, аргон, водяной пар, дымовые газы); гомо- геновые ингибиторы, низкокипящие гологеноуглероды-хлодоны;

гетерогенные ингибиторы — огнетушащие порошки; комбинированные составы.

Для тушения электроустановок под напряжением используются хладоны, порошки, диоксид углерода.

7.5 Правовые и организационные вопросы обеспечения безопасности

Работа программиста является монотонной, сидячей и умственной. Умственное перенапряжение, перенапряжение анализаторов, монотонность труда, эмоциональные перегрузки относятся к психофизиологическим вредным факторам. Их влияние следует уменьшать для поддержания качества работы сотрудника и уменьшения его утомляемости.

Организация работы с ПЭВМ должна осуществляться в зависимости от вида и категории трудовой деятельности. Для предупреждения преждевременной утомляемости пользователей ПЭВМ рекомендуется организовывать рабочую смену путем чередования работ с использованием ПЭВМ и без него, постоянно менять задачи и нагрузки. Во время регламентированных перерывов с целью снижения нервно-эмоционального напряжения, утомления зрения, устранения влияния гиподинамии целесообразно выполнять комплексы упражнений.

Для обеспечения оптимальной работоспособности и сохранения здоровья пользователя в течение рабочего дня необходимо проводить перерывы. Время перерывов для различных категорий работы с ПЭВМ в течение рабочего дня, согласно СанПиН 9-131 РБ, представлены на рисунке 18.

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

Рисунок 18 – Суммарное время регламентированных перерывов в зависимости от продолжительности работы, вида и категории трудовой деятельности с ПЭВМ.

В промышленных помещений необходимо соблюдать нормы полезной площади для сотрудников. Площадь на одно рабочее место с ПЭВМ для взрослых пользователей, согласно СанПиН 2.2.2/2.4.1340-03 [41], должна составлять не менее 4,0 кв.м. Данные требования в рабочем помещении соблюдены.

При организации рабочего места необходимо произвести требования эргономики, т.е. учитывать факторы, которые влияют на эффективность действий человека при обеспечении безопасных условий работы. Оптимальная планировка обеспечивает экономию сил и времени человека, удобство при выполнении работы [49].

Для профилактики производственных заболеваний следует соблюдать следующие правила:

— при работе с клавиатурой, угол сгиба руки в локте должен быть прямым (90 градусов);

— при работе с мышкой кисть должна быть прямой, и лежать на столе как можно дальше от края;

— стул или кресло должно быть с подлокотниками, так же желательно наличие специальной выпуклости для запястья (коврик для «мыши», специальной формы клавиатура или компьютерный стол с такими выпуклостями) [50].

ЗАКЛЮЧЕНИЕ

В ходе исследования были рассмотрена биометрические параметры человека, существующие способы и методы идентификации людей. Рассмотрены существующие типы сканеров отпечатков пальцев, и ключевые виды сканеров.

Был проведен анализ существующей архитектуры программно-аппаратного комплекса «ЮМС Диагностический шлюз», также было предложено решение по изменению архитектуры, включению новых компонентов.

Было подготовлено предложение по изменению бизнес-процесса прохождения идентификации сотрудников, рассмотрено финансовое обоснование проведения исследования, а также факторы, влияющие на магистра в ходе проведения исследования.

СПИСОК ЛИТЕРАТУРЫ

1) Biometrics Researcher Asks: Is That Eyeball Dead or Alive? [Электронный ресурс] / IEEE Spectrum: Technology, Engineering, and Science News. - Электрон. дан., URL: http://spectrum.ieee.org/the-human-os/biomedical/imaging/biometric-researcher-asks-is-that-eyeball-alive-or-dead, свободный. – Яз. англ.

2) Биометрические системы безопасности. [Электронный ресурс] / БДИ №1(41); ред. М. Попов; - Электрон. дан., URL: http://www.bre.ru/security/12571.html. свободный. – Яз.рус.

3) Р. М. Болл, Руководство по биометрии / Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. — М.; Техносфера, 2007. – 368 с.

4) ГОСТ Р ИСО/МЭК 19794-4-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. 2006 – 24 с.

5) Алексеев В.Н. Глава 2. Анатомия органа зрения / Астахов Ю.С., Басинский С.Н., Е.А.Егоров — М.: ГЭОТАР-Медиа: Офтальмология: Учебник для студ. мед. Вузов, 2008. — 240 с.

6) Anil Jain Biometrics Personal Identification in Networked Society / Ruud Bolle, Sharath Pankanti — Springer Science & Business Media: Recognising Persons by Their Iris Patterns, 2006. — 411 p.

7) Khalid Saeed Iris Pattern Recognition with a New Mathematical Model to Its Rotation Detection / Tomomasa Nagashima. — Springer Science & Business Media: Biometrics and Kansei Engineering, 2012. — 276 p.

8) J. Daugman How iris recognition works. – Transactionson Circuits and Systems for Video Technology, 2004.

9) Биометрические методы компьютерной безопасности [Электронный ресурс] / BYTE; ред. Шаров В. - Электрон. дан., URL: https://www.bytemag.ru/articles/detail.php?ID=6719. свободный. – Яз. рус.

10) Идентификация по почерку [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.biolink.ru/technology/handwriting.php. – Яз. рус

11) Биометрический контроль доступа [Электронный ресурс] / BioLink - Электрон. дан., URL: http://www.techportal.ru/glossary/biomet-kontrol-dostupa.html. свободный. – Яз. рус.

12) What’s the Difference Between Match-on-Host and Match-in-Sensor Fingerprint Authentication? [Электронный ресурс] / Anthony Gioeli. - Электрон. дан., URL: http://www.electronicdesign.com/embedded/what-s-difference-between-match-host-and-match-sensor-fingerprint-authentication. свободный. – Яз. англ.

13) Information Technology - Finger Minutiae Format for Data Interchange - Amendment 1INCITS 378. 2009

14) Подделка отпечатков пальцев [Электронный ресурс] / Techportal - Электрон. дан., URL: http://www.techportal.ru/glossary/poddelka-otpechatkov-palcev.html. свободный. – Яз. рус.

15) Идентификация по отпечаткам пальцев. Часть 1. [Электронный ресурс] / Институт экономической безопасности - Электрон. дан., ред. В. Задорожный. URL:http://www.bre.ru/security/20994.html. свободный. – Яз. рус.

16) BioLink U-Match BI USB [Электронный ресурс] / BioLink - Электрон. дан., URL: http://www.biolink.ru/products/scanners/emb/usb.php. свободный. – Яз. рус.

17) BioLink S-Match 4F [Электронный ресурс] / BioLink- Электрон. дан., URL:http://www.biolink.ru/products/scanners/special/umatch_4f.php. свободный. – Яз. рус.

18) BioLink S-Match 2F [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.biolink.ru/products/scanners/special/umatch_2f.php. свободный. – Яз. рус.

19) BioLink CI [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.biolink.ru/products/biolink-ci-system. свободный. – Яз. рус.

20) BioLink S-Match 1F [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.biolink.ru/products/scanners/special/umatch_1f.php. свободный. – Яз. рус.

21) BioLink U-Match BI Ethernet [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.hardbroker.ru/catalog/producs/view/90/. свободный. – Яз. рус.

22) Синергет STS-715 (Ethernet) [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.sinerget.ru/ru/hardware/17/sts-715. свободный. – Яз. рус.

23) Futronic FS-84 [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.futronic-tech.com/product_fs84.html. свободный. – Яз. англ.

24) Futronic FS88 OEM module (FS 89) [Электронный ресурс] / BioLink- Электрон. дан., URL: https://www.fulcrumbiometrics.com/Futronic-FS88-OEM-p/101114.htm. свободный. – Яз. англ.

25) Futronic FS88H [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.futronic-tech.com/product_fs88h.html. свободный. – Яз. англ.

26) Futronic FS26 [Электронный ресурс] / BioLink- Электрон. дан., URL: http://www.futronic-tech.com/product_fs26.html. свободный. – Яз. англ.

27) Идентификация по отпечаткам пальцев. Часть 2. [Электронный ресурс] / Институт экономической безопасности - Электрон. дан., ред. В. Задорожный. URL:http://www.bre.ru/security/20994.html. свободный. – Яз. рус.

28) Плюсы и минусы использования биометрии [Электронный ресурс] / CNews - Электрон. дан., ред. Д. Кондратьев. URL: http://www.cnews.ru/reviews/free/techsec2006/articles/plus_biometry.shtml. свободный. – Яз. рус.

29) Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ. 2006 – 21с.

30) Современные технологии идентификации личности по отпечатку пальца с использованием емкостных датчиков [Электронный ресурс] /

RadioRadar.net; ред. Рябов Г. В.; URL:http://www.radioradar.net/articles/scientific_technical. свободный. – Яз. рус.

31) Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека. СПб: Политехника, 2004 – 204с.

32) Огнев А. В., Центрирование отпечатков пальцев при инвариантном распознавании на основе метрики Хаусдорфа. Типикин А. П. Курск: КурскГТУ: Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации, 2008. С. 34—35.

33) СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы: с изменениями от 25 апреля 2007 г. – М.: Информационно-издательский центр Минздрава России, 2003.

34) ГОСТ 12.0.003-74 ССБТ Опасные и вредные производственные факторы. Классификация. – М.: Информационно-издательский центр Минздрава России, 1974.

35) НПАОП 0.00-1.28-10 ПРАВИЛА охраны труда при эксплуатации электронно-вычислительных машин (ЭВМ, компьютеров) Охрана труда http://www.ohranatruda.in.ua/pages/184/

36) Алексеев С.В., Усенко В.Р. Гигиена труда. М.: Медицина, 1988. — 576 с.

37) СНиП 23-05-95 «Естественное и искусственное освещение» (Утверждены 02.08.1995г.);

38) СНиП 2.2.4/2.1.8.562-96 Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки. – М.: Информационно-издательский центр Минздрава России, 1996.

39) Д.А. Кривошеин. Экология и безопасность жизнедеятельности. М.: ЮНИТИ-ДАНА, 2000. - 447 с.

40) СанПиН 2.2.4.548-96 «Гигиенические требования к микроклимату производственных помещений»

41) СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы: с изменениями от 25 апреля 2007 г. – М.: Информационно-издательский центр Минздрава России, 2003.

42) Санитарные правила и нормы СанПиН 2.2.1/2.1.1.1200-03 «Санитарно-защитные зоны и санитарная классификация предприятий, сооружений и иных объектов. Санитарно-эпидемиологические правила и нормативы» (Утверждены 10.04.2003г.);

43) Санитарные правила и нормы СанПиН 2.1.5.980-00 "2.1.5. Водоотведение населенных мест, санитарная охрана водных объектов. Гигиенические требования к охране поверхностных вод" (Утверждены 22.06.2000 г.);

44) ГОСТ 30775-2001. Классификация, идентификация и кодирование отходов;

45) ГОСТ 6825-91 Лампы люминесцентные трубчатые для общего освещения.

46) Чрезвычайная ситуация [Электронный ресурс] / Википедия — свободная энциклопедия. – Электрон. дан. URL:http://ru.wikipedia.org/wiki/, свободный. – Загл. с экрана. – Яз. рус., англ.

47) ГОСТ Р 22.0.07-95 Безопасность в чрезвычайных ситуациях. Источники техногенных чрезвычайных ситуаций. Классификация и номенклатура поражающих факторов и их параметров. – М.: Госстандарт России, 1995.

48) Нормы пожарной безопасности (Утверждены 18.06.2003);

49) Нормы пожарной безопасности 160-97 (Утверждены 24.07.1997г.);

50) Ахатов А. Г. Экология. Энциклопедический словарь. - Казань, ТКИ, Экополис, 1995. — с. 168

Приложение А

(обязательное)

Раздел 1

Обзор литературы

Студент:

Группа	ФИО	Подпись	Дата
8ВМ5Г	Шипицина Варвара Павловна		

Консультант кафедры АиКС :

Должность	ФИО	Ученая степень, звание	Подпись	Дата
ассистент	Ефремов А.А.			

Консультант – лингвист кафедры ИЯИК :

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель	Денико Р.В.			

Biometric Authentication

The relevance of biometric authentication issues increases year by year, and this is due not so much to the dynamic development of the computer industry as a whole. To date, when the computing power of modern computers can open cryptically protected information and select a password for accessing the system for a few minutes to several hours, and information tapes are full of reports about the next hacking of security systems previously considered reliable, the value of a security system based on unique For each person biometric parameters, it is very difficult to overestimate.

The existing authentication methods for biometric parameters are divided into two main classes:

– Static;

– Dynamic.

Statistical methods are based on the physiological characteristics of a person who are present from birth to death, who are with him throughout his life, and who cannot be lost, stolen and copied.

Dynamic methods are based on human behavior characteristics, i.e. based on the characteristic of the unconscious movements during playback or duplication of any ordinary steps.

Criteria for biometric parameters. They must comply with the following points:

1) Universality: This attribute should be present for all people without exception.

2) Uniqueness: Biometrics deny the existence of two people with the same physical and behavioral parameters.

3) Persistence: for correct authentication, you need to be consistent over time.

4) Measurability: Professionals should be able to measure a characteristic by some device for further entry into the database.

5) Acceptability: a society should not be against the collection and measurement of a biometric parameter.

Types of biometric parameters used for authentication

Fingerprint Authentication

The most common biometric technology for user authentication is fingerprint identification.

The basis of the method is the use of a unique pattern of papillary patterns on the fingers of people. The scanner reads the papillary pattern, converts it into a digital model, and then compares it with the previously introduced print pattern, which is considered to be the reference pattern.

The main advantage of this method is its ease of use and implementation.

It is also worth noting the versatility of this method. It allows you to apply it in all areas and to solve any and all kinds of tasks, where you need accurate identification of users.

To obtain information about fingerprints, you need to use fingerprint scanners. Due to the fact that the fingerprint is small enough, it is necessary to use knowledge-based methods. To form a print of sufficient accuracy, special methods are used. Since the fingerprint is too small, and it is very difficult to get well-distinguishable papillary patterns.

Three main types of fingerprint scanners are commonly used:

– Capacitive;
– Rolling;
– Optical.
– The most common are optical scanners.

The main drawback of fingerprint authentication is the instability to dummies and dead fingers, which means that they are not as effective as other types of scanners.

Also in some sources, fingerprint scanners are divided into 3 classes according to their physical principles:

– Optical,

– Silicon,

– Ultrasonic.

In each fingerprint, you can define two types of characteristics - global and local.

The papillary pattern consists of:

– The pattern area is the fragment of the fingerprint that contains all the global signs.

– The core or center is a point localized in the middle of the print or some selected area.

– Point "delta" - the starting point. The place where the grooves of the papillary lines are divided or joined, or a very short groove (can reach the point).

– Line type - the two largest lines that start as parallel, and then diverge and envelop the entire region of the image.

– Line counter - the number of lines in the image area, or between the core and the "delta" point.

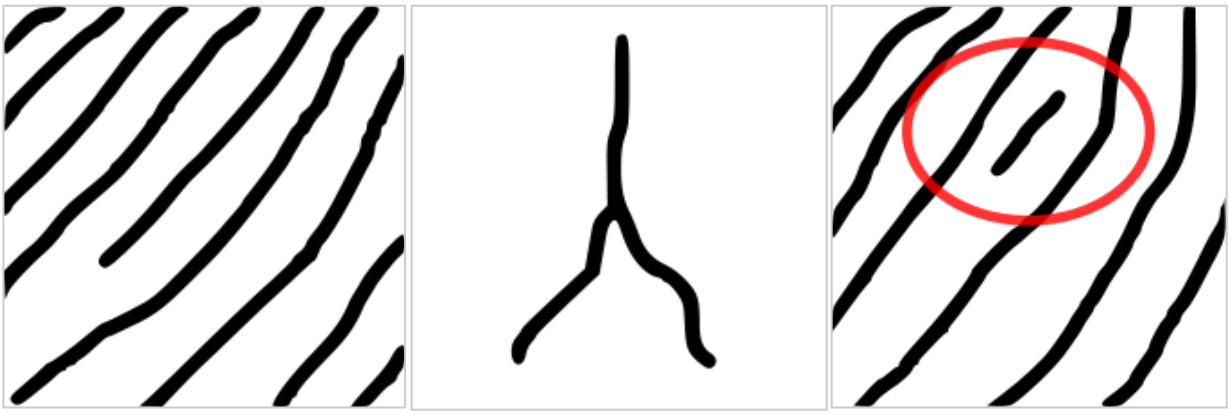


Figure 1 – Types of minations from left to right (ending, branching, islet)

Types of papillary patterns:

– Patterns such as "loop" (left, right, center, double);

– Patterns such as "delta" or "arc" (simple and sharp);

– Patterns of the "spiral" type (central and mixed).

Local signs are characteristics unique to each parent that determine the points of change in the structure of the papillary lines (ending, bifurcation, rupture, etc.), the orientation of the papillary lines, and the coordinates of these points. Each print can contain up to 70 or more mines.

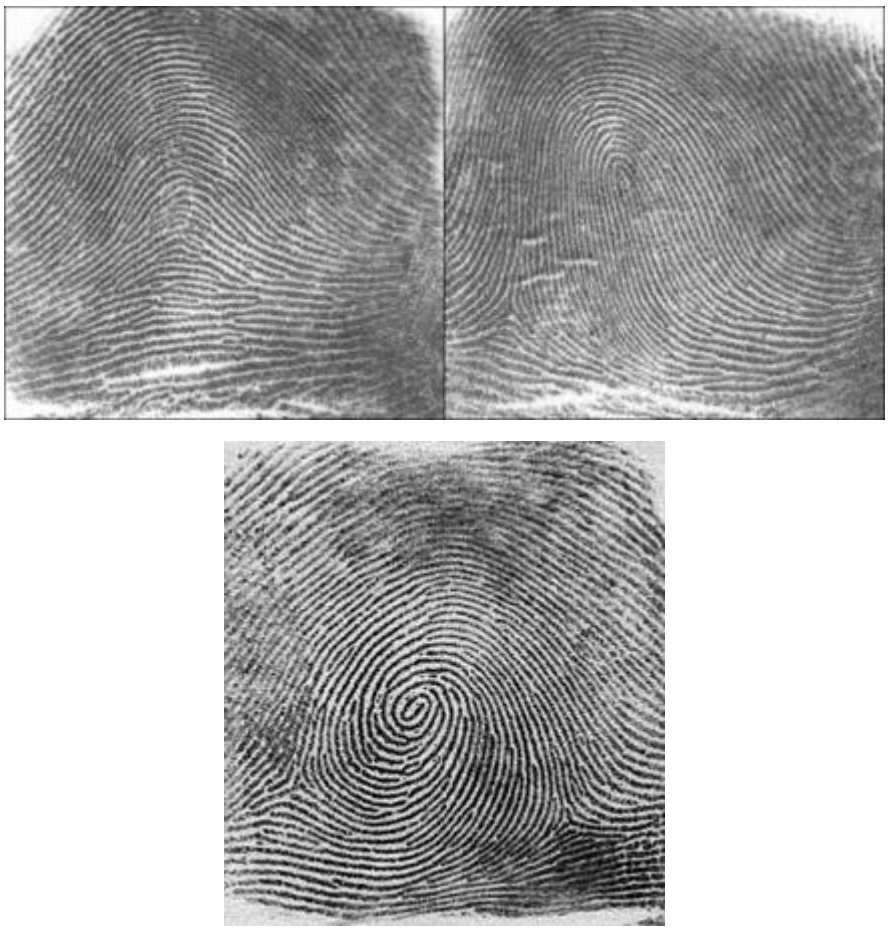


Figure 2 – Types of papillary patterns (arch, loop, curl)

On this fingerprint the following signs are noted: two lines - "line type"; What between them - can act as a pattern area, but usually the whole area of the print is taken; The circle on the left is the "delta" point; The red circle below is an island. The papillary pattern is the left loop.

Practice shows that fingerprints of different people can have the same global signs, but it is absolutely impossible to have the same micro-views of minuses.

Therefore, global characteristics are used to divide the database into classes and at the authentication stage. At the second stage of recognition, local signs are already used.

Standards on fingerprints in Russia

In Russian biometric standards regulated by ISO / IEC 19794-4-2006.

The image of the fingerprint must be represented by square elements (points) that have the same dimensions in the horizontal and vertical directions. The permissible difference between the horizontal and vertical dimensions of the point should not be more than 1%. The ratio of the horizontal dimension to the vertical dimension should be in the range from 0.99 to 1.01.

The bit depth of the grayscale (the number of bits used to represent the halftone) determines the accuracy of the grading scale. For example, the bit depth of the 3-bit gray scale provides 8 levels of grayscale; The bit depth of the gray scale of 8 bits provides 256 levels of gray scale. The minimum level of brightness of a point corresponding to a black color must be zero. The maximum level of the brightness of the point corresponding to the white color is encoded by the value "1" for each bit. The brightness of the "darkest" image paint itself can be greater than zero, and the brightness of the "light" point itself can be less than the maximum value determined by the gray scale. For example, the brightness of the "lightest" point with the 5-bit bit depth of the gray scale should be no more than 31, and the brightness of the "lightest" point with the 8-bit gray scale should be no more than 255. The gray scale value should be set In the range from 1 to 16 bits.

The gradation data of a gray image of a fingerprint can be stored, recorded or transmitted in both compressed and uncompressed form. The data record of the fingerprint image in grayscale in uncompressed form should contain information about the points of the original image. In images with a gray scale of 8 bits (256 grayscale), one byte is coded for each point. The brightness values of points with a grayscale of less than 8 bits should be stored and transmitted in a packed binary code. If the brightness value of the points is greater than 255, you must use a two-byte unsigned

format (16 bits) corresponding to the brightness range from zero to 65535. The compression of the compressed image data is determined by the compression algorithm used. The gray scale data of the image restored after compression should be represented in the same way as the uncompressed image data.

The image in grayscale should be encoded with an accuracy that meets the system requirements for the dynamic range of the image. It is assumed that these requirements are set in advance.

To obtain a black and white image of a fingerprint, a biometric scanner must have a specific resolution. When the resolution of the fingerprint scan is increased, the details of the papillary ridges in the image are increased. To detect control points and small objects, special algorithms are used in the image of the fingerprint; While high resolution allows you to detect objects that cannot be detected at low resolution.

The image resolution can be the same as the scan resolution. The resolution of the image can be changed by thinning and interpolating methods or by other methods to represent the structure and shape of the papillary ridges and the areas of the fingerprints of the fingerprint image.

The greatest efficiency of most biometric systems is achieved when the finger pad is located in the central area of the biometric scanner window. During the imaging process, the central region of the finger should be located approximately in the center of the window area of the biometric scanner. To identify and verify multiple fingerprint images, there are scanners designed to capture images of multiple fingerprints simultaneously. These devices allow you to receive images of four fingerprints of one hand or two thumbs of both hands simultaneously. Imaging images of all 10 fingers can be obtained for three scan cycles - four fingers of the right hand, four fingers of the left hand and two thumbs. To simultaneously obtain fingerprint images, it is necessary that half of these images are located to the left of the center of the common image, and the other half to the right.

Authentication for the iris of the eye

Iris - thin mobile iris eye in vertebrates with a hole in the center; located behind the cornea between the anterior and posterior chamber of the eye before the lens . Iris is formed before the birth of a person, and does not change throughout life. Iris on a structure resembles a network with a large number of surrounding circles and graphics, which can be measured by computer, pattern of the iris is very complicated, it allows to select the order of 200 dots by which a high degree of reliability of the authentication.

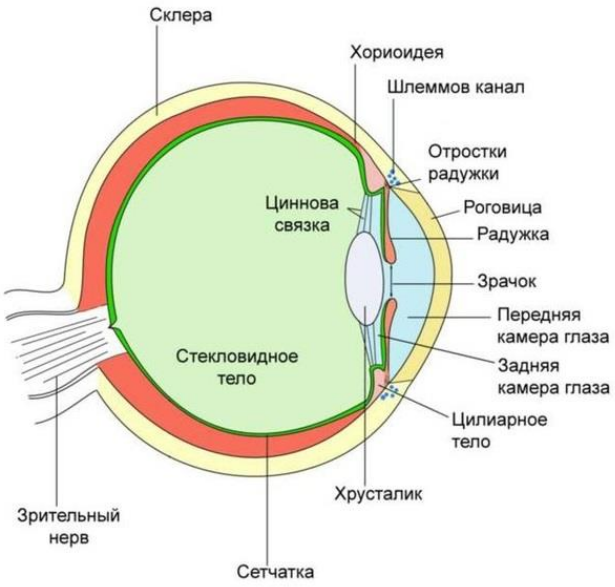


Figure 3 – The structure of the human eye

There is an iris between the cornea and the lens and performs the function of a kind of natural diaphragm that regulates the flow of light into the eye. The iris pigmented, and it determines the amount of pigment color of the human eye [7].

In its structure, the iris consists of elastic matter - the trabecular network. This is a reticular formation, which is formed by the end of the eighth month of pregnancy. Trabecular network consists of depressions, comb-like screeds, furrows, rings, wrinkles, freckles, vessels and other features. Due to such a number of components, the "pattern" of the network is quite random, which leads to a high probability of uniqueness of the iris. Even twins this parameter does not coincide completely.

Despite the fact that the iris of the eye can change its color up to one and a half years from the moment of birth, the pattern of the tuberculosis network remains unchanged throughout the life of a person. An exception is considered serious injury and surgery.

Most current operating systems and identification technology for iris recognition based on the principles proposed by John. Daugmanom article «High confidence visual recognition of persons by a test of statistical independence».

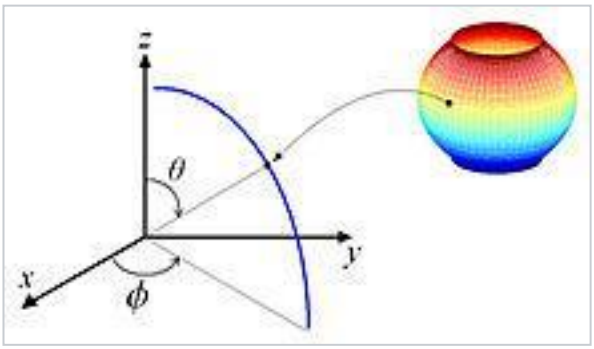


Figure 4 – Polar coordinate system

The process of personality recognition using the iris of the eye can be divided into three main stages: digital image acquisition, segmentation and parameterization. Each of these steps will be discussed in more detail below.

The authentication process begins with obtaining a detailed image of the human eye. The image for further analysis is trying to do with high quality, but it is not necessary. The iris is so unique that even a fuzzy image will give a reliable result. For this purpose, use a monochrome CCD camera with a dim illumination, which is sensitive to infrared radiation. Usually they make a series of several photographs because the pupil is sensitive to light and constantly changes its size. The backlight is unobtrusive, and a series of pictures is taken in just a few seconds. Then, from the obtained images to select one or more segments and proceed to.

During the parameterization of the iris from the normalized image, a control area is selected. Two-dimensional Gabor waves are applied to each point of the selected region (other filters can be used, but the principle remains the same) in order to extract

the phase information. The undoubted advantage of the phase component is that it, in contrast to the amplitude information is independent of the image and contrast lighting.

The resting phase is usually quantized by 2 bits, but you can use a different amount. The total length of the description of the iris, thus, depends on the number of points in which the phase information is found and the number of bits necessary for encoding. In the end, we get an iris pattern that will be checked against other patterns in the authentication process. The measure by which the degree of difference between the two irises is determined is the Hamming distance.

Authentication of the retina

About retina

The retina is the inner shell of the eye, which is the peripheral part of the visual analyzer; Contains photoreceptor cells that ensure the perception and transformation of electromagnetic radiation from the visible part of the spectrum into nerve impulses, and also provides for their primary processing.

The retina of an adult human has a diametrical size of 22 mm and covers about 72% of the surface area of the inner eyeball.

The pigmentary layer of the retina (the most external) with the choroid of the eye is connected more closely than with the rest of the retina.

Near the center of the retina (closer to the nose) on the back of its surface is the disc of the optic nerve, which sometimes due to the lack of photoreceptors in this part is called a "blind spot." It looks like a towering pale oval-shaped zone about 3 mm². Here, from the axons of ganglionic retinal neurocytes, the formation of the optic nerve occurs. In the central part of the disc, there is a depression through which the vessels participating in the blood supply of the retina pass.

Lateral to optical disk, approximately 3 mm spot located in the center of which has a recess, fovea centralis, is the most sensitive portion of the retina to light and is responsible for central vision clear. In this area of the retina contains only cones. Man and other primates have one central force in each eye, in contrast to some species of

birds, such as hawks, in which there are two of them, as well as dogs and cats that have a strip in front of the retina in the central part of the retina, the so-called visual stripe. The central part of the retina is represented by a fosse and an area within a radius of 6 mm from it, followed by the peripheral part, whereas the forward progresses the number of rods and cones decreases. Ends inner shell serrated edge, at which the photosensitive elements are absent.

Over its length, the thickness of the retina is not the same and is at the thickest part, at the edge of the optic nerve disk, no more than 0.5 mm; The minimum thickness is observed in the area of the five of the yellow spot.

Authentication of the retina

The authentication method of the retina received practical application around the middle of the 50s of the last century. It was then that the uniqueness of the picture of the blood vessels of the funds was established (even with the twins, these figures do not coincide). To scan the retina using infra-red radiation of low intensity, directed through the pupil to the blood vessels at the back of the eye. From the received signal, several hundred special points are allocated, the information about which is stored in the template.

The disadvantage of such systems should be primarily attributed psychological factor: Not everyone is pleasant to look at the strange dark hole where something shining in his eyes. Moreover, such systems require a clear image and is usually sensitive to the incorrect orientation of the retina. Therefore, it is required to look very carefully, and the presence of certain diseases (e.g., cataract) may prevent the use of this method. Scanners retina became widespread access to top-secret facility, as it provides one of the lowest of type I error probability (the denial of access to a registered user), and near-zero error rates.

Comparison with authentication on the retina

Most often, people confuse physiological parameters such as the retina and iris. More often they combine the two concepts into one. This is a huge mistake, as the retina authentication method includes the study of the ocular fundus. Due to the duration of this process and the large size of the installation this type of authentication is difficult to call public and convenient. This biometric authentication retina loses authentication iris.

Authentication hand geometry

This biometric method for identity authentication using a form of the hand. Due to the fact that the individual parameters hand forms are not unique, it is necessary to use some features. Such parameters are scanned hand bends as the fingers, and their length and thickness, the width and the thickness of the back of the hand, the distance between the joints and bone structure. Also, hand geometry includes small parts (e.g., skin wrinkles). Although the structure of the joints and bones are relatively persistent symptoms, but swelling of tissue injuries or hands can distort the original structure. Technology problem: even without the possibility of amputation, the disease called "arthritis" can strongly interfere with the use of scanners.

With a scanner, which consists of a camera and illuminating diodes (by scanning the hand, LEDs are turned on, it allows you to get different arms of the projection), then built a three-dimensional image of the hand. The reliability of authentication, hand geometry is comparable to fingerprint authentication.

Authentication system for hand geometry are widespread, which is proof of their convenience for users. Using this option is attractive for several reasons. The procedure for obtaining the sample is quite simple and does not impose higher requirements to the picture. The size of the resulting pattern is very small, a few bytes. An authentication process is not affected by temperature, humidity or contaminated. Calculations made by the comparison with the standard, it is very simple and can be easily automated.

Authentication systems based on hand geometry, began to be used in the world in the early 70s.

Geometry of the face authentication

Biometric authentication is a man face geometry fairly common method of identification. Technical realization is a complicated mathematical problem. Extensive use of multimedia technologies, with the help of which you can see a sufficient number of cameras at stations, airports, squares, streets, roads and other public places, was decisive in the development of this direction. To construct the three-dimensional model of a human face, is isolated eye contours, eyebrows, lips, nose, and various other facial elements, and then calculating the distance between them, and with its help build three-dimensional models. To determine the unique pattern corresponding to a specific person, it requires between 12 and 40 characteristic elements. The template should take into account the plurality of image variations in the rotation of the cases the person, tilt, change lighting, change of expression. The range of options varies depending on the application of this method (for identification, authentication, remote search over large areas, and etc.). Some algorithms are used to compensate for the presence of human points, hat, mustache and beard.

Thermogram of the face authentication

The method is based on studies that have shown that facial thermogram is unique for each person. The thermogram obtained by means of an infrared camera. In contrast to the geometry of the face authentication, this method distinguishes between twins. The use of special masks, plastic surgery, the aging of the human body, body temperature, cooling of the skin in cold weather do not affect the accuracy of the thermogram. Due to the low quality of the authentication method currently is not widely used.

Voice authentication

Biometric voice authentication method that is characterized by ease of use. This method does not require expensive equipment, enough to a microphone and a sound card. Currently, this technology is developing rapidly, as this method of authentication is widely used in modern business centers. There are many ways to construct the voice pattern. Normally, these are different combinations of frequency and statistical characteristics of the voice. Can be considered parameters such as modulation, tone, pitch, and etc.

The main and decisive disadvantage of voice authentication - the low accuracy of the method. For example, a person with a cold system can not recognize. An important problem is the manifold manifestations of the human voice: the voice is able to vary depending on the health condition, age, mood, etc. This manifold presents serious difficulties when allocating distinctive properties of the human voice. In addition, the account of the noise component is another important and unsolved problem in the practical use of authentication by voice. Since the probability of error of the second kind by using this method is high (about one percent), the authentication, voice is used for access control in areas the average level of security, such as computer rooms, laboratories, industrial companies, and etc.

Authentication of handwriting

Biometric authentication method of handwriting is based on a specific motion of a human hand signing documents. To save the signature using a special pen or a pressure-sensitive surface. This kind of person authentication using his signature. The template is created, depending on the required level of protection. Usually two isolated processing method signature data:

Analysis of the signature itself, that is used by just a degree of coincidence of the two images.

Analysis of the dynamic characteristics of the writing, that is to authenticate constructed bundle, which includes information for a signature, time and statistical characteristics of her writing.

Combination biometric authentication system

Combined (multimodal) biometric authentication system uses a variety of add-ons to use multiple types of biometric characteristics, which allows to combine several types of biometrics authentication system in one. This enables allied meet the most stringent performance requirements for the authentication system. For example, fingerprint authentication can easily be combined with hand scanning. Such a structure can use all types of human biometric data and can be used where necessary to limit boost one biometric characteristic. Combined systems are more reliable in terms of the possibility of simulating human biometric data, as difficult to forge a number of characteristics than falsify one biometric feature.

Приложение Б

(справочное)

Инструкция по применения сканера отпечатков пальцев сотрудниками

5. ПРОЦЕДУРА ПРОХОЖДЕНИЯ ОСМОТРА

1

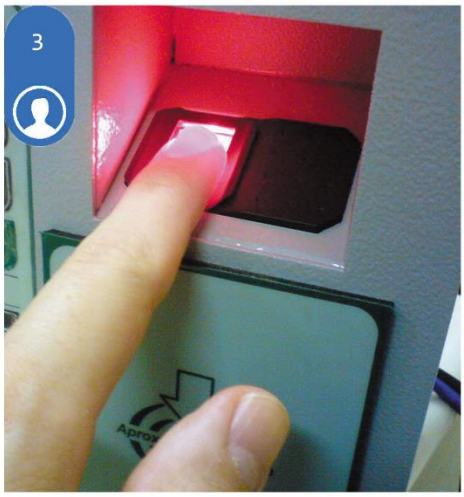
Сядьте удобно в кресло

2

Палец не должен иметь повреждений или загрязнений

Проверьте состяние пальца

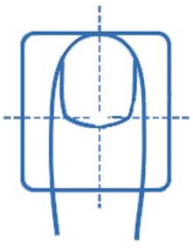
3



Приложите палец к датчику идентификации

4

Палец должен лежать в центре окна считывателя. Палец должен плотно прилегать к окну считывателя



Приложение В

(справочное)

Следующие фрагменты кода иллюстрируют, как создать объект License.

```
namespace Sample
{
class Class1
{
static void Main(string[] args)
{
try
{
// Create License object. The object must exist
// all the time during using BSDK
using (License license = new License())
{
//... The program
}
}catch(Exception ex)
{
Console.WriteLine("Error: {0}", ex.Message);
}
}
}
}
```

Следующие фрагменты кода иллюстрируют сканирование изображения отпечатка пальца.

```
namespace Sample
{
class Class1
{
static void Main(string[] args)
{
try
```

```
{
// Create License object. The object must exist
// all the time during using BSDK
using (License license = new License())
{
//creating the list of devices
using (DeviceList deviceList = new DeviceList())
{
//selecting first found device
using (DeviceDescriptor deviceDescriptor =
deviceList.DeviceDescriptor(0))
{
//creating Scanner object
using (Scanner scanner = new
Scanner(deviceDescriptor))
{
//acquiring image from the scanner
Image image = scanner.AcquireImage();
}
}
}
}
}catch(Exception ex)
{
Console.WriteLine("Error: {0}", ex.Message);
}
}
}
}
```

Следующие фрагменты кода иллюстрируют, как создать, сохранить и загрузить шаблон отпечатка пальцев.

```
namespace Sample
{
class Class1
{
static void Main(string[] args)
{
try
```

```
{
// Create License object. The object must exist
// all the time during using BSDK
using (License license = new License())
{
//creating the list of devices
using (DeviceList deviceList = new DeviceList())
{
//selecting first found device
using (DeviceDescriptor deviceDescriptor =
deviceList.DeviceDescriptor(0))
{
//creating Scanner object
using (Scanner scanner = new
Scanner(deviceDescriptor))
{
//acquiring image from the scanner
Image image = scanner.AcquireImage();
byte[] bufferTemplate;
//creating ImageSet object to hold Image
objects
using (ImageSet imageSet = new ImageSet())
{
//adding Image objects to ImageSet with
some FingerCode
imageSet.AddImage(image, 0);
//creating ImageProcessor object to create
template
/* You can specify math type when creating
ImageProcessor, Template, TemplateSet or Matcher objects.
* The math type should be the same for
all these objects.
*/
using (ImageProcessor imgPrc = new
ImageProcessor())
{
//creating template
Template templ =
imgPrc.CreateTemplate(imageSet);
//saving template to bufferTemplate
byte array
```

```
bufferTemplate = templ.ToArray();
}
}
//loading template from buffer
Template template = new Template();
template.Load(bufferTemplate);
}
}
}
}
}
catch (Exception ex)
{
Console.WriteLine("Error: {0}", ex.Message);
}
}
}
}
```

Следующие фрагменты кода иллюстрируют, как сравнить два шаблона.

```
namespace Sample
{
class Class1
{
static void Main(string[] args)
{
try
{
// Create License object. The object must exist
// all the time during using BSDK
using (License license = new License())
{
//creating the list of devices
using (DeviceList deviceList = new DeviceList())
{
//selecting first found device
using (DeviceDescriptor deviceDescriptor =
deviceList.DeviceDescriptor(0))
{
```

```
//creating Scanner object
using (Scanner scanner = new
Scanner(deviceDescriptor))
{
//acquiring image from the scanner
Image image1 = scanner.AcquireImage();
Image image2 = scanner.AcquireImage();
//creating ImageSet object to hold Image
objects
using (ImageSet imageSet1 = new ImageSet())
{
//adding Image objects to ImageSet with
some FingerCode
imageSet1.AddImage(image1, 0);
using (ImageSet imageSet2 = new
ImageSet())
{
imageSet2.AddImage(image2, 0);
//creating ImageProcessor object to
create template
/* You can specify math type when
creating ImageProcessor, Template, TemplateSet or Matcher objects.
* The math type should be the same
for all these objects.
*/
using (ImageProcessor imgPrc = new
ImageProcessor())
{
//creating templates
Template template1 =
imgPrc.CreateTemplate(imageSet1);
Template template2 =
imgPrc.CreateTemplate(imageSet2);
//matching template1 with
template2
using (Matcher matcher = new
Matcher())
{
int score =
matcher.Compare(template1, template2);
}
```

```
}
}
}
}
}
}
}
}
catch (Exception ex)
{
Console.WriteLine("Error: {0}", ex.Message);
}
}
}
}
```

Следующие фрагменты кода иллюстрируют использование TemplateSet.

```
using System;
using Biolink.Biometrics2;
namespace Sample
{
class Class1
{
static void Main(string[] args)
{
try
{
// Create License object. The object must exist
// all the time during using BSDK
using (License license = new License())
{
//creating the list of devices
using (DeviceList deviceList = new DeviceList())
{
//selecting first found device
using (DeviceDescriptor deviceDescriptor =
deviceList.DeviceDescriptor(0))
{
//creating Scanner object
using (Scanner scanner = new
```

```
Scanner(deviceDescriptor))
{
//acquiring image from the scanner
Image image1 = scanner.AcquireImage();
Image image2 = scanner.AcquireImage();
Template template1;
Template template2;
//creating ImageSet object to hold Image
objects
using (ImageSet imageSet1 = new ImageSet())
{
//adding Image objects to ImageSet with
some FingerCode
imageSet1.AddImage(image1, 0);
using (ImageSet imageSet2 = new
ImageSet())
{
imageSet2.AddImage(image2, 0);
//creating ImageProcessor object to
create template
/* You can specify math type when
creating ImageProcessor, Template, TemplateSet or Matcher objects.
* The math type should be the same
for all these objects.
*/
using (ImageProcessor imgPrc = new
ImageProcessor())
{
//creating templates
template1 =
imgPrc.CreateTemplate(imageSet1);
template2 =
imgPrc.CreateTemplate(imageSet2);
}
}
}
//creating TemplateSet object to hold all
templates for identification
using (TemplateSet templateSet = new
TemplateSet())
{
```

```
//adding templates to the templateSet
templateSet.AddTemplate(template1, 1,
"template1");
templateSet.AddTemplate(template2, 2,
"template2");
//matching template2 with templates in
templateSet with threshold equal to 600
using (Matcher matcher = new Matcher())
{
//creating IdentifyInfoSet class
holding a set of IdentifyInfo objects returned by Identify method
//IdentifyInfo objects are sorted by
score in descending order
using (IdentifyInfoSet infoSet =
matcher.Identify(template2, templateSet, 600))
{
for (int i = 0; i < infoSet.Size;
i++)
{
//IdentifyInfo object used to
view matching score...
using (IdentifyInfo
identifyInfo = infoSet.GetItem(i))
{
Console.WriteLine("Template id {0}, number {1}, score {2}",
identifyInfo.Id,
identifyInfo.Number, identifyInfo.Score);
}
}
}
}
}
}
}
}
}
}
catch (Exception ex)
{
Console.WriteLine("Error: {0}", ex.Message);
}
```

```
}
}
}
```