

Федеральное государственное автономное  
образовательное учреждение  
высшего образования  
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ КОСМИЧЕСКИХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
Кафедра «Информационных систем»

УТВЕРЖДАЮ  
И. О. Заведующий кафедрой ИС  
\_\_\_\_\_ Л.С. Троценко  
«13» июня 2018 г.

## БАКАЛАВРСКАЯ РАБОТА

09.03.02 «Информационные системы и технологии»

Система контроля и управления доступом на предприятии

Руководитель	_____	доцент, к.т.н	С.А. Виденин
	подпись, дата		
Выпускник	_____		А.В. Киселёв
	подпись, дата		
Нормоконтролер	_____		Ю.В. Шмагрис
	подпись, дата		

Красноярск 2018

Федеральное государственное автономное  
образовательное учреждение  
высшего образования  
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ КОСМИЧЕСКИХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
Кафедра «Информационных систем»

УТВЕРЖДАЮ  
Заведующий кафедрой ИС

— С.А Виденин  
подпись инициалы, фамилия

«2» марта 2018 г.

**ЗАДАНИЕ  
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ  
в форме бакалаврской работы**

Студенту Киселёву Александру Владимировичу

фамилия, имя, отчество

Группа ЗКИ13-13б Направление (специальность) 09.03.02

номер

код

Информационные системы и технологии

наименование

Тема выпускной квалификационной работы Система контроля и управления доступом на предприятии

Утверждена приказом по университету № 3758/с от 14.03.2018

Руководитель ВКР С.А. Виденин, доцент, заведующий кафедрой Информационные системы

Исходные данные для ВКР Введение, анализ проблемы, технические аспекты, анализ существующих решений, разработка проекта, выбор архитектуры, проектирование базы данных, разработка интерфейса, контрольный пример реализации

Перечень разделов ВКР Анализ проблемы идентификации и контроля доступа в помещениях на предприятии; разработка проекта по управлению доступом сотрудников в помещения предприятия

Перечень графического материала Презентация, выполненная в Microsoft: PowerPoint 2007

Руководитель ВКР \_\_\_\_\_

подпись

С.А. Виденин

инициалы и фамилия

Задание принял к исполнению \_\_\_\_\_

А.В. Киселёв

подпись, инициалы и фамилия студента

«2» марта 2018 г.

## **РЕФЕРАТ**

Выпускная квалификационная работа по теме: «Система контроля и управления доступом на предприятии» содержит 58 страниц текстового документа, 24 иллюстраций, 10 таблиц, 18 использованных источников.

**СИСТЕМА, КОНТРОЛЬ, УПРАВЛЕНИЕ ДОСТУПОМ, ПРОГРАММА, ОБЪЕКТ, ИНФОРМАЦИЯ, ОТЧЕТ.**

Объектом исследования работы является программная система контроля и управления доступом на предприятии».

Целью работы является разработка системы контроля и управления доступом.

В ходе выполнения данной работы была создана система по контролю и управлению доступом на предприятии, сформирована база данных и разработан алгоритм работы программной части системы, также создан пользовательский интерфейс программы.

В результате была реализована система по контролю и управления доступом на предприятии.

## **СОДЕРЖАНИЕ**

<b>ВВЕДЕНИЕ.....</b>	<b>4</b>
<b>1 Анализ проблемы идентификации и контроля доступа в помещения на предприятия.....</b>	<b>6</b>
1.1 Технические аспекты реализации.....	6
1.2 Информационное обеспечение систем управления доступом.....	14
1.3 Анализ существующих решений по организации доступа .....	24
<b>2 Разработка проекта по управлению доступом сотрудников в помещения предприятия .....</b>	<b>26</b>
2.1 Выбор архитектуры решения и средств разработки.....	26
2.2 Проектирование базы данных информационной системы доступа ....	34
2.3 Разработка интерфейса системы управления доступом.....	39
2.4 Контрольный пример реализации решения.....	44
<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>55</b>
<b>СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....</b>	<b>57</b>

## **ВВЕДЕНИЕ**

Перед современным предприятием сегодня стоит множество проблем: удержание клиентов, поиск лучших поставщиков, что в конечном итоге должно повлиять на увеличение прибыли и снижение издержек.

Однако все усилия компании могут быть напрасны, в случае если новые технологии, которые использует компания на рынке, станут доступны конкурентам.

Для защиты коммерческой тайны компании от внешних посягательств применяют множество технологий, включая специализированное оборудование и программное обеспечение. Тем не менее, по статистике наибольшее число краж информации связано не с внешними «врагами», а собственными сотрудниками, имеющими доступ либо к самой информации, либо к технологиям ее получения.

Решение проблемы лежит обычно в разработке комплексной политики безопасности на предприятии, которая включает как специализированное программное и аппаратное обеспечение, так и организационное, правовое и другие виды обеспечения.

Для предприятий, занимающихся обработкой закрытой информации или предоставляющих особые виды услуг, особенно важным становится организационное обеспечение доступа к помещениям, в которых расположены объекты с корректируемыми правами доступа к ним. В таком случае возникает необходимость регулирования такой системы управления доступом посредством специализированных технических и программных средств.

Целью данной работы является совершенствование системы управления доступом к помещениям на предприятии.

Для достижения поставленной цели в работе предполагается решение целого комплекса задач:

- анализ проблемы идентификации и контроля доступа в помещения на предприятии в техническом и информационном аспекте;
- обзор существующих решений по организации доступа;
- построение проекта решения и выбор инструментов разработки;
- проектирование базы данных и прототипа интерфейса системы;
- реализация проектного решения.

# **1 Анализ проблемы идентификации и контроля доступа в помещения на предприятии**

## **1.1 Технические аспекты реализации**

Под системой контроля и управления доступом (СКУД) в общем случае понимается совокупность организационно-методических и программно-технических средств, позволяющих осуществить решение задачи контроля и управления территорией на объекте и оперативными помещениями, а также оперативного контроля за движением сотрудника и временными интервалами их нахождения на объекте.

Следует подробнее остановиться на качественном составе современных систем контроля и управления доступом. В данном случае, СКУД представляет из себя набор средств (электротехнических, электронных, механических и иных), которые объединены в комплексы и обеспечивают возможность доступа определенных сотрудников в заданные зоны (например, здание, территория, помещение), либо к заранее определенным техническим средствам, аппаратуре и предметам (автомобилю, персональному компьютеру, сейфу), а также запрещают этот доступ лицам, которые не наделены таким правом. Благодаря использованию подобных систем обеспечивается безопасность посетителей и персонала, сохранность информационных и материальных ресурсов предприятия осуществляется контроль за перемещением транспорта и людей по территории охраняемого объекта. Использование систем контроля и управления доступом целесообразно в офисах, промышленных предприятиях, на автостоянках, в магазинах, жилых помещениях и автосервисах.

Рост актуальности СКУД обусловлен еще и важностью ее наличия для эффективного функционирования предприятия. Осуществление контроля дает возможность не только существенно увеличить уровень безопасности, но и производить оперативное реагирование на поведение посетителей и

персонала. Помимо этого, не следует преуменьшать важность задачи, заключающейся в необходимости проведения контроля графика и учета рабочего времени. Повышенное внимание на многих предприятиях уделяется системам, которые позволяют осуществлять выстраивание требуемых конфигураций из стандартных блоков с учетом специфики предприятия.

Согласно существующему ГОСТ 51241-2008 «Средства и системы контроля и управления доступом», устанавливающему классификацию, методы испытаний и общие технические требования, все СКУД могут быть разделены в соответствии с нижеследующими признаками:

- по количеству контролируемых точек доступа;
- по уровню защищенности системы от несанкционированного доступа;
- по функциональным характеристикам;
- по способу управления.

К СКУД первого класса относятся малофункциональные системы малой емкости, которые функционируют в автономном режиме и обеспечивают доступ всех лиц, обладающих соответствующим идентификатором. Такая система использует автоматическое или ручное управление исполнительными устройствами, а также звуковую или световую сигнализацию (рисунок 1.1).



Рисунок 1.1 – Типовая схема СКУД первого класса (в помещении одна дверь)

СКУД второго класса являются многофункциональными системами. Они могут представлять из себя как одноуровневую, так и многоуровневую

систему и, соответственно, осуществлять работу как в сетевом, так и в автономном режимах. Допуск лиц или групп лиц может быть осуществлен в соответствии с датой, временными интервалами. Система позволяет выполнить обеспечение автоматической регистрации событий и автоматического управления сетевыми устройствами. Структурная схема подобной системы представлена на рисунок 1.2.



Рисунок 1.2 – Типовая схема СКУД второго класса

СКУД третьего класса относятся, чаще всего, к сетевым системам. Они используют усложненные идентификаторы сетевого взаимодействия (интерфейсы считывания магнитных карт или карт Виганда, клиент-сервер, интерфейсы специализированного типа). Пример реализации подобной СКУД представлен на рисунок 1.3.



Рисунок 1.3 – Типовая схема СКУД третьего класса

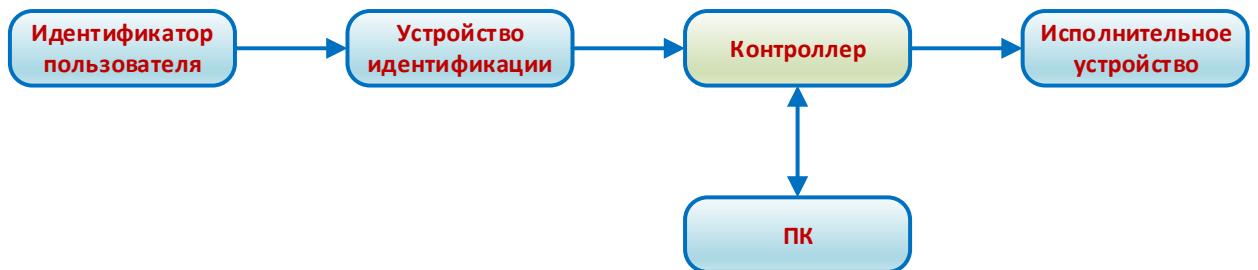
Согласно способам управления, все системы контроля и управления доступом могут быть разделены на:

- автономные – предназначены для управления одним или несколькими устройствами управления, информация не передается на центральное устройство управления, контроль со стороны оператора не осуществляется;
- централизованные (сетевого типа) – предназначены для управления устройствами управления с возможностью обмена данными с центральным устройством управления, контроль системы со стороны центрального устройства управления осуществляется;
- универсальные (сетевого типа) – включают в себя функциональные возможности как автономных, так и централизованных систем, функционирующие в сетевом режиме под управлением центрального устройства управления и обладающие возможностью перехода в автономный режим в случае, когда возникают отказы в сетевом оборудовании, центральном устройстве, а также при обрыве связи.

Все СКУД должны обладать совокупностью характеристик, значения которых должны удовлетворять стандартам и (или) техническим условиям на системы определенного типа. К таким характеристикам относятся:

- максимальное количество точек доступа зон доступа пользователей, которые обслуживаются системой;
- максимальное количество контроллеров в системе;
- количество и вид временных интервалов доступа, а также уровней доступа;
- время реакции системы на заявку на проход;
- максимальное расстояние действия считывателя (актуальный параметр для бесконтактных считывателей);
- максимальная пропускная способность для системы в точках доступа;
- максимальное время хранения в памяти системы о произошедших событиях;
- максимальная протяженность линии связи с контроллерами и допустимые параметры линии связи;
- количество типов считывателей, которые используются в системе;
- количество считывателей на один контроллер системы;
- максимальное количество точек доступа, которые обслуживаются одним контроллером.

Таким образом, общая схема системы управления и контроля доступом приведена на рисунок 1.4.



#### Рисунок 1.4 – Общая схема системы управления и контроля доступа

Для СКУД в качестве основного понятия чаще всего используется понятие идентификации и идентификатора. Под идентификацией понимается поиск по признаку, опознавание. Для идентификации применимыми являются следующие основные принципы:

- идентификация в соответствии с запоминаемым кодом. В данном случае ввод кода осуществляется вручную с помощью кодовых переключателей, клавиатуры и других устройств подобного типа;
- идентификация в соответствии с вещественным кодом. Здесь запись кода осуществляется на идентификатор (магнитный носитель), в качестве которого могут быть использованы различные карты, брелоки, ключи и т.д.;
- биометрическая идентификация – в основе данного типа идентификации лежит определение индивидуальных, неповторяющихся физических признаков человека.

Следует подробнее остановиться на каждом из типов идентификации.

При идентификации в соответствии с запоминаемым кодом роль считывателя играет алфавитно-цифровая клавиатура, а также кодовые переключатели различного типа, панели и иные устройства. Ввод кода осуществляется вручную, набором соответствующих символов или установкой переключателей в определенные позиции. Название данного типа идентификации свидетельствует о необходимости запоминания пользователем вводимого пароля или кода. Достоинство метода заключается в отсутствии материального носителя кода, и, соответственно, отсутствии затрат на его применение. Вместе с тем, необходимость запоминания пароля или кода человеком имеет очевидные недостатки. Чтобы повысить надежность пароля или кода требуется использование как можно большего числа знаков. Например, в соответствии со стандартом на СКУД количество знаков в пароле к компьютерной программе не должно составлять значение,

меньшее шести. В кодах доступа для некоторых сейфовых замков, обладающих высокой секретностью, содержится до двенадцати знаков. Запоминание такого числа цифр или знаков для большинства людей представляется достаточно нелегкой задачей. Следствием этого является достаточно частая запись кода на бумаге и хранение ее в непосредственной близости от сейфа или компьютера, что приводит в практической потере секретности доступа. Еще один недостаток связан с проходными на больших предприятиях. В случае большого потока людей через проходную, допускаемые при вводе кода ошибки приводят к резкому снижению пропускной способности и увеличению числа конфликтов с охранной службой. Клавиатурные считыватели обладают недостаточной защищенностью от манипуляций (наблюдения, подбора кода). Вместе с тем они обладают и рядом преимуществ, например, подбор разрядности кода может быть осуществлен произвольно, установка кода производится самим пользователем, как и его изменение. Код обычно неизвестен оператору системы, кроме этого существует возможность ввода дополнительных кодов, например, управляющих кодов, кода «тихой» тревоги в случае нападения.

В настоящее время наиболее распространенными являются системы управления и контроля доступом, которые используют идентификацию в соответствии с вещественным кодом. Популярность данного вида идентификации связана с тем обстоятельством, что использование удостоверения личности, пропуска или другого документа (другими словами, предмета на котором наносится информация о человеке в виде соответствующих записей и его фотографии) является традиционным.

Само опознавание (идентификация) человека осуществляется тоже человеком (охранником, дежурным на проходной и т.д.) в основном согласно фотографии на документе. Это и приводит к главному недостатку метода – наличию человеческого фактора. Плохое состояние человека, потеря внимания, недостаточная концентрация, усталость ведут к снижению качества надежности охраны.

В электронных автоматических системах роль идентификаторов играют брелоки, пластиковые карты, электронные или механические ключи, браслеты и любые другие устройства подобного типа. В последнее время основным идентификатором для контроля доступа в автоматизированных системах являются пластиковые карты. На них можно наносить различные надписи, а также и фотографии владельцев, используя для этого принтеры специального типа или наклейку пленок. При этом карта доступа может использоваться и как обычный, традиционный документ.

Методика кодирования пластиковых карт достаточно разнообразна – от дешевых и простых карт, обладающих штриховым кодом, до карт, имеющих электронную начинку. На постоянной основе выпускаются новые типы пластиковых карт, которые используют различные технологии, позволяющие повысить надежность, секретность кода и улучшить другие характеристики.

Наиболее перспективным направлением идентификации, которой, собственно, и посвящена эта работа, является биометрическая идентификация. При идентификации в соответствии с индивидуальными биометрическими признаками происходит определение именно человека – носителя этих признаков, а не выданного ему документа – карты, ключа и т.д. Именно в этом заключается основное отличие систем подобного типа от других любых устройств, производящих идентификацию. К самым распространенным человеческим признакам, использующимся для биометрической идентификации, можно отнести:

- отпечатки пальцев;
- геометрию кисти;
- динамику подписи;
- изображение лица;
- голосовые характеристики;
- узор кровеносных сосудов сетчатки глаза.

Пример внешнего вида биометрического идентификатора, использующего отпечаток пальца человека, приведен на рисунок 1.5.



Рисунок 1.5 – Пример биометрического идентификатора

## 1.2 Информационное обеспечение систем управления доступом

Неоспоримым является утверждение, что по своей сути биометрия – это математическая статистика. Математическая статистика относится к точным наукам, алгоритмы которой находят повсеместное применение – и в байесовских системах, и в радарах. Двумя основными характеристиками любой биометрической системы являются ошибки первого и второго рода. В такой науке, как теория радиолокации, они обычно называются «ложная тревога» либо «пропуск цели», а в биометрии их принято называть FAR (False Acceptance Rate) и FRR (False Rejection Rate). Первое из чисел свидетельствует о вероятности ложного совпадения характеристик биометрии двух людей, а второе – о вероятности отказа в доступе человеку, который имеет допуск. Очевидно, что качество системы тем выше, чем меньше величина FRR при одинаковых величинах FAR. Иногда применяют сравнительную характеристику EER, которая определяет точку пересечения графиков FRR и FAR. Однако она далеко не всегда является репрезентативной.

Можно утверждать, что если в характеристиках системы не присутствуют значения FAR и FRR по открытым биометрическим базам, то,

несмотря на любые заявления производителей, с высокой долей вероятности система не является дееспособной, либо сильно отстает от конкурентов.

Однако, качество биометрической системы определяется не только FAR и FRR. Если бы дело обстояло подобным образом, то лидирующая технология заключалась бы в распознавании людей по ДНК, где показатели FAR и FRR практически равны нулю. Однако данная технология слабо применима на текущей стадии развития человечества. Существует несколько эмпирических характеристик, которые дают возможность произвести оценку качества системы. Такая эмпирическая характеристика, как «устойчивость к подделке» обобщает степень того, насколько легко может быть произведен обман эмпирического идентификатора. Характеристика «устойчивость к окружающей среде» оценивает степень устойчивости работы системы при разных внешних условиях, например, изменение температуры помещения или освещения. «Простота использования» свидетельствует об уровне сложности применения биометрического сканера, возможности идентификации «на ходу». К важным характеристикам могут быть отнесены «скорость работы» и «стоимость системы». Важно учитывать и подверженность биометрической характеристики человека к изменениям со временем, поэтому существенным минусом является ее неустойчивость.

Существует очень много биометрических методов. К основным методам, использующим статические биометрические характеристики, могут быть отнесены идентификация по радужной оболочке, сетчатке глаза, геометрии рук, рисунку вен руки, геометрии лица, папиллярному рисунку на пальцах. Помимо этого, есть совокупность методов, которые используют динамические характеристики, такие как идентификация по динамике рукописного подчерка, походке, сердечному ритму, голосу.

В настоящее время понятия «биометрический сканер» и «биометрический алгоритм» не являются обязательно взаимосвязанными. Эти элементы могут выпускаться производителями как по одиночке, так и совместно. Наибольшей дифференциации производителей программного

обеспечения и сканеров достиг рынок биометрии папиллярного узора пальцев. Наименьшая дифференциация наблюдается на рынке сканеров 3D лица. Можно сказать, что степень выбора определяет насыщенность и развитость рынка. Различным сканерам присущ разный набор умений. По большей части, это совокупность тестов, с помощью которых проверяется, была ли подделка объекта биометрии или нет. Для сканеров пальцев в качестве проверки рассматриваются температура и рельефность, для сканеров глаза – аккомодация зрачка, для сканеров лица – движение лица.

Влияние сканеров на статистику FAR и FRR очень велико. В некоторых ситуациях изменение этих цифр достигает десятков раз, особенно в условиях реального времени. Принято давать характеристики алгоритма для некоторой «идеальной» базы, либо для наиболее точно подходящей, в которой выполнено отбрасывание нерезких и смазанных кадров. Только в очень немногих алгоритмах честно указывается и база, и полные выкладки по показателям FAR и FRR. Теперь следует остановиться на каждом из методов подробнее.

Распознавание отпечатков пальцев (дактилоскопия) является наиболее разработанным на настоящий момент методом биометрической идентификации личности. Стимулом для развития данной технологии являлось ее повсеместное использование в криминалистике прошлого века. Каждому человеку присущ папиллярный узор отпечатков пальцев, являющийся уникальным, что и позволяет проводить идентификацию. Чаще всего алгоритмами используются характерные точки на отпечатках пальцев, а именно линии узора, одиночные точки, разветвление линии.

Кроме этого собирается информация, касающаяся морфологической структуры отпечатка пальца: относительное положение замкнутых линий папиллярного узора, спиральных и «арочных» линий. Производится преобразование особенностей папиллярного узора в некий код, являющийся уникальным и сохраняющий информативность отпечатка и изображения. В базе данных, которая используется для поиска и сравнения, осуществляется

хранение именно таких «кодов отпечатков пальцев». Величина времени, необходимого для перевода изображения отпечатка пальца в код, и проведения его идентификации обычно не превышает одной секунды и определяется размером базы. Время, необходимое на поднесение руки, в учет не берется.

К преимуществам данного метода можно отнести его высокую достоверность (статистические показатели метода выше, чем у методов идентификации по голосу, росписи, лицу). Также немаловажным является достаточно низкая стоимость устройств, которые осуществляют сканирование изображения отпечатка пальца. Еще следует отметить простоту процедуры сканирования отпечатка. Однако у метода существуют и свои недостатки, такие как подверженность папиллярного узора пальца повреждениям вследствие мелких порезов и царапин. Также практика показывает наличие высокой степени отказа сканирования на предприятиях, насчитывающих несколько сотен сотрудников. Некоторые сканеры теряют адекватность при наличии сухой кожи, плохо идентифицируют пожилых людей. Кроме этого, можно сказать о недостаточной защищенности от подделок изображения отпечатка, которая является следствием повсеместного распространения метода. Для некоторых людей с уникальными данными (особенности, касающиеся температуры тела, влажности) вероятность отказа в доступе составляет 100%.

К уникальным характеристикам человека может быть отнесена радужная оболочка глаза. Формирование рисунка радужки происходит на восьмом месяце внутриутробного развития, окончательная стабилизация происходит в возрасте около двух лет, после чего практически не наблюдается изменений в течение жизни, помимо тех, которые вызваны сильными травмами или резкими патологиями. Метод также относится к одному из наиболее точных в биометрии. Систему идентификации личности по радужной оболочке можно логически разделить на две части: устройство захвата изображения, производящее его первичную обработку и передачу

вычислителю, и сам вычислитель, в обязанности которого входит сравнение изображения с изображениями, хранящимися в базе данных, передача команды о допуске на исполнительное устройство. Временной интервал, необходимый для первичной обработки изображения, составляет в современных системах около  $300 - 500\text{ ms}$ , уровень скорости сравнения полученного изображения с базой данных составляет  $50000 - 150000$  сравнений в секунду на типовом персональном компьютере. Очевидно, что при такой скорости сравнения не накладываются ограничения на применение метода на предприятиях, которые имеют большое количество сотрудников. Благодаря использованию алгоритмов оптимизации поиска и специализированных вычислителей появляется возможность производить идентификацию человека среди жителей целого государства.

Преимуществом этого метода является высокая степень статистической надежности алгоритма. Существует возможность захвата изображения радужной оболочки на расстоянии, составляющем от нескольких сантиметров до нескольких метров, при этом нет необходимости в физическом контакте человека с устройством. Также следует отметить высокую степень защищенности радужной оболочки от повреждений, благодаря чему практически не происходит ее изменения со временем. Кроме того, к преимуществам относится наличие возможности использования большого числа методов, которые защищают от подделки. Недостатками метода можно считать цену системы, которая выше, чем у систем, выполняющих распознавание по отпечатку пальца или распознавание лица. Также характерной является достаточно низкая доступность готовых решений. Типичной является ситуация, при которой происходит продажа дорогих систем под ключ для нужд больших предприятий, таких, как, например, LG или Iridian.

В настоящее время разработано большое количество методов распознавания по геометрии лица. В основе всех из них лежит то факт, что для каждого человека уникальными являются форма черепа и черты лица. Для

многих данная область биометрии считается очень привлекательной, так как людям свойственно узнавать друг друга в первую очередь по лицу. Эту область можно условно разделить на два направления: 2-D распознавание и 3-D распознавание. Каждое из направлений обладает своими достоинствами и недостатками, однако на степень применимости того или иного направления сильное влияние оказывают область требований и применения, которые предъявляются к определенному алгоритму.

Метод 2-D распознавания лица является одним из наиболее неэффективных биометрических методов со статистической точки зрения. Разработан он достаточно давно, ориентирован на применение, в основном, в криминалистике, благодаря чему, собственно, и происходило его развитие. В последнее время были разработаны компьютерные интерпретации метода, благодаря чему повысилась его надежность, однако нельзя не отметить его неуклонное отставание с каждым годом от других биометрических методов идентификации личности. На данный момент, следствии плохих статистических показателей, сфера его применения ограничена мультимодальной (перекрестной) биометрией, а также социальными сетями.

Преимуществом метода можно считать отсутствие необходимости в дорогостоящем оборудовании, а также возможность распознавания на достаточно больших расстояниях от камеры. Недостатками являются низкая степень статистической достоверности, наличие определенных требований к освещению (например, отсутствует возможность регистрации лиц у людей, входящих с улицы, в солнечный день). Многие алгоритмы не дееспособны при различных помехах, таких как наличие очков, бороды, некоторых элементов прически. Также нельзя считать достоинством обязательность фронтального изображения лица, допускающую очень незначительные отклонения. Большинство алгоритмов не способны учитывать возможные изменения мимики лица, другими словами, в них подразумевается, что выражение лица должно быть нейтральным.

Реализация метода 3-D распознавания лица является весьма сложной задачей. Однако, в нынешнее время разработано большое количество методов, которые выполняют 3-D распознавание лица. Методы практически не поддаются сравнению друг с другом, потому что в них применяются различные базы данных и сканеры, далеко не всеми из них выдаются показатели FAR и FRR, они основаны на принципиально различных подходах. Переходным от 2-D к 3-D можно считать метод, в котором реализуются накопления информации о лице. Данный метод обладает лучшими характеристиками, чем 2-D, однако, подобно нему, основан на использовании всего одной камеры. В процессе занесения субъекта в базу данных, субъект поворачивает голову, после чего алгоритмом выполняется соединение изображения воедино и создание 3-D шаблона. Для распознавания же применяется несколько кадров видеопотока. Данный метод может быть отнесен к экспериментальным, так как его готовой реализации пока не замечено.

Наиболее классическим можно считать метод проецирования шаблона. Он заключается в том, что производится проецирование сетки на лицо (объект). После этого камерой делаются снимки со скоростью в несколько десятков кадров в секунду, а обработка полученных изображений производится с помощью специальной программы. Происходит изгибание луча, падающего на искривленную поверхность, причем с ростом кривизны поверхности растет и изгиб луча. В первых разработках использовался источник видимого света, который подавался через «жалюзи». В дальнейшем, была осуществлена замена видимого света на инфракрасный, обладающий некоторыми преимуществами. Чаще всего на первом этапе обработки происходит отбрасывание изображений, на которых либо вообще не видно лица, либо присутствуют посторонние предметы, приводящие к затруднению идентификации. По полученным снимкам осуществляется восстановление 3-D модели лица с выделением и удалением ненужных помех (например, борода, прически, усы, очки). Далее модель анализируется, то есть происходит

выделение антропометрических особенностей, которые и помещаются в уникальный код, заносимый в базу данных. Временной интервал, необходимый для захвата и обработки изображения, составляет 1–2 секунды для лучших моделей. В последнее время интенсивно развивается метод 3-D распознавания по изображению, которое получается с нескольких камер. В качестве примера можно упомянуть фирму Vocord со своим 3-D сканером.

К преимуществам метода можно отнести отсутствие необходимости в контакте со сканирующим устройством, низкую чувствительность к внешним факторам как на самом объекте (появление бороды, очков, изменение прически), так и в его окружении (поворот головы, освещенность). Также преимуществом является наличие высокого уровня надежности, сравнимого с методом идентификации по отпечаткам пальцев. Недостатками же являются высокая стоимость оборудования (на рынке присутствуют комплексы, цена которых выше цены сканеров радужной оболочки). При изменении мимики лица и появлении помех статистическая надежность метода ухудшается. Следует отметить, что метод не является еще хорошо разработанным, особенно в сравнении с очень давно использующейся дактилоскопией, следствием чего является его пока ограниченное применение.

Распознавание по венам руки является новой технологией в биометрической сфере, ее повсеместное применение началось менее десяти лет назад. Инфракрасной камерой делаются снимки внешней или внутренней стороны руки. Формирование рисунка вен происходит за счет поглощения ИК-излучения гемоглобином крови. Вследствие этого, наблюдается уменьшение степени отражения, что и приводит к видимости вен на камере в виде черных линий. Специальной программой, основываясь на полученных данных, осуществляется формирование цифровой свертки. Нет необходимости в контакте человека со сканирующим устройством. Данную технологию можно сравнить по надежности с распознаванием по радужной оболочке глаза, в чем-то она превосходит ее, а в чем-то уступает.

Данный метод обладает рядом преимуществ: отсутствие необходимости в контакте со сканером, высокая степень достоверности, скрытость характеристики (данная характеристика не может быть получена просто «на улице» с помощью, например, фотоаппарата). Существуют и свои недостатки: недопустимость засветки сканера солнечными лучами, а также лучами, исходящими от галогеновых ламп. Помимо этого, из-за наличия некоторых возрастных заболеваний, например, артрита, очень ухудшаются показатели FAR и FRR. Данный метод еще недостаточно изучен по сравнению с другими статистическими биометрическими методами.

До последнего времени было распространено мнение, что самым надежным методом биометрической идентификации и аутентификации личности является метод, в основе которого лежит сканирование сетчатки глаза. В нем содержатся лучшие черты идентификации по радужной оболочке и по венам руки. Сканером считывается рисунок капилляров на поверхности сетчатки глаза. Структура сетчатки является неподвижной, неизменной во времени (не учитывая изменения, вызванные болезнью, например, катарактой). Для сканирования сетчатки применяется инфракрасный свет, имеющий низкую интенсивность, который направлен на кровеносные сосуды на задней стенке глаза через зрачок. Сканеры сетчатки глаза широко распространены в системах контроля доступа на объекты особого уровня секретности, потому что они обладают одним из самых низких процентов отказа в доступе зарегистрированных пользователей, а также практически не допускают ошибочного разрешения доступа. Однако, использование данного биометрического метода сопряжено с целым рядом проблем. В качестве сканера здесь выступает оптическая система с высоким уровнем сложности, а от человека требуется не двигаться в течение значительного времени, пока системой не будет выполнено наведение, что влечет за собой неприятные ощущения.

Преимущества метода: высокая статистическая надежность. Так как подобные системы достаточно мало распространены, вероятность разработки

метода их «обмана» достаточно низка. Недостатками метода можно считать, в первую очередь, сложность системы и длительное время обработки, а также большую стоимость подобных систем. Кроме того, отсутствует широкий рынок предложения, следствием чего является недостаточная интенсивность развития метода.

Метод идентификации по геометрии руки был достаточно распространен еще десять лет назад, он пришел из криминалистики, однако в последние годы наблюдается снижение интереса к нему. В его основе лежит получение геометрических характеристик рук, а именно ширины ладони, длин пальцев. Данный метод, подобно методу сетчатки глаза, является умирающим, и, поскольку он обладает достаточно низкими характеристиками, особого интереса не представляет. Иногда считается, что в системах распознавания по венам используются геометрические методы распознавания. Однако на реальном рынке конкретных предложений в этой области не наблюдается. Помимо этого, зачастую при распознавании по венам осуществляется снимок только ладони, а при распознавании по геометрии – снимок пальцев.

### **1.3 Анализ существующих решений по организации доступа**

На рынке программного и аппаратного обеспечения представлен достаточно широкий спектр систем биометрической идентификации. Однако, не смотря на разнообразие методик, большинство систем ориентировано на обработку именно отпечатков пальцев, и эти решения составляют больше половины рынка программного обеспечения.

Сканеры отпечатков пальцев прошли действительно длинный путь к улучшению. Современные системы оснащены различными датчиками (температуры, силы нажатия и т.п.), которые повышают степень защиты от подделок. С каждым днем системы становятся все более удобными и компактными. Наиболее популярные решения:

- SecuGen Solutions Showcare компании SecuGen [17] решение представлено USB-сканерами для PC, встраиваемыми сканерами, SDK и программным обеспечением для персонального компьютера;
- Bayometric, Inc. [13] – система контроля доступа и учета рабочего времени;
- BioTime [16] – решение использует биометрию для осуществления контроля доступа и учета рабочего времени;
- Сонда [9] - повышение удобства и комфорта граждан за счет внедрения биометрических решений в самых разных сферах жизни человека, от доступа на рабочее место до совершения покупок в магазине.

Сравнительный анализ систем согласно функциональным особенностям представлен в таблица 1.1.

Таблица 1.1 - Сравнительный анализ популярных систем

<b>Возможности</b>	<b>SecuGen Solutions Showcare</b>	<b>Bayometric, Inc.</b>	<b>BioTime</b>	<b>Сонда</b>
Используемые стандарты	ANSI, INCITS, NIST	ANSI, INCITS, NIST	ANSI, INCITS, NIST	ANSI, INCITS, NIST
Точность	Низкие ошибки FAR, FRR	FAR-10-6, FRR-10-2	Низкие ошибки FAR, FRR	Низкие ошибки FAR, FRR
Возможность поддержки работы с различными системами	Кросс-платформенность	Windows решения	Кросс-платформенность	Кросс-платформенность
Возможности учета рабочего времени	Пропускной контроль	Пропускной контроль	Пропускной контроль	Пропускной контроль
Удаленное управление терминалами	Автоматическое управление терминалами под GPRS			
Совместимость с популярными ИС	Microsoft Dynamics, SAP R/3	Microsoft Dynamics, SAP R/3	1C, Microsoft Dynamics, SAP R/3 и др.	1C, Microsoft Dynamics, SAP R/3 и др.
Стоимость решения	От 15000 \$	От 15000 \$	От 20000 руб.	От 30000 руб.

## **2 Разработка проекта по управлению доступом сотрудников в помещения предприятия**

### **2.1 Выбор архитектуры решения и средств разработки**

Организация процесса управления доступом предполагает постоянное отслеживание передвижения сотрудников, а также определение прав на доступ в конкретные помещения посредством карты сотрудника или сравнения отпечатка пальца. Соответственно требуется хранение информации о сотрудниках, шаблонов их отпечатков, параметров помещений и др. При этом возникает необходимость получать данные такого рода различным пользователям в значительной мере удаленным друг от друга, поэтому наиболее эффективной будет использование клиент-серверной архитектуры.

Очевидно, что наиболее популярной технологией организации хранения такого типа данных является технология реляционных баз данных. Таким образом, возникает необходимость выбора наиболее подходящей СУБД.

Критерии выбора СУБД определяются предметной областью, сравнительный анализ СУБД, которые можно использовать в качестве базы хранения данных пользователей для проведения идентификации, проводится согласно основным функциональным характеристикам:

- ограничение на размер базы данных (для определения периода, в рамках которого возможно предоставлять достаточно скоростной доступ к данным по перемещениям сотрудников без архивирования);
- работа с большим количеством пользователей (для создания условий проведения мониторинга в зданиях с большим числом помещений);
- простота интегрирования с интерфейсом, разработанным в RAD-средах (Embarcadero RAD Studio 10.2, Visual Studio 2015 Express);
- возможность использования разных операционных систем при необходимости интеграции с различными устройствами, например,

биометрическими сканерами для получения данных отпечатка пальца сотрудника;

- простота установки и сопровождения работы СУБД;
- возможности использования контроллера доменов, позволяющего осуществлять контроль над областью компьютерной сети, управлять взаимодействиями пользователей и домена, включая процессы входа пользователя в систему, проверку подлинности и поиска в каталоге;
- поддержка современных стандартов SQL.

Основой для системы разработки становится реляционная база данных, сравнительный анализ СУБД представлен в таблица 2.1.

Таблица 2.1 - Сравнительный анализ СУБД (общий)

Параметры	СУБД			
	FireBird 2.5	MySQL 5.5.	MS SQL 2012	PostgreSQL 9.4
Ограничения на размер базы данных	Возможностям и операционной системы	Возможности ми операционно й системы	524 ПБ (10 ГБ - Express)	Возможности ми операционно й системы
Работа с большим количеством пользователей	Да (официального ограничения нет)	Да (официальног о ограничения нет)	Да (до 32767)	Да (официальн ого ограничения нет)
Используемые операционные системы	Кроссплатфор менная	Кроссплатфо рменная	Unix, OS/2, Windows	Кроссплатфо рменная
Поддерживаемый стандарт SQL	SQL-92, SQL-99 (частично)	SQL-99	SQL-2011	SQL-92, SQL-99, SQL-2011

## Окончание таблицы 2.1

Параметры	СУБД			
	FireBird 2.5	MySQL 5.5	MS SQL 2012	PostgreSQL 9.4
Поддержка контроллера доменов	Использование пакета программ Samba	Использование пакета программ Samba	Использование службы Active Directory	Использование пакета программ Samba
Наличие бесплатного программного обеспечения	Да	Да (Community Edition)	Только версия Express	Да

Учитывая необходимость использования для решения задачи управления доступом имитации перемещений сотрудников или сравнения данных по отпечатку пальца сложных инструментов анализа образов, возникает потребность в оценке возможностей СУБД, которые можно использовать при осуществлении доступа к данным (таблица 2.2). К ним относятся: компоненты, классы, драйверы.

Таблица 2.2 – Технологии работы и возможности предоставления доступа к данным

Средства доступа к серверу	СУБД			
	FireBird 2.5	MySQL 5.0.	MS SQL 2012	PostgreSQL 9.4
Компоненты	C/C++, Delphi,	API для Delphi, C, C++, Эйфель, Java, Лисп, Perl, PHP, Python, Ruby,	C/C++	C, C++, Java (через модуль PL/Java)

## Окончание таблицы 2.2

Средства доступа к серверу	СУБД			
	FireBird 2.5	MySQL 5.0.	MS SQL 2012	PostgreSQL 9.4
Классы	Для ADO, ODBC, JDBC (Jaybird)	API для Delphi, C, C++, Эйфель, Java, Лисп, Perl, PHP, Python, Ruby,	Для ADO, ODBC, JDBC	Поддержка для PL/Lua, PL/LOLCODE, PL/Perl, PL/PHP, PL/Python, PL/Ruby
Драйверы	Для Python и PHP, OLE DB, dbExpress, провайдер данных .NET	ODBC, MyODBC	OLE DB	Поддержка для PL/Lua, PL/LOLCODE, PL/Perl, PL/PHP, PL/Python, PL/Ruby

Представленный анализ демонстрирует возможность использования для решения задачи всех указанных СУБД. Поэтому важным фактором при выборе СУБД становится возможность интеграции с автоматизированной системой управления, установленной на предприятии, на котором производится внедрение технологии управления доступом. Наиболее оптимальным вариантом является выбор в пользу решения Microsoft – MSSQL Server 2012 и выше как достаточно быстрой системы и обеспечивающей легкую интеграцию с клиентским приложением из-за большого числа библиотек, обеспечивающих достаточно простую разработку в рамках различных RAD-сред.

При сравнении средств разработки и языков программирования на первый план выходят инструменты и библиотеки, позволяющие осуществить подключение к реляционной СУБД, а также возможностей по работе с графическими изображениями, проведение сравнения изображений, использование специализированных инструментов анализа (нейронных сетей, корреляционного и регрессионного анализа, морфологического анализа) [6 – 11].

Так можно отметить, что популярные сценарные языки, используемые сейчас для разработки веб-приложений, достаточно громоздки при работе со сложными вычислительными алгоритмами, и в этом случае рекомендуется использовать среды разработки с поддержкой высокоуровневых языков типа Delphi или C#, Visual C++ [15, 19, 21].

С целью проведения сравнительного анализа языков программирования для решения поставленной задачи разработки системы управления доступом выбираются следующие параметры (таблица 2.3):

- возможность работы с реляционной базой данных. При этом база данных необходима для хранения персональной информации о пользователях и соответствия отпечатков пальца конкретному физическому лицу;
- необходимость использования сервера приложений. Сервер приложений может быть использован в случае внедрения системы идентификации для доступа к ресурсам или инструментам автоматизированной системы управления компанией;
- наличие инструментов для разработки эргономичного интерфейса;
- наличие библиотек для поддержки математического аппарата, используемого для сравнения изображений и имитирования движения сотрудников;
- простота использования, которая предполагает оценку сложности и громоздкости используемых технологий для реализации.

Таблица 2.3 - Сравнительный анализ языков программирования

Параметры	Язык программирования			
	Java SE 9	Visual C++ 12	Visual C# 4.0	Delphi 10 Lite v.3.0
Наличие инструментов работы с СУБД	JDBC (Jaybird)	OLE DB, ODBC, MyODBC	OLE DB, ODBC, MyODBC	ADO
Среда разработки	Visual Studio, Borland Enterprise Studio	Visual Studio	Visual Studio	Turbo Delphi Borland Enterprise Studio
Наличие механизма работы с математическим аппаратом	MathGL, libfann, fannj, jna, JavaCV	Math.h, math.h, numeric.h, fann, OpenCV	Math.h, math.h, numeric.h, fann, OpenCV	Math, fann, OpenCV (с оберткой)
Простота использования	Средняя	Средняя	Высокая	Высокая
Наличие бесплатного программного обеспечения	Только версия Express	Только версия Express	Только версия Express	Только версия Turbo Delphi Explorer

Указанные выше сравнительные характеристики (таблица 2.3) позволяют говорить о том, что в рамках решаемой задачи наиболее оптимальным становится использование RAD-среды разработки MS Visual Studio 2015 [19]. Наиболее оптимальным представляется использование языка C# [8].

История Visual C# — является недавней. Язык C# появился на свет в июне 2000 г. в результате кропотливой работы большой группы разработчиков компании Microsoft, возглавляемой Андерсом Хейлсбергом (Anders Hejlsberg). Этот человек известен как автор одного из первых компилируемых языков программирования для персональных компьютеров IBM — Turbo Pascal. Кроме того, во время работы в корпорации Borland Андерс Хейлсберг прославился созданием интегрированной среды Delphi (он руководил этим проектом вплоть до выхода версии 4.0).

Появление языка C# и инициативы .NET отнюдь не случайно пришлось на начало лета 2000 г. Именно к этому моменту компания Microsoft

подготовила промышленные версии новых компонентных технологий и решений в области обмена сообщениями и данными, а также создания Internet-приложений (COM+, ASP+, ADO+, SOAP, Biztalk Framework). Несомненно, лучшим способом продвижения этих новинок является создание инструментария для разработчиков с их полноценной поддержкой. В этом и заключается одна из главных задач нового языка C#. Кроме того, Microsoft не могла больше расширять все те же инструменты и языки разработки, делая их все более и более сложными для удовлетворения конфликтующих между собой требований поддержки современного оборудования и обеспечения обратной совместимости с теми продуктами, которые были созданы в начале 1990-х гг. во время первого появления Windows. Ориентация на пользователя совсем не испортила разработки компании, а скорее выделила новое направление. Отправной точкой этого развития явилась разработка для программистов, которая дает возможность не отвлекаться на мелкие детали, а использовать, например, инструменты интерфейса целостно только корректируя их под свои нужды.

C# и .NET являются той самой отправной точкой. Если говорить упрощенно, то .NET представляет собой новую платформу, новый API для программирования в Windows, а C# её новый язык, созданный с нуля, для работы с этой платформой, а также для извлечения всех выгод из прогресса сред разработки и нашего понимания принципов объектно-ориентированного программирования в течение последних 20 лет.

Необходимо отметить, что обратная совместимость не потеряна. Существующие программы будут выполняться, а платформа .NET была спроектирована таким образом, чтобы она могла работать с имеющимся программным обеспечением. Связь между компонентами в Windows сейчас почти целиком осуществляется при помощи COM. С учетом этого .NET обладает способностью создавать оболочки (wrappers) вокруг существующих компонентов COM, так что компоненты .NET могут общаться с ними, и

создавать оболочки вокруг компонентов .NET, что позволяет им выглядеть как обычные СОМ-компоненты.

Авторы C# стремились создать язык, сочетающий простоту и выразительность современных объектно-ориентированных языков (вроде Java) с богатством возможностей и мощью C++. По словам Андерса Хейлсберга, C# позаимствовал большинство своих синтаксических конструкций из C++. В частности, в нем присутствуют такие удобные типы данных, как структуры и перечисления (другой потомок C++ — Java — лишен этих элементов, что создает определенные неудобства при программировании). Синтаксические конструкции C# унаследованы не только от C++, но и от Visual Basic. Например, в C#, как и в Visual Basic, используются свойства классов. Как C++, C# позволяет производить перегрузку операторов для созданных вами типов Java не поддерживает ни ту, ни другую возможность. C# — это фактически гибрид разных языков. При этом C# синтаксически не менее (если не более) чист, чем Java, так же прост, как Visual Basic, и обладает практически той же мощью и гибкостью, что и C++.

Среди особенностей языка C# можно выделить следующие:

- полный и хорошо определенный набор основных типов;
- встроенная поддержка автоматической генерации XML-документации, автоматическое освобождение динамически распределенной памяти;
- возможность отметить классов и методов атрибутами, определяемыми пользователем. Это может быть полезно при документировании и способно воздействовать на процесс компиляции (например, можно пометить методы, которые должны компилироваться только в отладочном режиме);
- полный доступ к библиотеке базовых классов .NET, а также легкий доступ к Windows API (если это действительно необходимо);

- указатели и прямой доступ к памяти, если они необходимы. Однако язык разработан таким образом, что практически во всех случаях можно обойтись и без этого;

- поддержка свойств и событий в стиле VB;
- простое изменение ключей компиляции. Позволяет получать исполняемые файлы или библиотеки компонентов .NET, которые могут быть вызваны другим кодом так же, как элементы управления ActiveX (компоненты COM).
- возможность использования C# для написания динамических web-страниц ASP.NET.

Все выше сказанное дает право говорить о том, что простота и удобство среды программирования Microsoft Visual Studio 2012 и возможности языка C# стали основой в выборе инструментов для разработки программного обеспечения данного исследования.

## **2.2 Проектирование базы данных информационной системы доступа**

В процессе анализа общего массива данных, которые необходимы для осуществления основных функций системы в рамках компании по получению прав доступа в определенные помещения компании выделены основные сущности:

- сущность «Сотрудники» хранит данные о сотрудниках для которых определяется технология доступа в определенные помещения компании;
- сущность «Должности» хранит данные о должностном составе компании и привязывается к конкретным сотрудникам;
- сущность «Подразделения» хранит данные о структуре компании для определения разграничений по осуществлению доступа в различные помещения;

- сущность «Помещения» хранит данные о помещениях, для которых вводится особый режим доступа;
- сущность «Разрешения» хранит данные о выданных разрешениях на доступ в конкретные помещения компании выбранным сотрудникам;
- сущность «Журнал перемещений» хранит данные о движении сотрудника по помещениям с учетом времени входа и выхода из конкретных помещений, включая проходную.

Спецификации по выделенным сущностям представлены в таблице 2.4 – таблице 2.9.

Таблица 2.4 - Спецификация атрибутов сущности «Сотрудники»

<b>Название атрибута</b>	<b>Описание атрибута</b>	<b>Тип данных</b>	<b>Диапазон значений</b>	<b>Пример атрибута</b>
<u>Код сотрудника</u>	Число, однозначно определяющее каждого сотрудника	Числовой	> 0	4587
Фамилия_сотрудника	Фамилия сотрудника	Текст	–	Петров
Имя_сотрудника	Имя сотрудника	Текст	–	Петр
Отчество_сотрудника	Отчество сотрудника	Текст	–	Петрович
Отпечаток	Отпечаток (ссылка на расположение файла отпечатка пальца с наименованием файла)	Текст	-	101_1.tif.
Ключ_безопасности	Ключ безопасности	Текст		-
Номер карты	Номер карты доступа	Числовой	> 0	4587 5678 356

Таблица 2.5 - Спецификация атрибутов сущности «Должности»

<b>Название атрибута</b>	<b>Описание атрибута</b>	<b>Тип данных</b>	<b>Диапазон значений</b>	<b>Пример атрибута</b>
<u>Код должности</u>	Число, однозначно определяющее каждую должность.	Числовой	> 0	4587
Наименование_должности	Наименование должности	Текст	–	Менеджер по продажам

Таблица 2.6 - Спецификация атрибутов сущности «Подразделения»

<b>Название атрибута</b>	<b>Описание атрибута</b>	<b>Тип данных</b>	<b>Диапазон значений</b>	<b>Пример атрибута</b>
<u>Код подразделения</u>	Число, однозначно определяющее каждого ответственного.	Числовой	> 0	4587
Наименование_подразделения	Наименование подразделения	Текст	—	Отдел продаж

Таблица 2.7 - Спецификация атрибутов сущности «Помещения»

<b>Название атрибута</b>	<b>Описание атрибута</b>	<b>Тип данных</b>	<b>Диапазон значений</b>	<b>Пример атрибута</b>
<u>Код помещения</u>	Число, однозначно определяющее каждое помещение.	Числовой	> 0	4587
Наименование_помещения	Наименование помещения	Текст	—	Склад уникальных товаров

Таблица 2.8 - Спецификация атрибутов сущности «Журнал перемещений»

<b>Название атрибута</b>	<b>Описание атрибута</b>	<b>Тип данных</b>	<b>Диапазон значений</b>	<b>Пример атрибута</b>
<u>Код перемещения</u>	Число, однозначно определяющее каждое перемещение между помещениями.	Числовой	> 0	4587
Данные входа	Дата и время входа в помещение	Дата	≤ текущая дата	21.04.2018
Данные выхода	Дата и время выхода из помещения	Дата	≤ текущая дата	21.04.2018
Помещение	Данные помещения	Текст	—	Склад уникальных товаров
Сотрудник	Данные сотрудника	Текст	—	Петров

Таблица 2.9 - Спецификация атрибутов сущности «Разрешения»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
<u>Код разрешения</u>	Число, однозначно определяющее каждый документ разрешения.	Числовой	> 0	4587
Дата разрешения	Дата разрешения	Дата	≤ текущая дата	21.04.2018

Разработанная концептуальная модель имеет вид (рисунок 2.1):

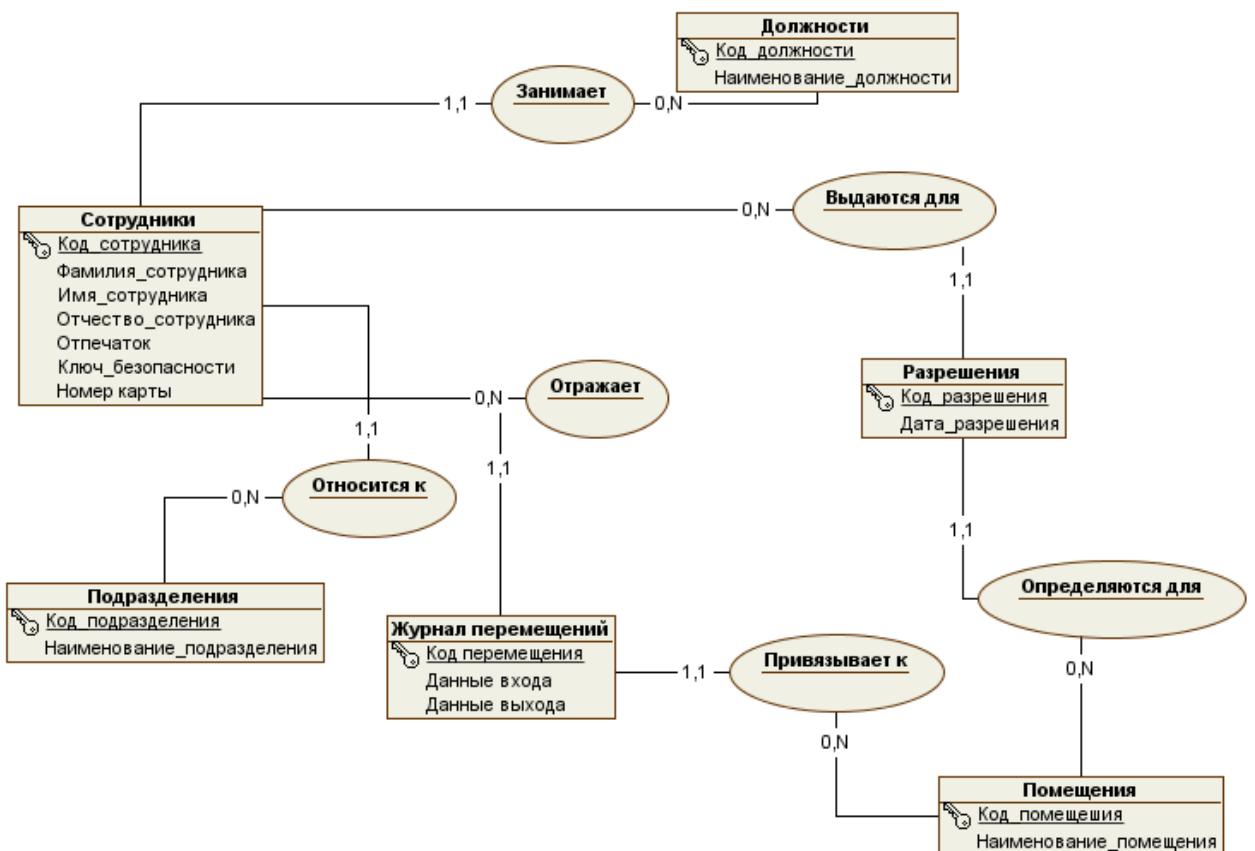


Рисунок 2.1 – Концептуальная модель данных

На основании концептуальной модели после очистки и проверки на валидацию построена логическая модель данных с учетом типов данных и условий, накладываемых на значения (рисунок 2.2)

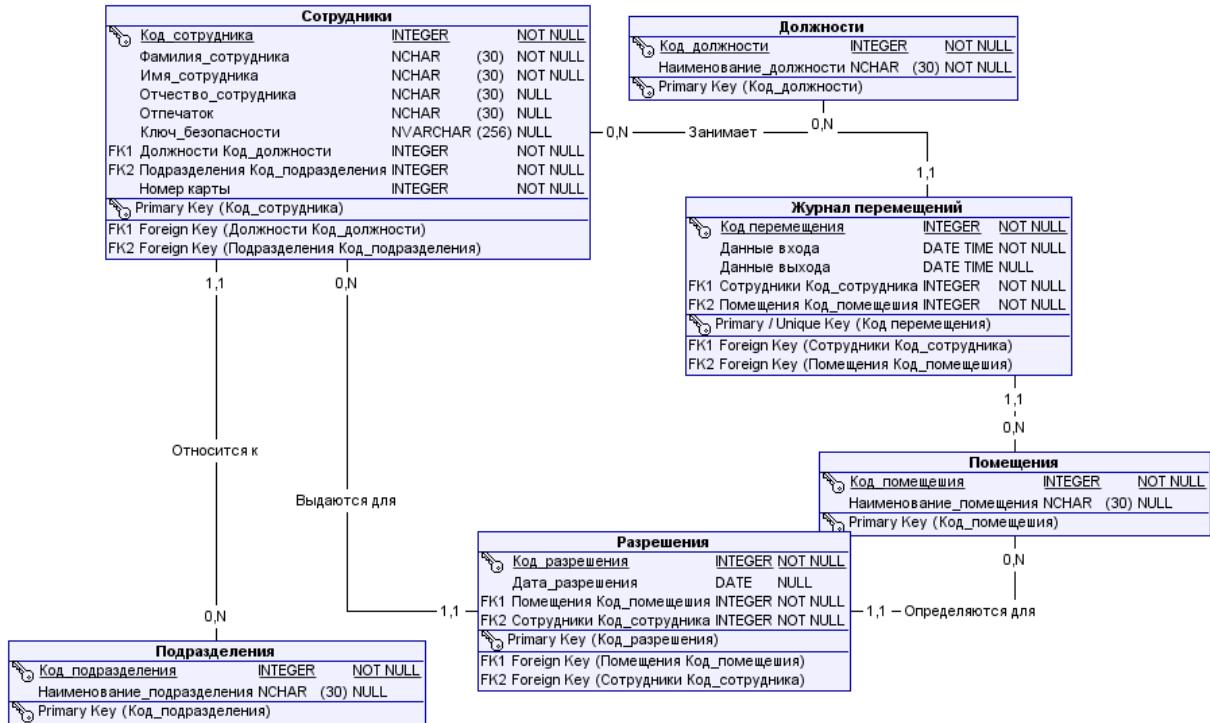


Рисунок 2.2 – Логическая модель данных

С учетом выбранной СУБД MSSQL Server 2012 физическая модель данных имеет вид (рисунок 2.3).

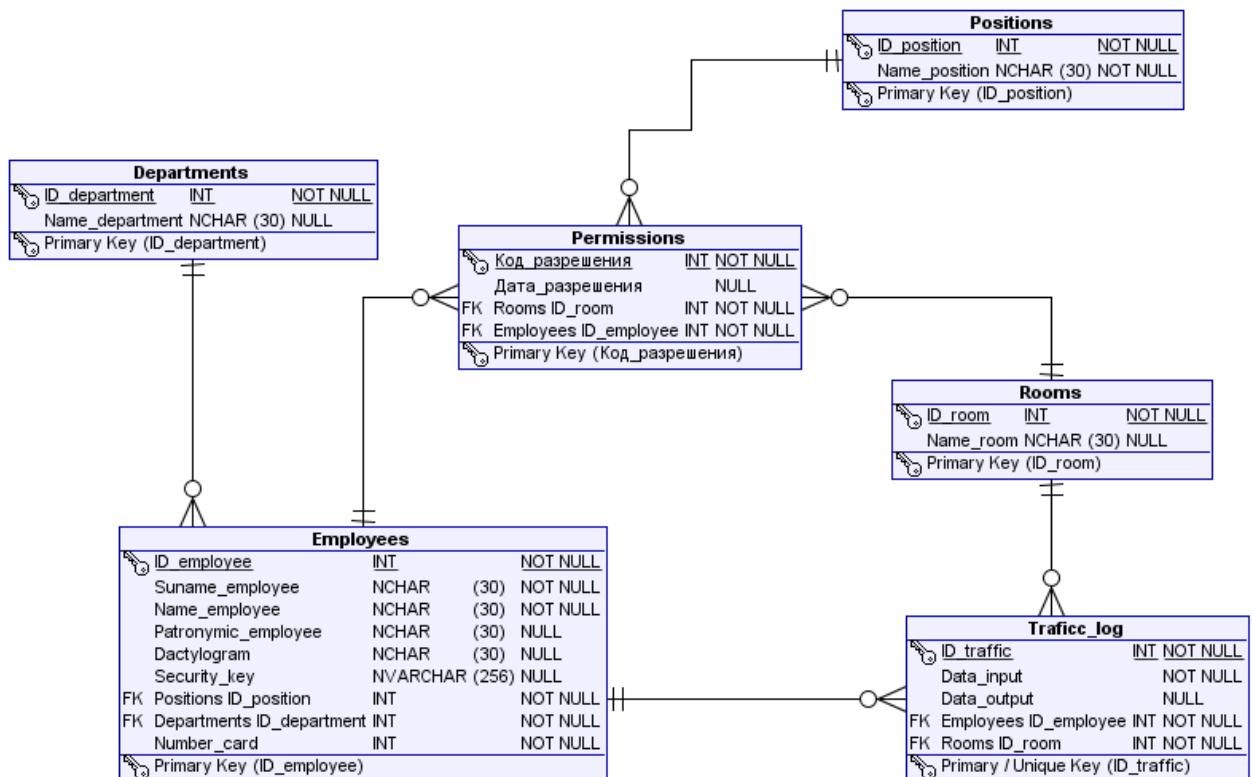


Рисунок 2.3 – Физическая модель данных

Построенная структура данных позволяет оперативно получать информацию о сотрудниках и их перемещениях, а также манипулировать информацией о помещениях, подразделениях и должностях сотрудников.

### **2.3 Разработка интерфейса системы управления доступом**

Технология использования программы, как средства по обеспечению доступа или учета рабочего времени предполагает обязательное использование в системной архитектуре проекта реляционной базы данных, хранящей данные о сотрудниках, отпечатках пальцев, местах доступа, правах доступа и т.п. Таким образом, необходимым является выделение базы данных, а также средства управления (СУБД), поэтому используется двухзвенная архитектура, позволяющая реализовать не только сам доступ, но и вести учет получения доступа различными сотрудниками.

Как было указано в разделе по выбору программных средств для разработки решения в качестве СУБД выступает MSSQL Server 2012, а клиентское приложение получает доступ к данным посредством технологии ODBC.

Microsoft Visual Studio – это линейка продуктов, разработанных компанией Microsoft, которая состоит из интегрированной среды разработки программного обеспечения, а также ряда других инструментальных средств. Продукты этой линейки дают возможность создавать как консольные приложения, так и приложения с графическим интерфейсом, поддерживающие технологию Windows Form, и многие другие технологии.

В качестве вида разрабатываемого приложения принято решение использовать приложение с графическим интерфейсом, которое поддерживает технологию Windows Forms.

Windows Forms дает возможность создавать приложения – так называемые интеллектуальные клиенты. Под «интеллектуальным клиентом» понимается приложение, имеющее богатый графический интерфейс. Такое

приложение легко развертывается и обновляется, оно способно функционировать при наличии или отсутствии подключения к Интернету, а также использует доступ к ресурсам на локальном компьютере более безопасного уровня по сравнению с традиционными приложениями Windows.

Таким образом, Windows Forms – это технология интеллектуальных клиентов для .Net Framework; это набор управляемых библиотек, которые обеспечивают выполнение наиболее распространенных задач приложений (к примеру, чтение и запись в файловую систему). Благодаря среде разработки подобной Visual Studio существует возможность создания приложений Windows Forms, отображающих информацию, запрашивающих ввод от пользователей и обменивающихся данными с удаленными компьютерами по сети.

В Windows Forms видимой поверхностью является форма. На ней происходит отображение информации для пользователя. Как правило, построение приложения Windows Forms происходит в виде помещения разнообразных элементов управления на форму с последующим написанием кода для реагирования на соответствующие действия пользователя, такие как нажатия клавиш либо щелчки мыши. Здесь под элементом управления понимается отдельный элемент, принадлежащий пользовательскому интерфейсу и предназначенный для ввода или отображения данных.

В процессе выполнения пользователем каких-либо действий с одним из элементов управления формы или формы в целом, происходит событие, реакция приложения на такое событие происходит с помощью кода и происходит обработка данного события при его возникновении.

При помощи Windows Forms на формы возможно добавление большого набора элементов управления, а именно текстовых полей, кнопок, раскрывающихся списков, переключателей, веб-страниц и т.д. Также следует отметить, что в случае, когда среди стандартных не существует элемента управления, удовлетворяющего пользовательским потребностям, есть

возможность создания своего собственного пользовательского элемента управления. Для этого необходимо использовать класс `UserControl`.

В составе Windows Forms можно встретить элементы пользовательского интерфейса, имеющие расширенные функции, которые находятся в соответствии с возможностями таких мощных приложений как Microsoft Office. Благодаря использованию элементов управления `ToolStrip` и `MenuStrip`, создаются панели инструментов и меню, которые содержат текст и рисунки, отображающие подменю и аккумулирующие в себе другие элементы управления (к примеру, текстовые поля, а также поля с выпадающим списком).

Используя конструктор `Windows FormsVisual Studio`, который поддерживает перетаскивание достаточно легко создать приложение Windows Forms. Для этого вполне достаточно выделить необходимый элемент управления курсором и затем разместить его в нужном месте на форме. Конструктор обладает такими удобными средствами, как линии сетки и привязка линий – которые помогут выровнять элементы управления и преодолеть связанные с этим трудности. При использовании `Visual Studio` либо при компиляции из командной строки, используя элементы управления `FlowLayoutPanel`, `TableLayoutPanel`, `SplitContainer`, можно создавать весьма сложные разметки формы с приложением минимальных усилий.

В случае необходимости создания своих собственных элементов пользовательского интерфейса, существует пространство имен `System.Drawing`, которое насчитывает в себе большой набор классов, которые помогут при визуальном отображении кругов, линий, а также других фигур непосредственно на форме.

Структура программы представлена на рисунок 2.4. Программы включает в себя двенадцать модулей. Первый модуль «`Main_Form.cs`» – главный модуль, который имеет информативный характер и предназначен для управления работой всего приложения. Для ввода информации в справочник «Подразделения» разработан модуль «`Departments_Form.cs`». Модуль «`Positions_Form.cs`» отвечает за ввод и редактирование информации о

должностях. Аналогичную функцию выполняет модуль «Rooms\_Form.cs» - в нем находятся функции и методы управления данными об имеющихся помещениях.

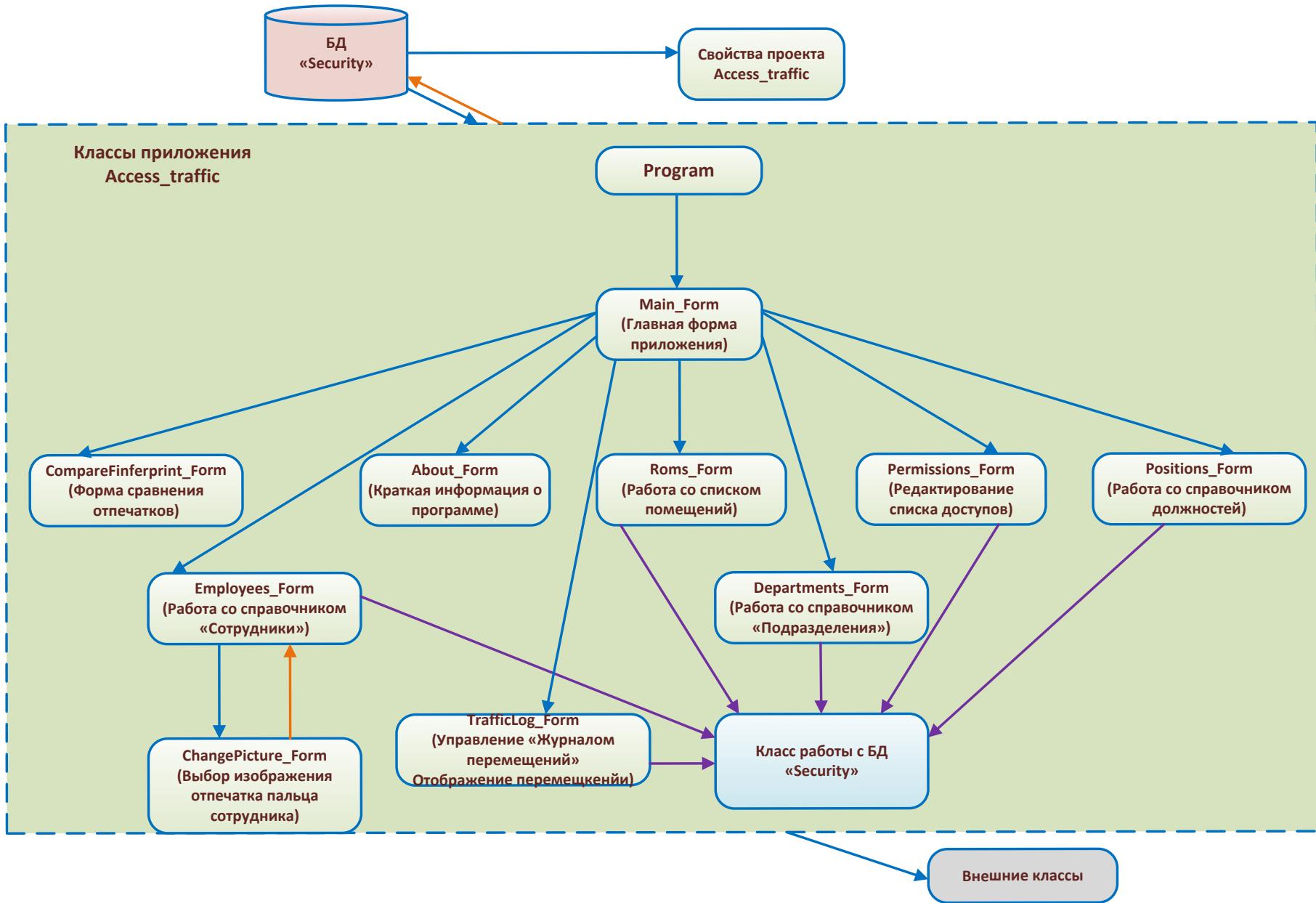
В модуле «Employees\_Form.cs» производится ввод и редактирование информации о сотруднике, а также основные методы формирования уникального 256-битного ключа по введенному отпечатку пальца (все основные библиотеки используются именно в этом модуле).

Для заполнения данных о доступах сотрудников в определенные помещения разработан модуль «Permission\_Form.cs». Выполнение сравнения двух экземпляров отпечатков пальцев производится в модуле «CompareFingerprint\_Form.cs». Модуль «ChangePicture\_Form.cs» предназначен для смены эталонного изображения отпечатка пальца сотрудника. За ведение журнала перемещений и отображение движения сотрудника по зданию отвечает модуль «TrafficLog\_Form.cs»

И, наконец, для вывода краткой информации о приложении служит модуль «AboutForm.cs».

Во всех модулях предусмотрена возможность ввода и редактирования, а также удаления – это необходимо для управления процессом ввода, редактирования и сохранения данных в БД (обеспечивается ввод, редактирование, удаление и сохранение данных всех таблиц БД, и вывод содержимого таблиц БД).

Рисунок 2.4 – Структура программного продукта



## 2.4 Контрольный пример реализации решения

В качестве иллюстрации разработанного решения целесообразным является рассмотрение принципов работы программы на конкретном примере.

После запуска приложения на экране появляется окно авторизации пользователя в программе (рисунок 2.5).

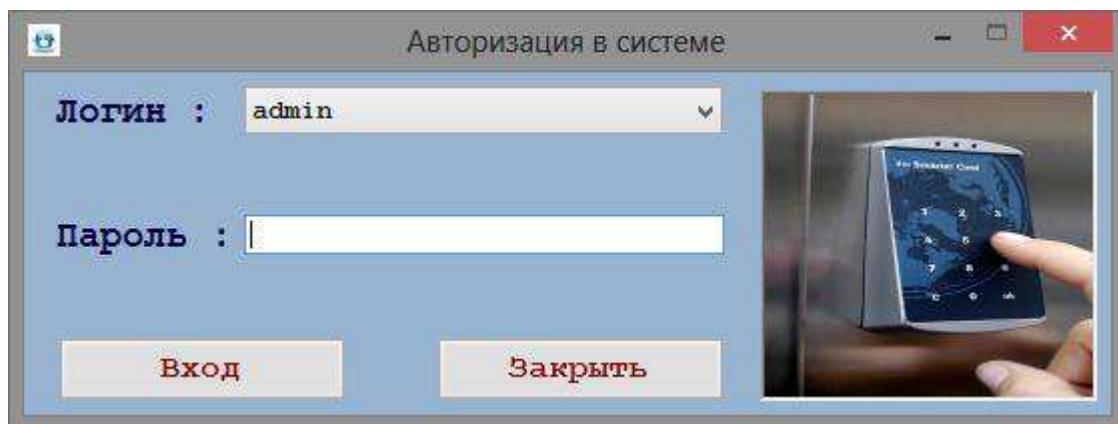


Рисунок 2.5 – Структура программного продукта

Пользователь выбирает свой логин из выпадающего списка, а затем вводит пароль. Если пароль неправильный, то на экран выдается соответствующее сообщение и предлагается повторить ввод пароля. В случае неверного ввода пароля заданное количество раз (на данный момент времени — это число в программе установлено равное трем, но может быть изменено), на экран выдается уведомление, после чего работа программы завершается (рисунок 2.6).

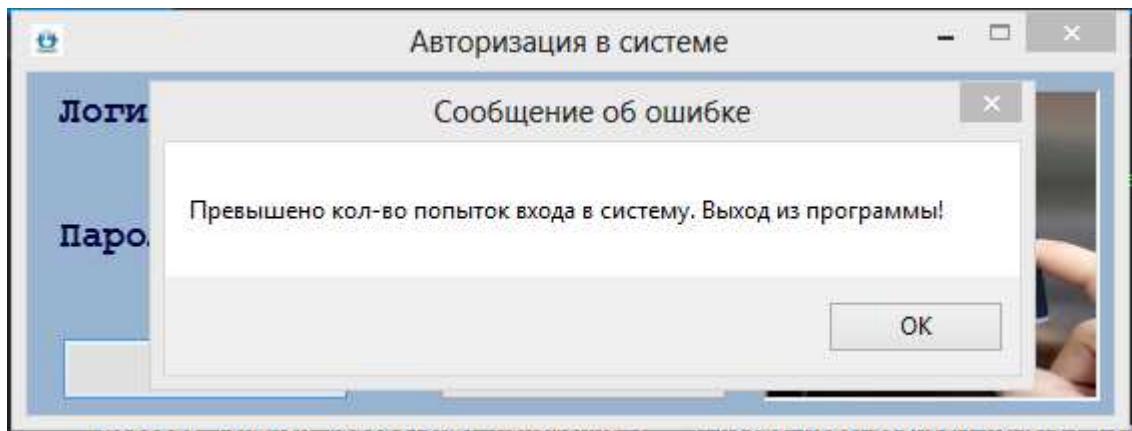


Рисунок 2.6 – Уведомление о превышении числа попыток входа в систему

В случае корректного ввода пароля пользователь попадает на главную форму приложения.

Следует отметить, что в системе реализован контроль прав доступа. Так пользователь с правами администратора обладает доступом ко всем функциональным возможностям программы. Главная форма приложения в данном случае выглядит так, как показано на рисунок 2.7.

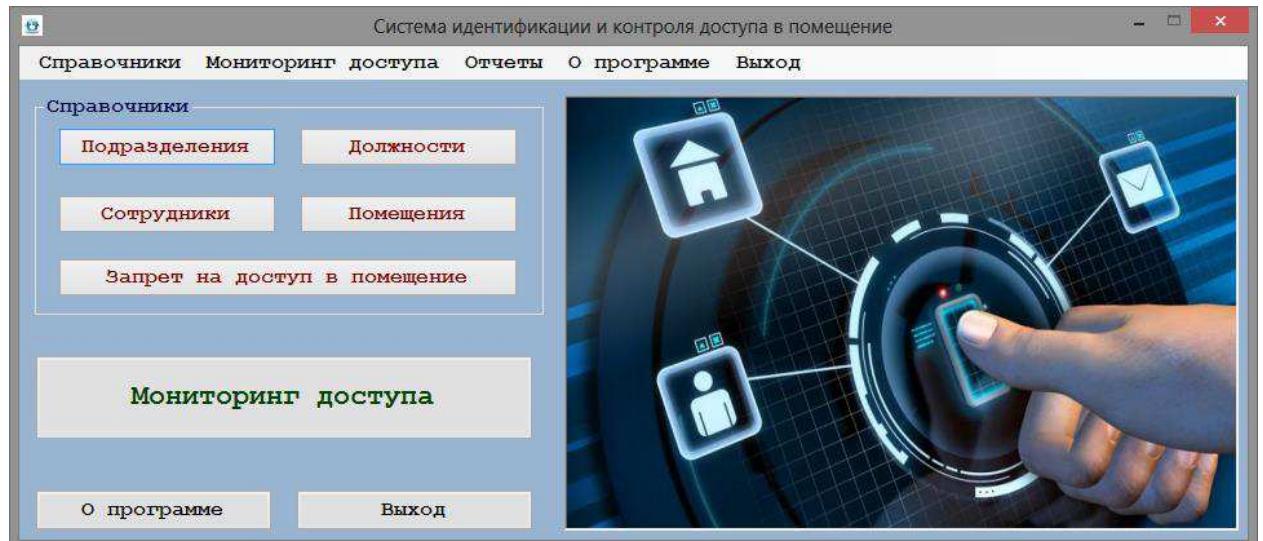


Рисунок 2.7 – Главная форма программы для пользователя с правами администратора

Обычному пользователю недоступна работа со справочниками, следовательно, главная форма имеет вид, представленный на рисунок 2.8.

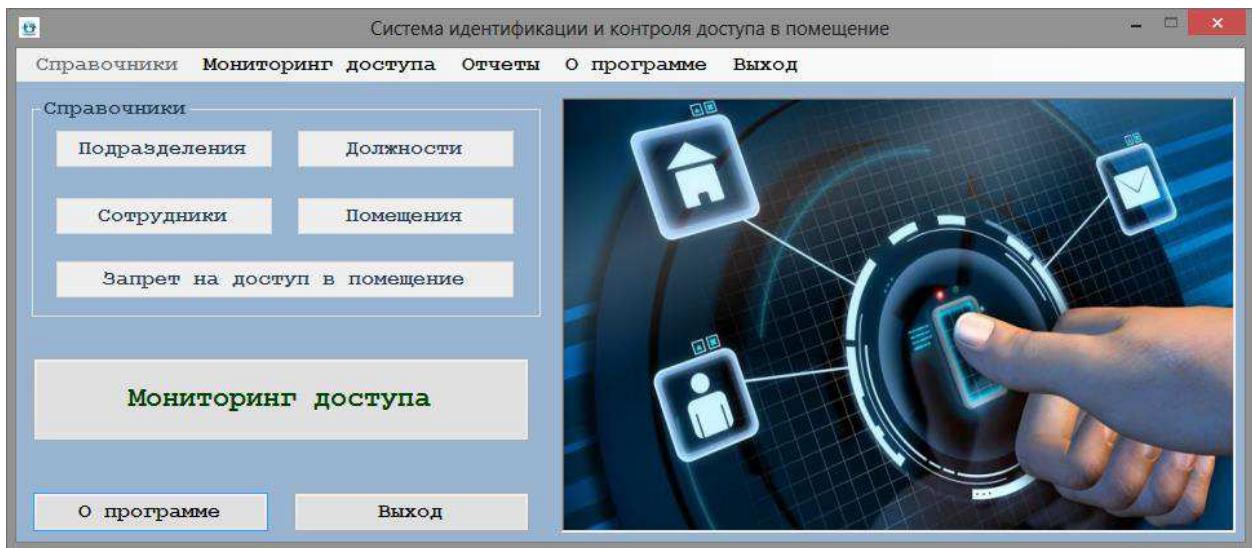


Рисунок 2.8 – Главная форма программы для обычного пользователя

В дальнейшем описании функциональных возможностей приложения будет подразумеваться, что был осуществлен вход в систему пользователем, наделенным правами администратора.

Как видно из внешнего вида главной формы (рисунок 2.7), пользователь может осуществить требуемое ему действие двумя способами: либо выбрав соответствующий пункт меню в главном меню программы (верхняя часть формы), либо нажав на соответствующую кнопку в группе кнопок (левая часть формы).

В системе предусмотрено ведение нескольких справочников.

Справочник «Подразделения» (рисунок 2.9) отображает информацию о существующих подразделениях на предприятии.

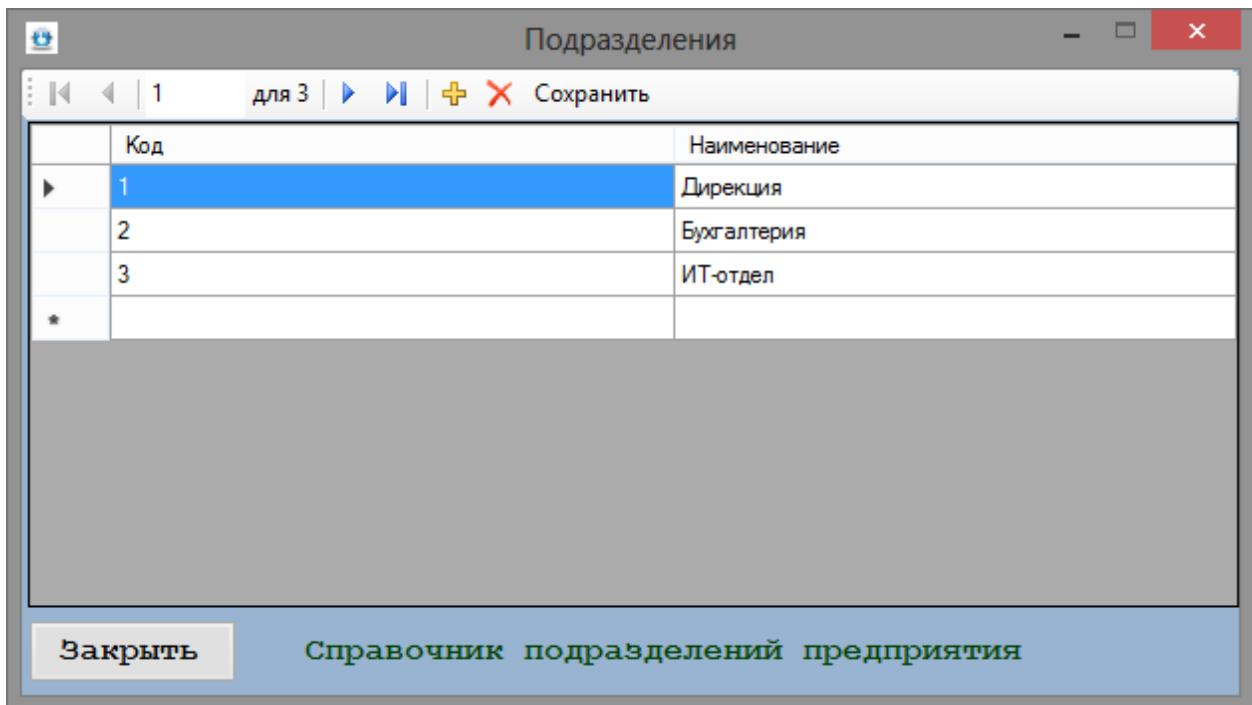


Рисунок 2.9 – Справочник подразделений предприятия

Следует отметить, что работа с данным и всеми последующими справочниками реализована идентичным способом. Пользователь может в табличной форме добавлять новый элемент справочника, изменять или удалять существующий элемент. Для перехода между записями используется панель навигации, которая расположена в верхней части формы. После выполнения всех необходимых изменений необходимо нажать на кнопку «Сохранить», которая расположена на панели навигации, после чего вся внесенная информация будет записана в соответствующую таблицу базы данных.

Для данного справочника вводится только одно поле – наименование подразделения предприятия.

Аналогичный вид имеет справочник «Должности» (рисунок 2.10), где вводится только наименование должностей.

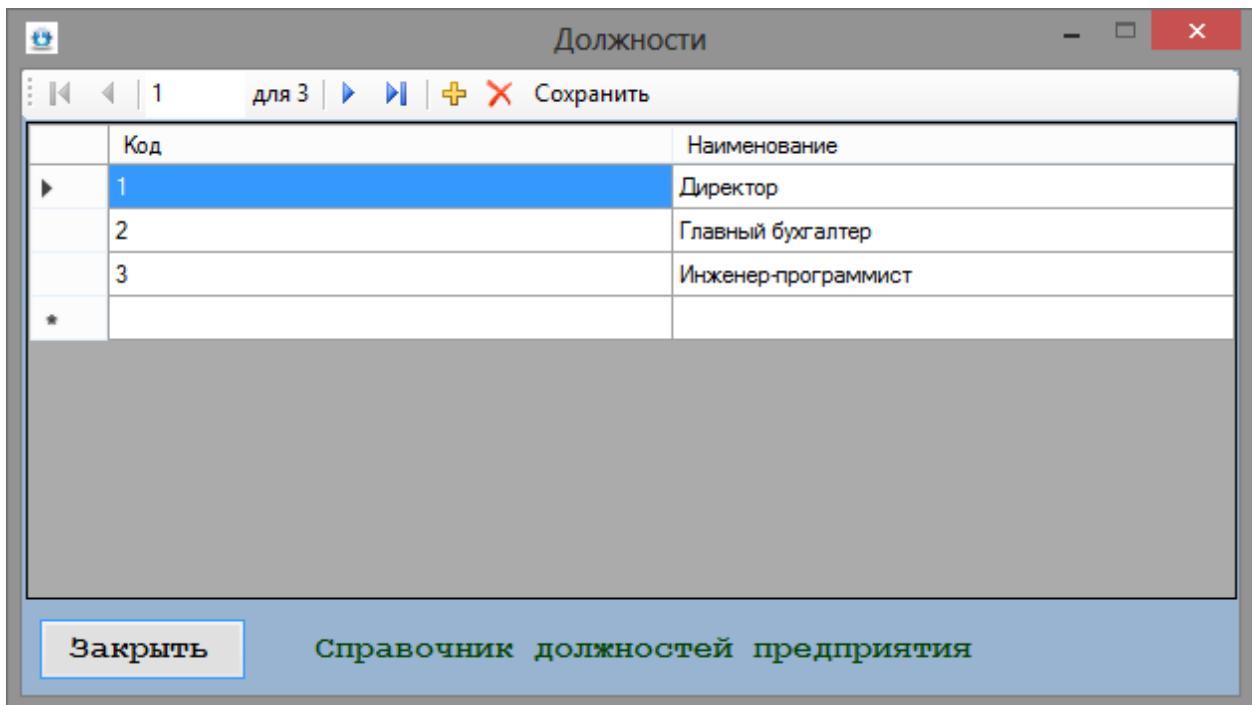


Рисунок 2.10 – Справочник должностей сотрудников

Справочник «Сотрудники» представлен на рисунок 2.11.

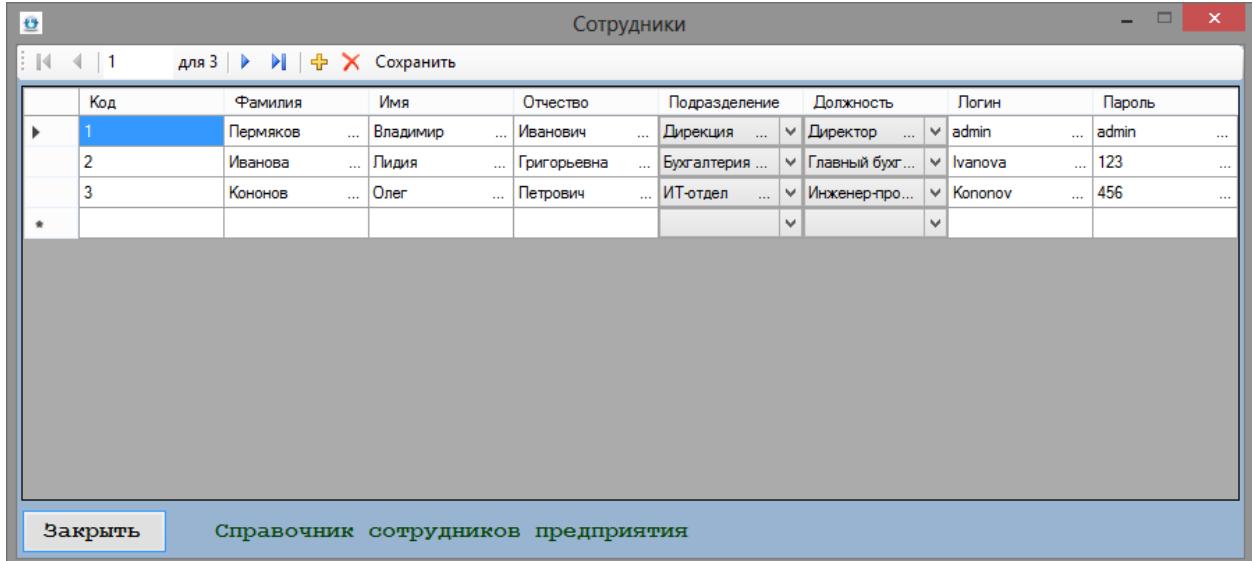


Рисунок 2.11 – Справочник сотрудников предприятия

Пользователь вносит информацию о фамилии, имени, отчестве сотрудника, наименовании подразделения, где работает сотрудник (выбирается из выпадающего списка), занимаемой им должности (выбирается из выпадающего списка), логине и пароле его в системе (последние два поля

не являются обязательными к заполнению, так как сотрудник может и не иметь доступа в данную программу).

Справочник помещений предприятия приведен на рисунок 2.12.

Код	Наименование
1	Серверная
2	Приемная
3	Бухгалтерия
4	Офис
*	

Рисунок 2.12 – Справочник помещений предприятия

Здесь заполнению подлежит только наименование помещения. Следует также отметить, что помещение с именем «Офис» и в данном случае с кодом «4» предназначено для идентификации того, что сотрудник находится на территории офиса и нешел еще не в одно из помещений. Другими словами, при приходе на работу и идентификации на проходной он попадает в помещение, имеющее название «Офис».

И, наконец, справочник «Запрет на доступ в помещение» имеет вид, представленный на рисунок 2.13.

Пользователь заполняет поля с наименованием помещения (выбирается из выпадающего списка), фамилией сотрудника (выбирается из выпадающего списка), а также датой, когда выбранному сотруднику запрещен доступ в выбранное помещение.

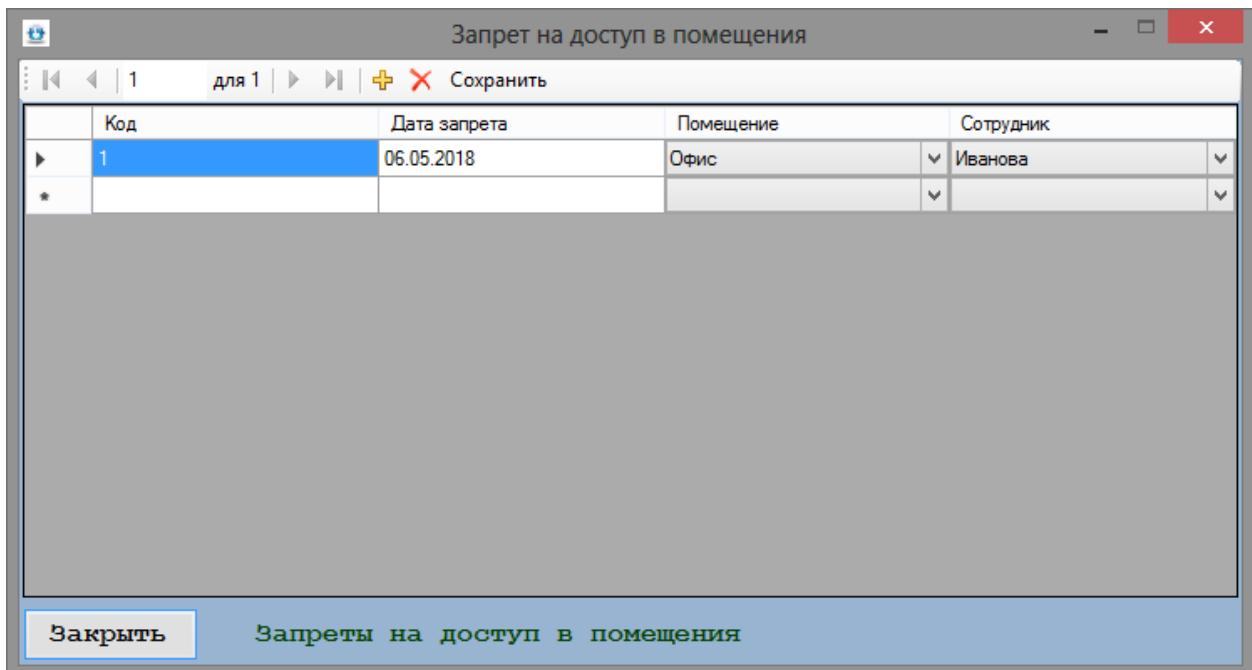


Рисунок 2.13 – Справочник «Запрет на доступ в помещение»

В примере на рисунок 2.13 сотруднику Ивановой 06.05.2018 г. запрещен доступ в помещение «Офис» (другими словами, ей запрещен вообще вход на территорию предприятия).

После заполнения справочников необходимо сделать переход на форму мониторинга доступа сотрудников в помещения предприятия либо путем выбора, соответствующего меню в главном меню программы, либо нажатием соответствующей кнопки из группы кнопок.

Форма мониторинга доступа приведена на рисунок 2.14.

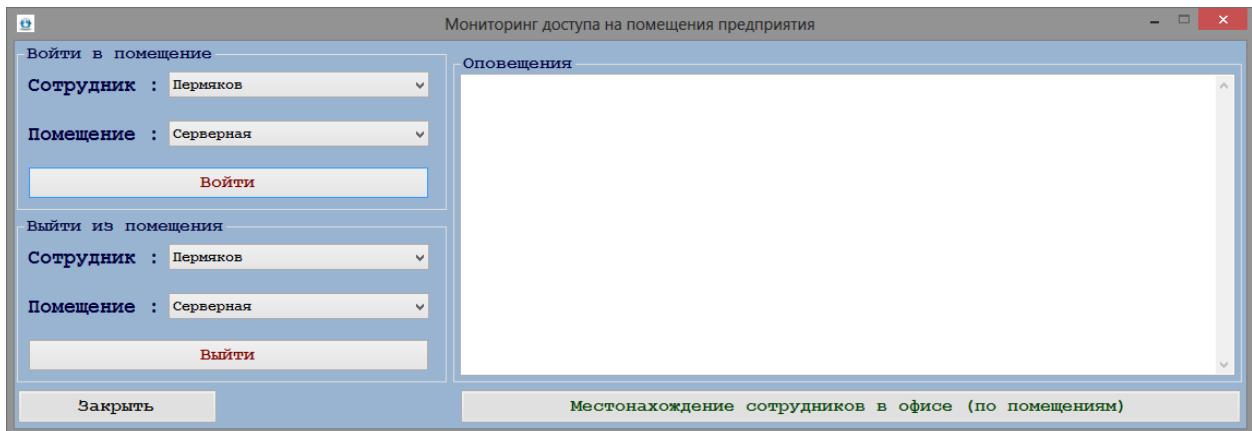


Рисунок 2.14 – Форма «Мониторинг доступа на помещение предприятия»

В данной форме слева на панели «Войти в помещение» пользователь может выбрать фамилию сотрудника (выбирается из выпадающего списка), наименование помещения (выбирается из выпадающего списка), после чего нажать кнопку «Войти», после чего будет осуществлена попытка идентификации доступа в выбранное помещение.

Аналогично, для выхода из помещения на панели «Выйти из помещения» пользователь может выбрать фамилию сотрудника (выбирается из выпадающего списка), наименование помещения (выбирается из выпадающего списка), после чего нажать кнопку «Выйти», после чего будет осуществлена попытка идентификации для выхода из выбранного помещения.

Весь процесс мониторинга контроля доступа отображается в окне журнала событий, расположенному в правой части формы.

Следует отметить, что при попытке входа в помещение может возникнуть несколько ситуаций, когда в доступе будет отказано. Аналогичная ситуация возникает и при попытке выйти из помещения.

В случае удачной авторизации входа/выхода делается автоматическая запись в соответствующую таблицу базы данных.

Пример журнала логов событий приведен на рисунок 2.15.

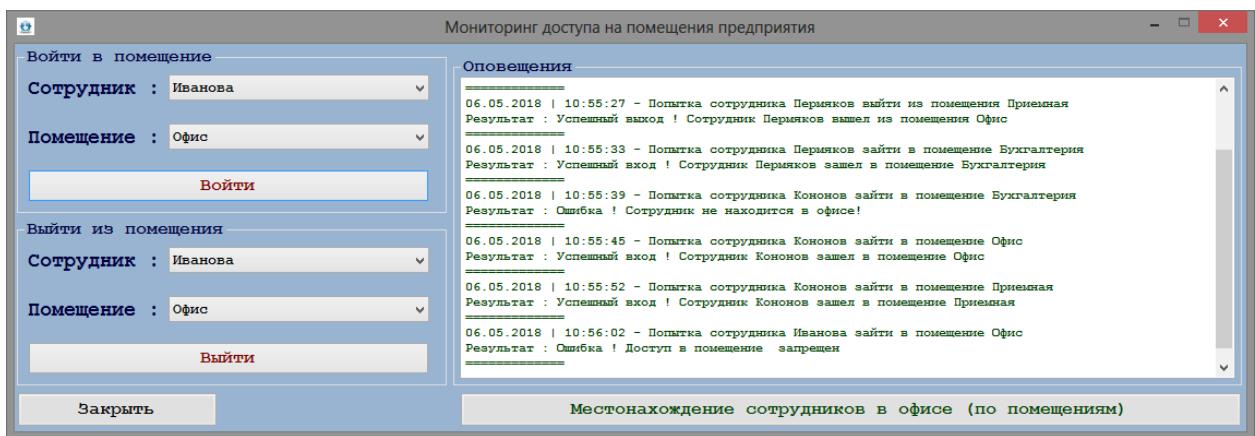


Рисунок 2.15 – Пример регистрации журнала логов событий

При попытке сотрудницы Ивановой зайти в офис будет выдан отказ в доступе, так как на текущую дату у нее стоит запрет посещения офиса (рисунок 2.16).

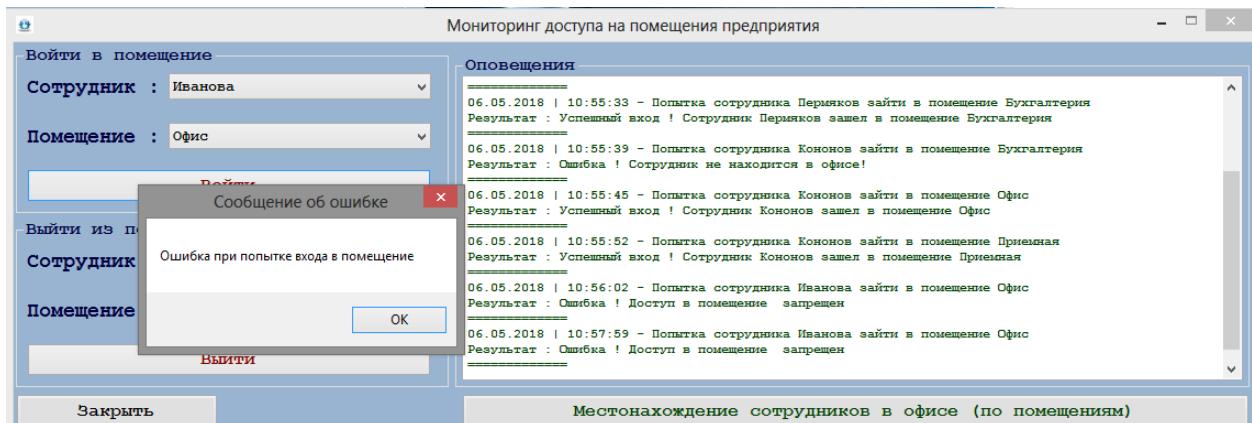


Рисунок 2.16 – Пример отказа при попытке входа в помещение

Также в нижней части формы мониторинга доступа расположена кнопка «Местонахождение сотрудников в офисе (по помещениям)». Нажатие данной кнопки инициирует вызов формы статистики, кто и где находится на предприятии в данный момент времени. Пример данной формы приведен на рисунок 2.17.

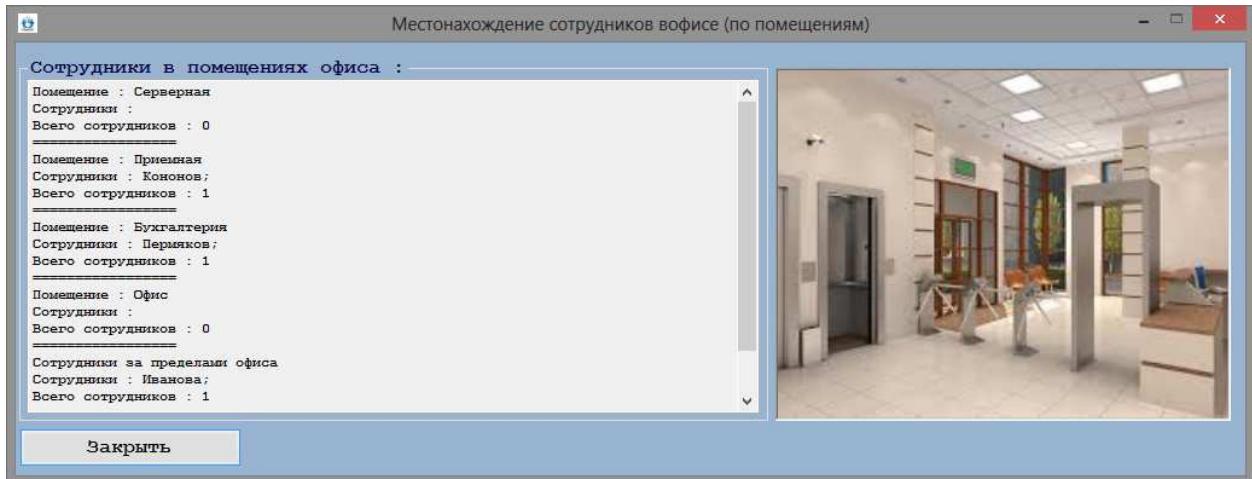


Рисунок 2.17 – Форма статистики

Как видно из рисунка 2.17, на экран выводится последовательно: наименование помещения, кто там находится в данный момент (по фамильно), общее количество людей в помещении, затем выводится информация о сотрудниках, находящихся в данный момент за пределами офиса

(пофамильно), внизу указывается общее количество сотрудников на предприятии.

Также нельзя не упомянуть о том, что выбор пункта меню «Отчеты – Журнал перемещений по офису» в меню на главной форме приложения открывает журнал перемещений по офису (рисунок 2.18).

Журнал перемещений по офису					
Код	Сотрудник	Помещение	Дата и время входа	Дата и время выхода	
21	Пермяков	Офис	06.05.2018 10:55		
22	Пермяков	Приемная	06.05.2018 10:55		
23	Пермяков	Приемная		06.05.2018 10:55	
24	Пермяков	Бухгалтерия	06.05.2018 10:55		
25	Кононов	Офис	06.05.2018 10:55		
26	Кононов	Приемная	06.05.2018 10:55		
*					

Рисунок 2.18 – Пример журнала перемещений по офису

В этом отчете указывается фамилия сотрудника, наименование помещения, дата и время входа в помещение, дата и время выхода из помещения.

При выборе пункта меню (или нажатии кнопки) «О программе» на экран выводится краткая информация о разработанном приложении (рисунок 2.19).

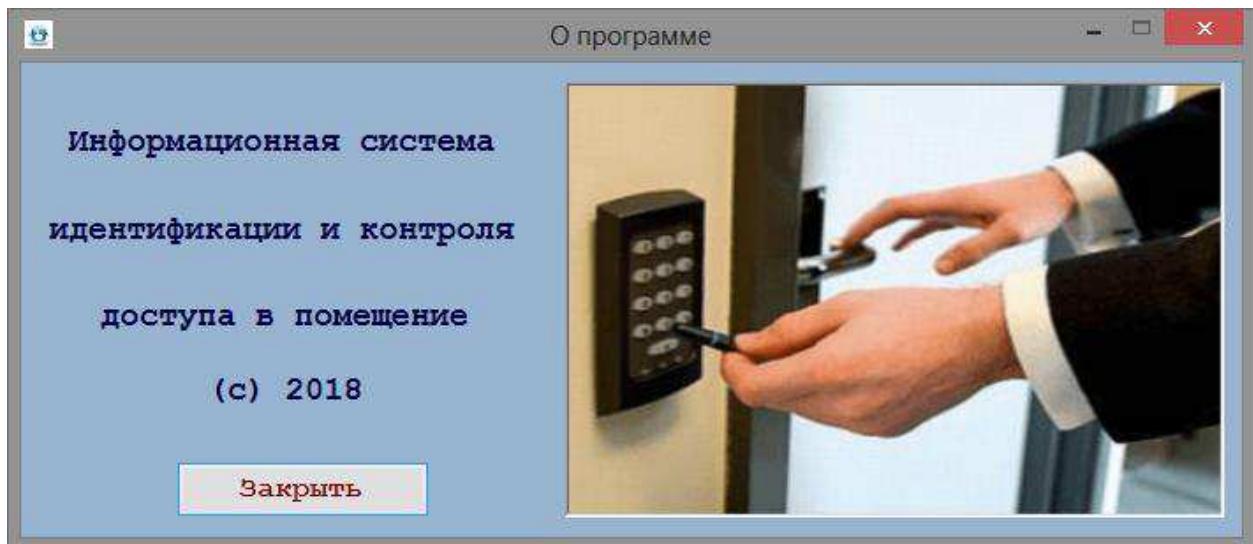


Рисунок 2.19 – Краткая информация о разработанном приложении

## **ЗАКЛЮЧЕНИЕ**

В ходе работы, целью которой является разработка системы идентификации и контроля доступа в помещения предприятия, были решены все поставленные задачи исследования. Выявлено, что под системой контроля и управления доступом (СКУД) в общем случае понимается совокупность организационно-методических и программно-технических средств, позволяющих осуществить решение задачи контроля и управления территорией на объекте и оперативными помещениями, а также оперативного контроля за движением сотрудника и временными интервалами их нахождения на объекте.

Рост актуальности СКУД обусловлен еще и важностью ее наличия для эффективного функционирования предприятия. Осуществление контроля дает возможность не только существенно увеличить уровень безопасности, но и производить оперативное реагирование на поведение посетителей и персонала.

На рынке программного и аппаратного обеспечения представлен достаточно широкий спектр систем биометрической идентификации. Однако, не смотря на разнообразие методик, большинство систем ориентировано на обработку именно отпечатков пальцев, и эти решения составляют больше половины рынка программного обеспечения. Сканеры отпечатков пальцев прошли действительно длинный путь к улучшению. Современные системы оснащены различными датчиками (температуры, силы нажатия и т.п.), которые повышают степень защиты от подделок.

Организация процесса управления доступом предполагает постоянное отслеживание передвижения сотрудников, а также определение прав на доступ в конкретные помещения посредством карты сотрудника или сравнения отпечатка пальца. Соответственно требуется хранение информации о сотрудниках, шаблонов их отпечатков, параметров помещений и др. При этом возникает необходимость получать данные такого рода различным

пользователям в значительной мере удаленным друг от друга, поэтому наиболее эффективной будет использование клиент-серверной архитектуры.

Результатом работы стала полностью работоспособная система идентификации и контроля доступа в помещения предприятия, основой которой стала СУБД MSSQL Server 2012, а клиентская часть разработана на языке C# с использованием интерфейса программирования приложений Windows Form.

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Булатников, Е. В. Сравнение библиотек компьютерного зрения для применения в приложении, использующем технологию распознавания плоских изображений / Е.В. Булатников, А.А. Гоева. // Москва ; Вестник МГУП имени Ивана Федорова. - 2015. - № 6. – С. 85-91.
2. ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств. - Введ. 30.11.2010. – Москва : Стандартинформ, 2011. – 83 с.
3. Жигалов, И. Е. Математические методы и алгоритмы сравнения изображений при автоматической оценке графических данных в телекоммуникационной системе / И. Е. Жигалов, Д. В. Шевченко, М. И. Озерова, А. С. Овдина // Самара ; Известия Самарского научного центра РАН. - 2013. № 4. – С. 356-359.
4. Каторин, В. Ф. Вестник Полиции. Методы и средства биометрической идентификации личности / В. Ф. Каторин // Сочи ; ООО «Научный издательский дом Исследователь». – 2015. № 4. – С. 48-75
5. Котов, О. М. Язык C#. Краткое описание и введение в технологии программирования. Учебное пособие. / О. М. Котов // Екатеринбург ; Изд. «Урал». – 2014. № 4. – С. 208
6. Куперштейн, В. И. Самоучитель Microsoft Project 2013 в управлении проектами. / В. И. Куперштейн // Санкт-Петербург ; Изд. БХВ-Петербург. - 2013. – 432 с.
7. Мерков, А. Б. Распознавание образов. Введение в методы статистического обучения. / А. Б. Мерков. Москва : Едиториал УРСС, 2011. – 256 с.
8. Пытьев, Ю. П., Чуличков, А. И. Методы морфологического анализа изображений. / Ю. П. Пытьев, А. И. Чуличков. Москва : ФИЗМАТЛИТ, 2012. – 336 с.

9. Сонда. Биометрический контроль доступа. [Электронный ресурс] : от доступа на рабочее место до совершения покупок. – Москва, // Сайт. - Режим доступа: <http://www.sonda.ru>

10. СТО 4.2-07-2014 Система менеджмента качества. Общие требования к построению, изложению и оформлению документов учебной и научной деятельности. – Красноярск: БИК СФУ, 2014. – 60с.

11. Хендерсон, К. Microsoft SQL Server: структура и реализация. Профессиональное руководство. / К. Хендерсон. – Москва: Вильямс, 2012. – 1056 с.

12. Baggio D.L. Mastering OpenCV with Practical Computer Vision Projects. / D. L. Baggio, S. Emami, D. M. Escrivá. – Изд.: Packt Publishing, 2012. – 321 с.

13. BioLink. Учет рабочего времени и контроль доступа. [Электронный ресурс] : содержит сведения о видах идентификации личности. – Москва, // Сайт. - Режим доступа: <http://www.biolink.ru>

14. Bayometric. Система контроля доступа и учета рабочего времени. [Электронный ресурс] : учет рабочего времени. – США, // Сайт. - Режим доступа: <http://www.bayometric.com>

15. Laganière R. OpenCV 2 Computer Vision Application Programming Cookbook / R. Laganière – Изд.: Packt Publishing, 2011. – 298 с.

16. MS Visual Studio 2015. [Электронный ресурс] : - Продукты Microsoft. – США, // Сайт. - Режим доступа: <https://www.visualstudio.com/ru>

17. SecuGen Solutions Showcare. [Электронный ресурс] : - Биометрические технологии. – США, // Сайт. - Режим доступа: <http://www.secugen.com/>

18. SQL Server. Microsoft. [Электронный ресурс] : - Базы данных SQL. – США, // Сайт. – Режим доступа: <https://www.microsoft.com/ru-ru/server-cloud/products/sql-server/>

Федеральное государственное автономное  
образовательное учреждение  
высшего образования  
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ КОСМИЧЕСКИХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
Кафедра «Информационных систем»

УТВЕРЖДАЮ  
И. О. Заведующий кафедрой ИС  
 Л.С. Троценко  
«13» июня 2018 г.

### БАКАЛАВРСКАЯ РАБОТА

09.03.02 «Информационные системы и технологии»

Система контроля и управления доступом на предприятии

Руководитель

доцент, к.т.н

С.А. Виденин

Выпускник

А.В. Киселёв

Нормоконтролер

Ю.В. Шмагрис

Красноярск 2018