Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт Космических и Информационных Технологий

Информационные Системы

УТВЕРЖДАЮ
Заведующий кафедрой ИС
_____ С.А. Виденин
подпись инициалы, фамилия
«____» _____ 2017 г.

БАКАЛАВРСКАЯ РАБОТА

09.03.02 Информационные системы и технологии

Организация системы защиты персональных данных

Руководитель	_____	ст.преподаватель	Ю.В.Шмагрис
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		Л.В.Терскова
	подпись, дата		инициалы, фамилия
Консультант	_____	к.т.н., доцент	И.А.Легалов
	подпись, дата	должность, ученая степень	инициалы, фамилия
Нормоконтролер	_____		Ю.В. Шмагрис
	подпись, дата		инициалы, фамилия

Красноярск 2017

Федеральное государственное автономное образовательное учреждение высшего образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

«Институт космических и информационных технологий» Кафедра «Информационные системы»

УТВЕРЖДАЮ

Заведующий кафедрой ИС

_____ С. А. Виденин

подпись инициалы, фамилия

«____» _____ 2017 г.

ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

в форме бакалаврской работы

Студенту: Терсковой Людмиле Валерьевне

Группа: ВКИ 12-13Б Направление 09.03.02 «Информационные системы и технологии»

Тема выпускной квалификационной работы: «Организация системы защиты персональных данных»»

Утверждена приказом по университету № 2836/с от 06.03.2017 г.

Руководитель ВКР: Ю.В.Шмагрис- старший преподаватель кафедры «Информационные системы и технологии» ИКИТ СФУ, консультант И.А.Легалов – к.т.н., доцент кафедры «Информационные системы»

Исходные данные для ВКР: Список требований к разрабатываемому приложению, методические указания научного руководителя.

Перечень разделов ВКР: Введение, порядок организации системы защиты персональных данных, база данных, криптографический модуль, реализация программного комплекса, список использованных источников.

Перечень графического или иллюстрированного материала с указанием основных чертежей, плакатов, слайдов: Презентация, выполненная в Microsoft Office PowerPoint 2010.

Руководитель ВКР _____ Ю.В.Шмагрис

(подпись)

Консультант _____ И.А.Легалов

(подпись)

Задание принял к исполнению _____ Л.В.Терскова

(подпись)

« ___ » _____ 2017г.

РЕФЕРАТ

Выпускная квалификационная работа по теме «Организация системы защиты персональных данных» содержит 52 страницы текстового документа, 14 использованных источников, 18 рисунков, 1 приложение.

ИНФОРМАЦИОННАЯ СИСТЕМА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, СУБЪЕКТ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИНФОРМАЦИЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, РАСПРЕДЕЛЕННАЯ СЕТЬ, ТЕХНИЧЕСКОЕ ЗАДАНИЕ, ПРОГРАММНЫЙ КОМПЛЕКС, КРИПТОГРАФИЯ, АЛГОРИТМ, КЛИЕНТ, СЕРВЕР.

Цель выпускной квалификационной работы – организовать защиту информационной системы персональных данных на предприятии.

В результате выполнения данной работы была изучена нормативно – правовая база, составлено и реализовано техническое задание по обеспечению мер безопасности персональных данных, реализован программный комплекс для защиты персональных данных внутри организации.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационная безопасность на предприятии – неотъемлемая часть его бизнес-процессов. Без обеспечения конфиденциальности, целостности и доступности информации, предприятие рискует потерять репутацию, денежные средства, либо вовсе стать не конкурентоспособным, при потере стратегически важной информации, нужной для дальнейшего развития предприятия. Возможна также уголовная и административная ответственность за потерю некоторых видов информации. Самым распространенным видом информации, которая нуждается в обеспечении безопасности, являются персональные данные (далее ПДн). Защита персональных данных является актуальной темой в нашей стране, так как законодательная база существует относительно не долгое время. В связи с этим, лица, которые отвечают за безопасность ПДн при их обработке, зачастую не знают правил организации защиты информационной системы персональных данных (далее ИСПДн).

Цель выпускной квалификационной работы – организовать защиту информационной системы персональных данных на предприятии.

Для достижения цели сформулированы следующие задачи:

1. изучение нормативно – правовой базы;
2. исследование ИСПДн предприятия;
3. определение уровня защищенности (далее УЗ) Пдн в соответствии с ПП-1119;
4. определение мер для защиты Пдн в соответствии с УЗ и приказом ФСТЭК №21;
5. В соответствии с видом вычислительной сети предприятия и базовой моделью угроз ФСТЭК, определить частную модель угроз, исходя из нее, составить список конкретных технических средств защиты;
6. Реализация системы защиты персональных данных внутри предприятия.

Глава 1 Порядок организации системы защиты персональных данных

1 Нормативно — правовая база

1.1 Федеральный закон №152-ФЗ «О персональных данных»

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления, муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации 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.

Данный Федеральный закон направлен на обеспечение защиты прав и свобод человека в случае обработки его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Так же описывает основные принципы, которых необходимо придерживаться при обработке персональных данных, категории персональных данных, основные определения, которые встречаются при работе с ПДн.

1.1.4 Меры по обеспечению безопасности ПДн при их обработке

Оператор при обработке персональных данных обязан 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.

Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Контроль и надзор за выполнением требований, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

1.2 Постановление правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в ИСПДн»

Федеральный закон №152-ФЗ «О персональных данных» говорит о том, что нужно защищать персональные данные, каким образом они могут применяться и в общем, регулирует отношение в области работы с ПДн. Однако каким именно образом их необходимо защитить, какие организационные и технические меры при этом нужно применять, в данном федеральном законе не объясняется.

Постановление правительства №1119 позволяет определить уровень защищенности ПДн и общие требования по их защите.

1.2.1 Типы актуальных угроз

Для определения уровня защищенности ПДн необходимо знать тип актуальных угроз в ИСПДн.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом, которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных

(недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

1.2.2 Уровни защищенности

1.2.3 Требования для обеспечения уровней защищенности

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных 4-ым уровнем защищенности, необходимо, чтобы было

назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, описанных для 3-го уровня защищенности, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных обязанностей.

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах необходимо учитывать все предыдущие требования и, в дополнении, следующие пункты:

а) автоматическая регистрация в электронном журнале безопасности изменений полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

1.3 Приказ ФСТЭК России № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013г

В соответствии с данным приказом и установленным ранее уровнем защищенности, определяется список конкретных технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Данный документ включает в себя следующие меры: идентификация и аутентификация, управление доступом, меры по ограничению программной среды, защита машинных носителей информации, регистрация событий, антивирусная защита, обнаружение/предотвращение вторжений, анализ защищенности ПДн, обеспечение целостности, обеспечение доступности, защита среды виртуализации, защита технических средств, защита информационной системы, выявление инцидентов, управление конфигурацией.

2 Исследование ИСПДн

Цель данного раздела работы – определить информацию, необходимую для составления акта об определении уровня защищенности и создания частной модели угроз**.** В качестве исследуемой была взята ИСПДн местного интернет провайдера. Организация занимается предоставлением телематических услуг физическим и юридическим лицам, что влечет за собой работу с большими объемами конфиденциальной информации, в том числе и персональные данные.

В ИСПДн используются персональные данные сотрудников и клиентов компании. Подавляющее большинство записей – данные клиентов в объеме более 100000 шт.

Схема корпоративной сети организации представлена на рисунке 1.

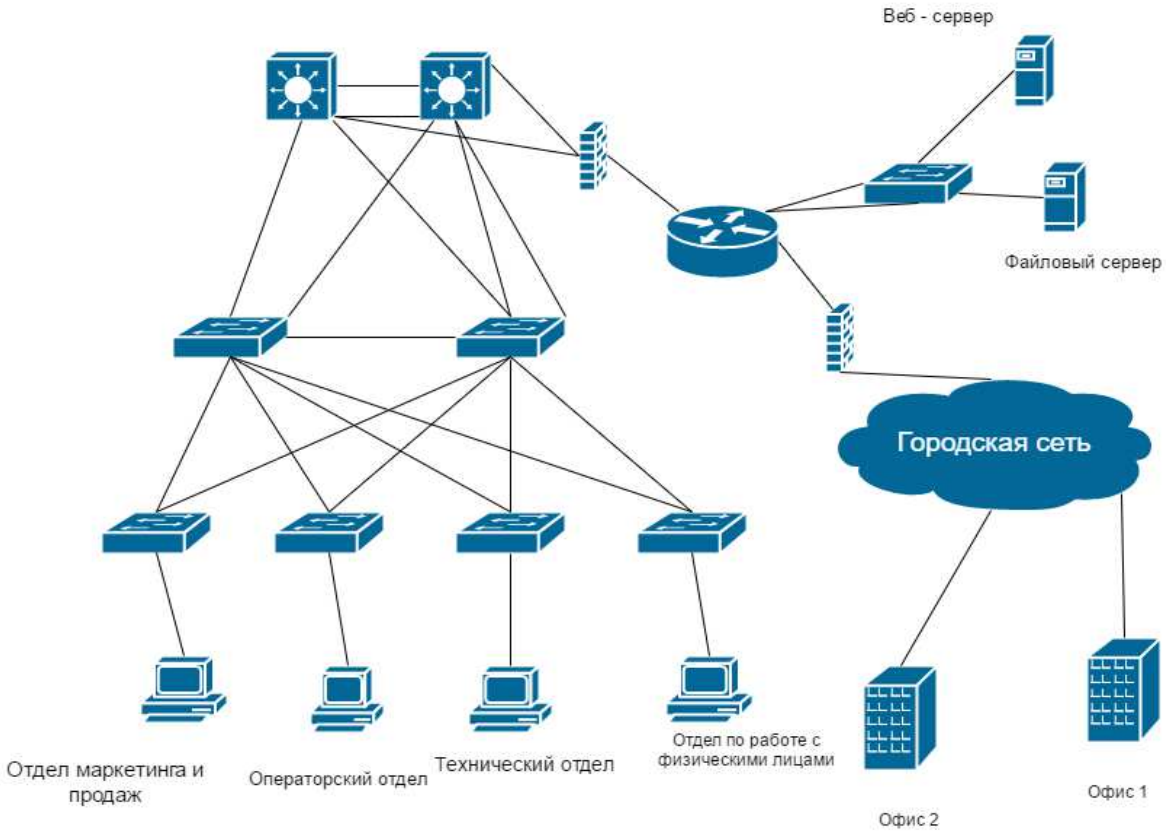


Рисунок 1 — Схема корпоративной сети организации

Исходя из схемы, представленной на рисунке 1, имеет место распределенная ИСПДн, имеющая подключение к сетям связи общего пользования, общедоступный файловый и ИСПДн сервера, отсутствует защита данных при передачи информации от Web-интерфейса до ИСПДн сервера. Было определено, что для данной ИСПДн актуальны угрозы 2-го типа. Обрабатываются специальные, общедоступные категории персональных данных, их количество более 100000 субъектов, по принадлежности данные субъекты не являются сотрудниками оператора.

Цель данного раздела достигнута, собрана вся необходимая информация для определения уровня защищенности и модели угроз.

3 Определение уровня защищенности

Для определения уровня защищенности на предприятии необходимо составить такой документ как: «Акт определения уровня защищенности персональных данных при их обработке в ИСПДн», который далее направляется в отделение Роскомнадзора. Для составления данного документа определяется состав комиссии, в который входят председатель комиссии и несколько ее членов. В акте указывается, на основании какого документа определяется какой уровень защищенности необходимо обеспечить. Делается это на основании ПП №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». После исследования ИСПДн организации, была составлена комиссия в лице главного инженера, ведущего системного администратора, коммерческого директора и главного бухгалтера, председателем комиссии был назначен генеральный директор. Документ, получившийся в результате проделанной работы, представлен в Приложении А.

4 Определение мер для защиты ИСПДн

После получения ответа от Роскомнадзора на высланный акт «Об определении уровня защищенности», прибыла комиссия, которая проверила соответствие информации указанной в акте и информации, которая соответствует действительной ситуации на предприятии. Если никаких нареканий не возникает, то для ИСПДн устанавливается требуемый уровень защищенности, в данном случае никаких претензий от лица Роскомнадзора не возникло и ИСПДн был присвоен первый уровень защищенности.

В соответствии с установленным уровнем защищенности необходимо определить комплекс мер по обеспечению безопасности ПДн. Данный комплекс определяется исходя из приказа ФСТЭК №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013.

Для первого уровня защищенности, который был определен ранее, список мер можно найти в приложении А данной работы.

Данный комплекс мер обеспечивается по средствам внедрения в систему соответствующих сертифицированных технических средств и совокупности организационно – административных мер по обеспечению информационной безопасности. Так же, для защиты персональных данных сотрудников и клиентов компании внутри сети корпоративной сети организации, будет разработан программный комплекс, который позволит передавать персональные данные в зашифрованном виде. Цель данного раздела достигнута, то есть был определен список мер по обеспечению безопасности ПДн в соответствии с Приказом ФСТЭК №21 и установленным уровнем защищенности.

5 Определение частной модели угроз информационной безопасности

Основываясь на базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных и информации, полученной на этапе исследования ИСПДн, определяем базовый набор угроз. С помощью него составляется частная модель угроз. В ходе исследования ИСПДн было выяснено, что имеет место распределенная сеть, имеющая подключение к сетям общего пользования, следовательно, на основания базовой модели угроз ФСТЭК для ПДн при их обработке в ИСПДн, определен следующий базовый набор угроз:

1) угрозы утечки информации по техническим каналам связи;

2) угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте;

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн.

Угрозы НСД нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место в распределенных ИСПДн, не имеющей подключения к сетям общего пользования. Кроме того, в такой ИСПДн имеют место угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

1) угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации;

2) угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций

ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

3) угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

4) угрозы подмены доверенного объекта;

5) угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;

6) угрозы выявления паролей;

7) угрозы типа «Отказ в обслуживании»;

8) угрозы удаленного запуска приложений;

9) угрозы внедрения по сети вредоносных программ.

В дополнении к уже имеющимся угрозам, исходя из специфики ИСПДн, существует угроза потери ПДн через Веб – интерфейс, через операторский отдел при совершении входящих/исходящих звонков.

6 Состав системы защиты ПДн

Исходя из раздела 4 данной работы, система защиты персональных данных должна состоять из:

1) подсистема управления доступом;

2) подсистема регистрации и учета;

3) подсистема контроля целостности;

4) подсистема криптографической защиты;

5) подсистема межсетевого экранирования;

6) подсистема защиты от утечек;

7) подсистема обнаружения атак;

8) подсистема анализа защищённости;

9) подсистема антивирусной защиты;

10) подсистема централизованного управления.

6.1 Выполнение технического задания по заданным требованиям

Данные требования достигаются при помощи сертифицированных технических средств защиты. Для обеспечения информационной безопасности предприятия было принято решения закупить следующие продукты:

система защиты информации от несанкционированного доступа (далее СЗИ от НСД) – SecretNet (сетевой вариант) цена около 46 тыс. руб. за базовую комплектацию без расходных материалов;

средства антивирусной защиты (далее САВЗ) (в том числе и хранилищ данных): Касперский типа Б и В или Г;.

для передачи данных в сторонние организации систему «КриптоПро», внутри распределенной сети решение для виртуальных частных сетей (VPN) на основе унифицированного шлюза безопасности (UTM) – системы CheckPointUTM-1, цена около 220 тыс. руб. умножить на количество сегментов распределенной сети;

сервер централизованного администрирования с ОС WindowsServerSEc использованием ActiveDirectory;

система обнаружения/предотвращения вторжений (IDS/IPS) на базе CheckPointUTM-1 – системы;

система предотвращения утечек (DLP) на базе CheckPointUTM-1 – системы.

Для снижения риска утечки информации из корпоративной сети в интернет необходимо ограничить доступ к внешним ресурсам (или их части) отделам, которые в них не нуждаются. Этого можно добиться применением фаерволов нового поколения (NGFW) или более дешевого унифицированного шлюза безопасности. Применение одного такого устройства на сегмент распределенной сети заместит потребность в отдельных IPS/IDS - системах Сетевых антивирусах, Песочницах, DLP – системах. Т.е. данное устройство заменяет целый эшелон защиты.

Применение данных технических средств не повлечет каких-либо проблем, связанных с законодательством РФ, так как имеют сертификаты ФСТЭК России для работы с информацией характеризующейся как персональные данные, по 1 уровню защищенности. Изменение схемы сети предприятия, с учетом рекомендаций, представлено на рисунке 2.

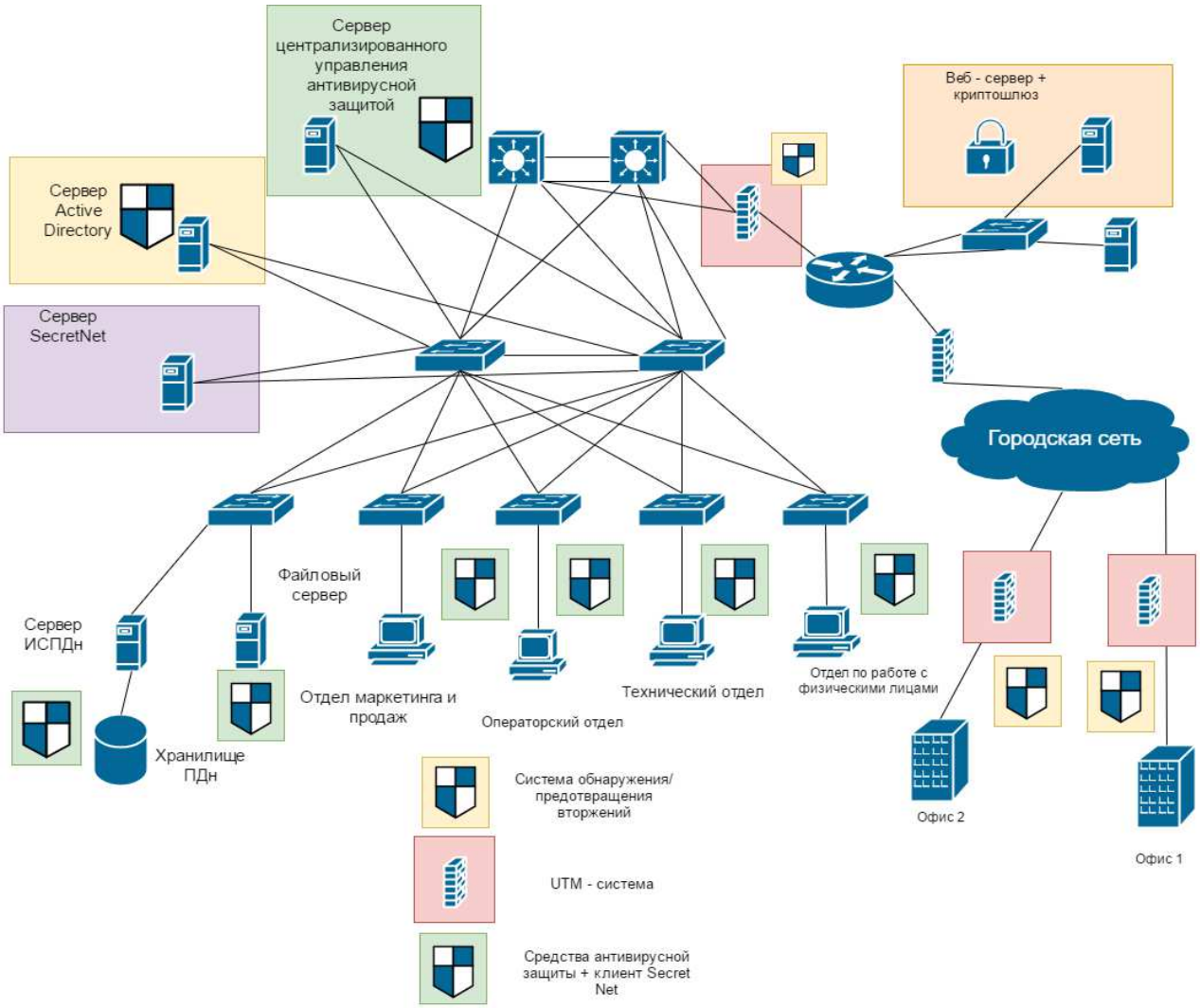


Рисунок 2 – Схема сети организации с учетом изменений

После проведения работ по обновлению СПД организации, была решена проблема утечки информации в сети общего доступа изнутри сети, несанкционированный доступ к ИСПДн из внешней сети. Организованное и централизованное управление САВЗ позволит защитить рабочие места, СХД от внедрения вредоносных объектов. Криптошлюз в сочетании с веб-сервером снизит до минимума вероятность утечки информации через веб-интерфейс. Ввод доменной системы с помощью сервера ActiveDirectory позволит ограничить доступ к сети несанкционированных пользователей, а разрешенным к доступу в сеть пользователям, выдать определенные права на доступ к функциям операционной системы. Ограничение прав позволит избежать лишних проблем с целостностью рабочих мест, установкой лишнего программного обеспечения на АРМ. Для обеспечения безопасности передачи данных в сторонние организации и другие офисы компании используется VPN соединение, которое организовано на базе «КриптоПро», вся эта система включена в унифицированный шлюз безопасности (UTM) – системы CheckPointUTM-1.

Для дополнительного обеспечения безопасности персональных данных необходим программный, комплекс, который будет предоставлять к ним доступ, учитывая специфику должности работника, который к такому типу данных допускается. Для этого решено разработать клиент – серверное приложение, которое будет взаимодействовать с базой данных.

Глава 2 РЕАЛИЗАЦИЯ ПРОГРАММНОГО КОМПЛЕКСА

1 Разработка структурной схемы программного комплекса

Программный комплекс состоит из следующих составляющих:

1. клиентская часть;
2. криптомодуль;
3. сервер в паре с базой данных.

Структурная схема представлена на рисунке 3.

Рисунок 3 – Структурная схема программного комплекса

2 Выбор языка программирования

2.1 Выбор языка программирования для разработки программного комплекса.

На первичном этапе разработки приложения встал вопрос, какой из известных языков программирования использовать, C++ , C# или Qt?

Для того чтобы ответить на возникший вопрос, необходимо сравнить их по следующим параметрам:

1. скорость разработки;
2. кроссплатформенность;
3. производительность кода и требовательность к ресурсам;
4. библиотеки;
5. удобство отладки;
6. язык и синтаксис;
7. стоимость поддержки;
8. самодостаточность приложений;
9. удобство сборки;
10. перспективы;
11. вывод.

2.2 Скорость разработки

Скорость разработки на C# и Qt на начальных этапах гораздо быстрее за счет готовых заранее конструкций и шаблонов, по сравнению с C++. Однако, когда каркас проекта создан, основные подходы и библиотеки выбраны, скорость разработки на C++ и скорость разработки на C#, Qt становятся практически одинаковыми.

Таким образом, в коротких малобюджетных проектах C# и Qt будет иметь преимущество по скорости разработки, но в длинных и относительно дорогих данное преимущество будет незначительным.

2.3 Кроссплатформенность

Сегодня практически невозможно предоставить себе приложение, не обладающее интерфейсом пользователя. Понятия Software и GUI неразрывно связаны друг с другом.

Хотя WindowsAPI обладает всем необходимым для создания графического интерфейса пользователя, использование доступных инструментов требуется больших затрат времени и практического опыта. Даже библиотеки, призванные облегчить процесс написания программ для ОС Windows, такие как, например, MFC, не дают процессу создания программ той простоты и легкости, какой хотелось бы. Поэтому и сегодня разработчики по-прежнему тратят массу времени на реализацию интерфейса пользователя. Но самый большой недостаток, связанный с применением таких библиотек – это кроссплатформенность.

Если создавать программное обеспечение только для ОС Windows, то достаточно будет платформы C#, но платформонезависимая реализация приложений – это будущее программной индустрии. С каждым днем она будет приобретать все более возрастающее значение.

2.4 Производительность кода и требовательность к ресурсам

Очевидным является факт того, что возможности по оптимизации неуправляемого кода куда шире, чем возможности по оптимизации управляемого кода. Таким образом, пиковая производительность кода достижима только в неуправляемом исполнении, т.е. в пределе, почти любая задача на C++/Qt может быть решена с меньшими требованиями к ресурсам. Поэтому в тяжелых задачах, связанных с обработкой большого количества данных, C++/Qt имеет сильные преимущества перед C#.

Но стоит понимать, что при выборе неправильного подхода, на C++/Qt вполне можно написать код, который будет работать медленнее кода на C#, выполняющего туже задачу.

Если говорить о совокупности субъективных «простоты разработки», «красоты кода» и объективной производительности, то используя C# проще написать код, удовлетворяющий этим критериям одновременно. Однако это не значит, что производительный код на C++/Qt обязательно будет страшным или сложным для восприятия, просто при его написании потребуется более своеобразный подход для удовлетворения перечисленных критериев одновременно.

Фундаментальные основы преимуществ C++/Qt в возможности писать код, который будет выполняться непосредственно процессором, и возможности прямой работы с памятью. Конечно, свобода дает больше возможностей создать себе проблемы, но в ряде случаев это лучше, чем невозможность преодоления потолка производительности. И этот потолок вполне может привести, например, к тому, что под решение задачи, для которого бы хватило одного хорошего сервера, вам придется собирать ферму из нескольких серверов, или же к тому, что ваше приложение будет требовать мощной аппаратной части на задачи, для которых хватило бы составляющих выпущенных 7-10 лет назад.

2.5 Библиотеки

Отличие ассортимента C++/Qt и C# библиотек в том, что C++/Qt библиотек больше, они имеют большую историю, за которую стали неплохо отлажены и оптимизированы, часто кроссплатформенные, многие с открытым кодом. Однако при всех положительных сторонах C++/Qt библиотеки как имеют очень разную, часто даже архаичную архитектуру, часто не объектный, а структурно-процедурный интерфейс. Связано это с тем, что многое в C++/Qt - это C библиотеки.

Другая неприятная особенность C++/Qt библиотек — это создание и переопределение своих базовых типов. Многие C++/Qt библиотеки заводят свои типы строк, контейнеров, переопределяют некоторые базовые типы. Этому есть логичные объяснения (лучшая производительность, поддержка кроссплатформенности, отсутствие подходящих типов на момент написание библиотеки), однако все это не добавляет удобства использования и красоты коду. Базовые же C++ библиотеки дают не так много, как дают стандартные библиотеки C#, поэтому подбор правильных библиотек для проекта C++ - это задача, необходимая даже в сравнительно простых проектах, однако, Qt в данном плане гораздо проще.

В C# перечисленных выше проблем значительно меньше. Огромное количество библиотек с .net идет в базе, плюс к ним множество свободно доступных библиотек, это покрывает практически все первостепенные задачи разработки под Windows. Наличие большого количества стандартных типов почти избавляет от библиотек, где базовые типы переопределены. И в силу того, что библиотеки C# сравнительно молодые, интерфейсы библиотек, как правило, лучше вписываются в те или иные шаблоны проектирования, что часто упрощает их изучение.

Однако же, при ближайшем рассмотрении велик шанс, что под вашу специфическую задачу C# библиотеки не окажется, более того, может

оказаться, что и решать такую задачу на C# достаточно не эффективно, поэтому подобной библиотеки не появится и в будущем, а если и появится, то будет работать недостаточно быстро. Так же для Qt, маловероятно не найти нужную библиотеку.

Вторая неприятная особенность библиотек C# в том, что многие из них являются просто оберткой над неуправляемыми библиотеками, что будет всегда приводить к потерям производительности на конверсиях типов, и создавать дополнительные проблемы отладки и распространения.

2.6 Удобство отладки

Под WindowsC# в большей степени удобней отлаживать, в отличие от C++. Однако если по какой-то причине на ряду с управляемым кодом из C# сборки используется неуправляемый, то его отладка станет более сложная по сравнению с обычной отладкой неуправляемого кода из C++.

В C#, как и в других появившихся до .NET языках, главная методика по отладке состоит в добавлении точек останова и изучении того, что происходит в коде в конкретные моменты во время его выполнения.

В отличии от других сравниваемых языков программирования, в Qt используется специализированная библиотека для отладки – QDebug, так же есть возможность использования точки останова.

2.7 Язык и синтаксис

В общем, синтаксис сравниваемых языков достаточно схож, особых аргументов, которые помогли бы сделать выбор в ту или иную сторону нет. В Qt и C# упор идет больше на работу с классами, в отличие от C++, тут выбор предоставляется разработчику в большей степени.

2.8 Стоимость поддержки

В поддержке приложений большой разницы между C++ и C# нет. Хотя стоит понимать, что некоторые баги в приложениях, написанных на C#, средствами .net, исправить невозможно и при необходимости их исправить стоимость поддержки может существенно возрасти. Однако, если говорить о переструктурировании, то зачастую приложения, написанные на C#, реструктурировать несколько дешевле. С фреймворком Qt, особых сложностей в поддержке не возникает, так как все библиотеки для всех платформ одинаковы.

2.9 Самодостаточность приложений

Полной самодостаточности приложений нет ни у C++ ни у C#. Для C++ так или иначе нужен runtime, а для C# .netframework.

Однако хотелось бы отметить, что runtime C++, как и любая другая библиотека, может быть статически линкована в исполняемый модуль, таким образом исполняемый модуль может содержать все необходимое для работы, и за счет чего станет самодостаточным, в случае C# такое, стандартными средствами не реализуемо. Для Qt так же необходимо использование библиотек qt, но не обязательно устанавливать весь их пакет, достаточно использование тех, которые использовались при разработке.

2.10 Удобство сборки

Сборка C++ проектов заметно сложнее сборки проектов C#. Однако стоит понимать, что большая сложность предоставляет и дополнительную гибкость, которая рано или поздно может стать полезной вам. Однако до этого момента будет лишь увеличивать расходы вашего времени.

Создание дистрибутива приложения Qt с учётом всех его файлов, которые должны устанавливаться на компьютерах пользователей, вероятно, является самым сложным этапом развёртывания. Требуется тщательно проанализировать исполняемый файл программы на наличие зависимостей, позаботиться о файлах переводов, не забыть про ресурсы приложения. Решить часть этих проблем поможет утилита windeployqt.exe, которая поставляется вместе с комплектом сборки. Данный инструмент работает в командной строке и поддерживает некоторые параметры конфигурации. Последним параметром обязательно должен быть указан путь к двоичным файлам собранного приложения или имена этих файлов. После запуска утилиты возле исполняемого файла программы должны появиться различные библиотеки и служебные файлы, которые позволят приложению корректно запускаться и работать на многих компьютерах.

2.11 Вывод

Для разработки данного программного комплекса важным фактором является простота и скорость сборки, с использованием минимальных затрат по времени и ресурсам, использование минимального количества библиотек, для того, чтобы не загружать систему.

В случае возникновения нужды переноса приложения на другую платформу, отличающуюся от Windows, необходимо, чтобы приложение было как можно более независимым от операционной системы. Язык программирования C# в данном случае не может этого обеспечить из-за нужды в .Net. Однако, C++ и фреймворк Qt являются достаточно гибкими и подойдут для кроссплатформенных приложений. Одним из решающих факторов в данном случае стала скорость разработки и отладки приложений. Ферймворк Qt оказался более удобным для разработки приложений с GUI, в отличие от C++. Для создания приложений с диалоговыми окнами стандартными средствами C++ слишком проблемно и затратно по времени, будь что изучение библиотеки MFC или WindowsAPI.

Так как будет разрабатываться клиент-серверное приложение, которое осуществляет взаимодействие с базой данных на MSSQL, необходимо рассмотреть возможности C++ и фрейморка Qt в этом плане. Базовый набор библиотек на Qt, которые учитывают работу с базами данных любых типов, гораздо шире, чем в стандартном наборе C++, что позволит сэкономить время на разработку приложения.

Учитывая все вышесказанное, был остановлен выбор на фреймворке Qt.

3 База данных

Для хранения персональных данных и иной информации, относящейся к специфике работы компании, используется база данных на платформе MSSQL.

База данных содержит следующие таблицы:

1. сотрудники;
2. абоненты;
3. авторизация;
4. тарифные планы;
5. учетная запись;
6. изменения пользователей.

Таблица «Сотрудники» хранит в себе записи о сотрудниках организации, они является персональными данными, которые так же необходимо защищать от лиц, не имеющим к ним доступ.

Таблица «Абоненты» хранит в себе информацию об абонентах, включая все паспортные данные, адрес проживания, вплоть до номера подъезда и квартиры, ИНН, КПП, номер телефона. Основной упор в данной работе делается на защиту именно этих данных.

Таблица «Авторизация» хранит в себе записи о пользователях, которые имеют право получать доступ к базе данных через клиентскую часть приложения. Так же в данной таблице хранятся правила авторизации, то есть определяется, какому пользователю выдать какие права на этапе авторизации, что позволит ограничить доступ к персональным данным.

Таблица «Тарифные планы» хранит в себе записи о размерах абонентской платы за каждый из тарифных планов, скорости, которая предоставляется в соответствии с ними и идентификационный номер, по которому идет присвоение каждому абоненту выбранного тарифного плана.

Таблица «Учетная запись» хранит в себе информацию по каждому лицевому счета абонента: Лицевой счет, Тарифный план, Баланс лицевого счета, IP – адрес свитча и номер порта, к которым подключен абонент.

Таблица «Изменения пользователей» содержит записи обо всех изменениях в учетных записях абонентов. Данное логирование необходимо, чтобы в случае, какой-либо спорной ситуации с абонентом, можно было найти лицо, которое совершило то или иное действие.

4 Криптографический модуль

В нынешних реалиях, при работе организации в сфере информационных систем, всегда есть вероятность утечки информации, что может отрицательно сказаться на финансовом положении организации и его авторитете.

Для того, чтобы минимизировать потери и обезопасить организацию от финансовых потерь, данные, которые передаются по сетям передачи данных, необходимо шифровать.

В данном программном комплексе решено организовать шифрование данных на основании алгоритма Эль-Гамаля.

Первым этапом, в реализации шифрования по Эль-Гамалю является генерация открытого и закрытого ключа.

Алгоритм генерации ключей можно представить в следующем виде:

1. генерация простого числа ***p;***
2. выбор целого числа ***g***, которое является первообразным корнем числа p;
3. выбор случайного числа ***x,*** такого, что 1 <***x<p*** – закрытый ключ;
4. вычислить число ***y = g^xmodp***;
5. определить закрытый ключ, как тройку ***(p,g,y).***

Шифрования данных представляется в соответствии со следующими этапами:

1. выбирается случайный целый сессионный ключ ***k***такой, что 1< ***k*< *p-1***;

2. вычисляется числа ***a = g^kmodp***и ***b=y^k*Mmodp;***

3. пара чисел ***(a,b) – шифротекст.***

В данном алгоритме M – участок исходного текста, который должен быть меньше простого числа ***p***.

Дешифрование заключается в вычислении числа:

M = b*a^(p-1-x) modp;

Общая схема алгоритма:

1. исходный текст передается в криптомодуль;
2. генерация ключей и передача открытого ключа;
3. шифрование;
4. передача шифротекста получателю;
5. дешифрация;
6. передача дешифрованного текста получателю.

Для того, чтобы увеличить криптостойкость алгоритма, необходимо ввести для его реализации операции, основанные на длинной арифметике.

Известно, что компьютер может оперировать числами, количество бит которых ограниченно. Как правило, мы привыкли работать с 32-х и 64-х разрядными целыми числами, которым на платформе .NET соответствуют типы Int32 (int) и Int64 (long) соответственно.

А что делать, если надо представить число, такое как, например, 884176199373970195454361600000? Такое число не поместится ни в 64-х разрядный, ни тем более 32-х разрядный тип данных. Именно для работы с такими большими числами существует длинная арифметика.

Длинная арифметика — в вычислительной технике операции (сложение, умножение, вычитание, деление, возведение в степень и т.д.) над числами, разрядность которых превышает длину машинного слова данной

вычислительной машины. Эти операции реализуются не аппаратно, а программно, используя базовые аппаратные средства работы с числами меньших порядков.

В данной работе класс длинной арифметики имеет название BigInteger. В нем реализованы следующие операции для работы с длинной арифметикой: сложение, вычитание, инкремент, декремент, умножение, деление, деление на число, которое не является длинным, модуль, возведение в степень по модулю.

Так же реализованы операции сравнения, а так же битовые операции сдвига влево, вправо.

Для реализации криптографических алгоритмов вышеперечисленных операций не достаточно. В каждом алгоритме используются случайные числа, для их генерации так же реализована функция genRandomBits, которая возвращает случайную последовательность бит фиксированной длинны.

Так как иногда появляется нужда вывести результат куда-либо, реализована функция преобразования числа BigInteger в строковое значение String или шестнадцатеричное значение HexString.

5 Реализация программного комплекса

5.1 Клиентская часть

В соответствии со структурной схемой, разработанной на первоначальном этапе, необходимо реализовать клиентскую часть, криптомодуль, серверная часть.

Клиентская часть программного комплекса предоставляет интерфейс взаимодействия пользователя с базой данных. В зависимости от прав, выданных на этапе авторизации.

При первоначальном запуске программы перед пользователем представляется окно авторизации, которое представлено на рисунке 4.

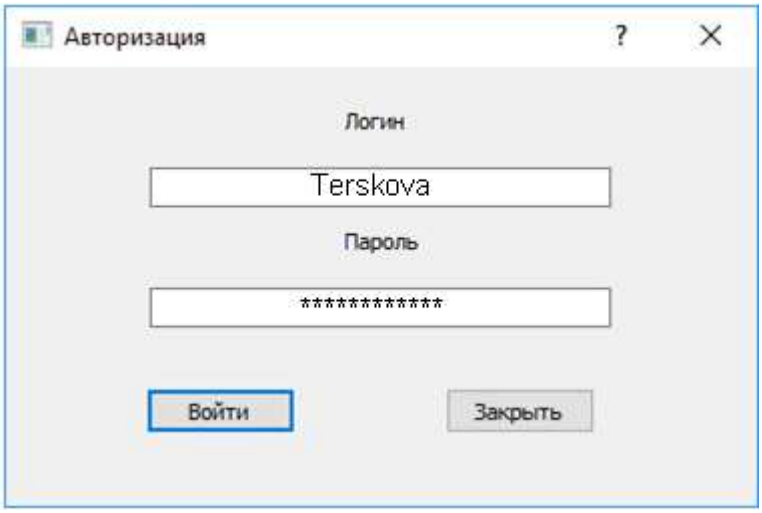


Рисунок 4 – Окно авторизации

В случае прохождение аутентификации, то есть верно, введённых логина и пароля, перед пользователем появляется окно, представленное на рисунке 5.

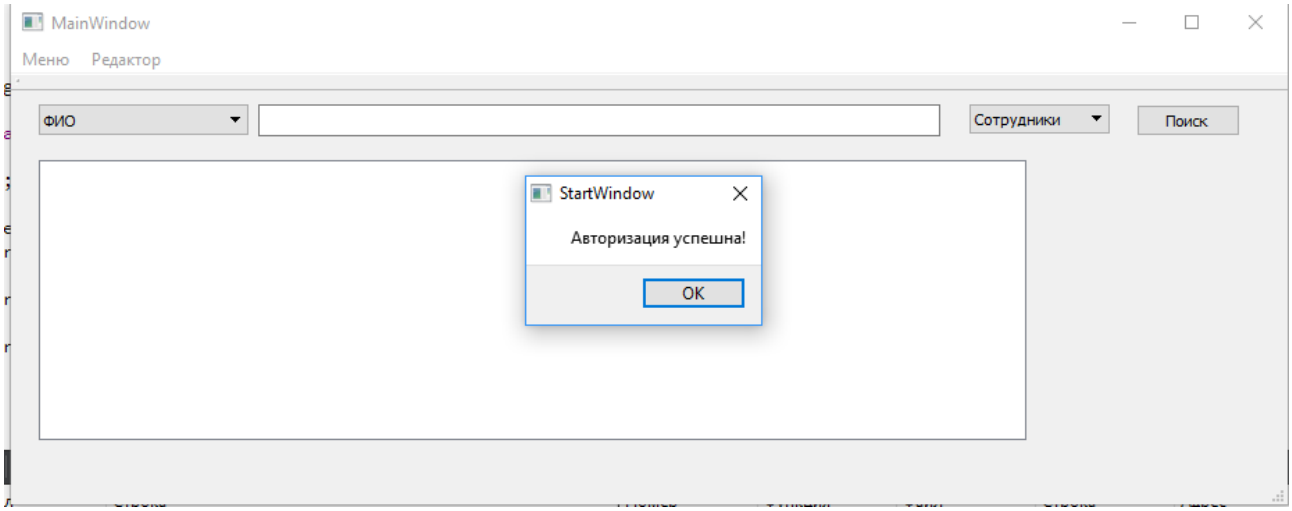


Рисунок 5 – Окно пройденной аутентификации

Если же аутентификация не была пройдена, то пользователю будет выдана ошибка, представленная на рисунке 6. После нажатия кнопки «ОК» представится возможность повторить попытку ввода логина и пароля.

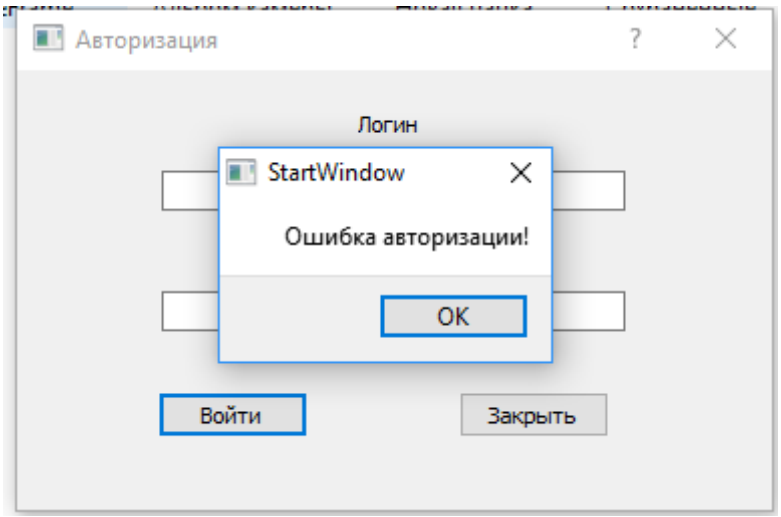


Рисунок 6 – Окно ошибки авторизации

Так же есть вероятность того, что сервер, к которому подключается клиент, может быть не доступен в момент авторизации по той или иной

причине. В программе предусмотрен и этот случай, в случае недоступности сервера, пользователю представится окно ошибки соединения с базой данных, которое изображено на рисунке 7.

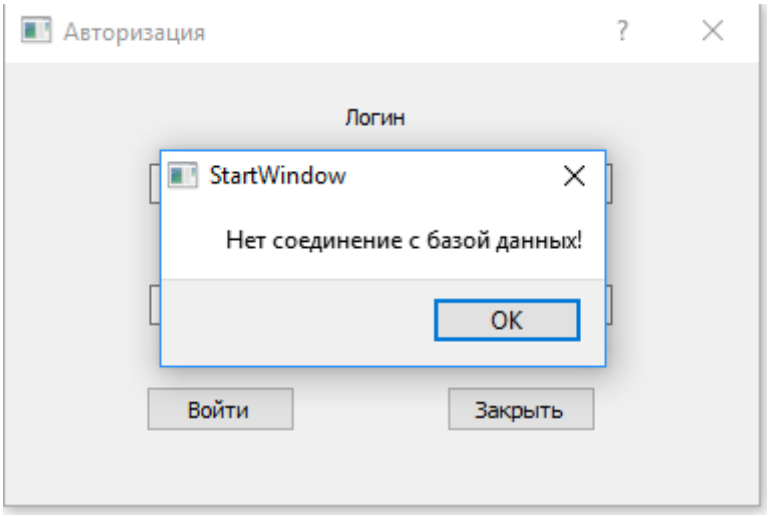


Рисунок 7 – Ошибка соединения с сервером

После прохождения авторизации пользователю открывается основное окно программы, в котором есть возможность делать различные запросы к базе данных. Рисунок 8 отображает данное окно.

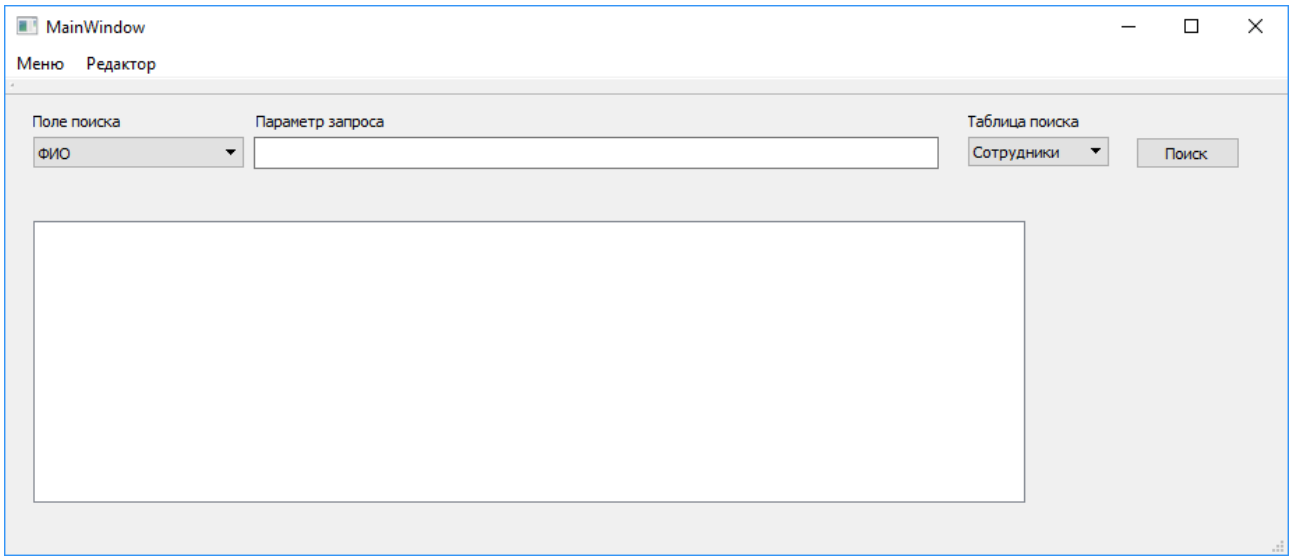


Рисунок 8 – Главное окно программы

Главное окно программы дают пользователю основной интерфейс для взаимодействия с сервером, который в свою очередь работает в паре с базой данных. В данном окне содержатся два ComboBox: поле поиска, таблица поиска. Поле поиска определяет столбец, в соответствии с которым будет производиться выборка. Таблица поиска позволяет программе выбрать таблицу из базы данных, к которой будет осуществляться запрос. Параметр запроса – условие, которое определяет результат исходного запроса. Кнопки «Меню» и «Редактор» позволяют пользователю использовать системное меню. Редактор содержит два подменю для выполнения добавления сотрудников и клиентов в базу данных.

После выбора пункта меню «Редактор», далее «Добавить сотрудника», появляется диалоговое окно, предлагающее ввести информацию, которая указана на рисунке 9.

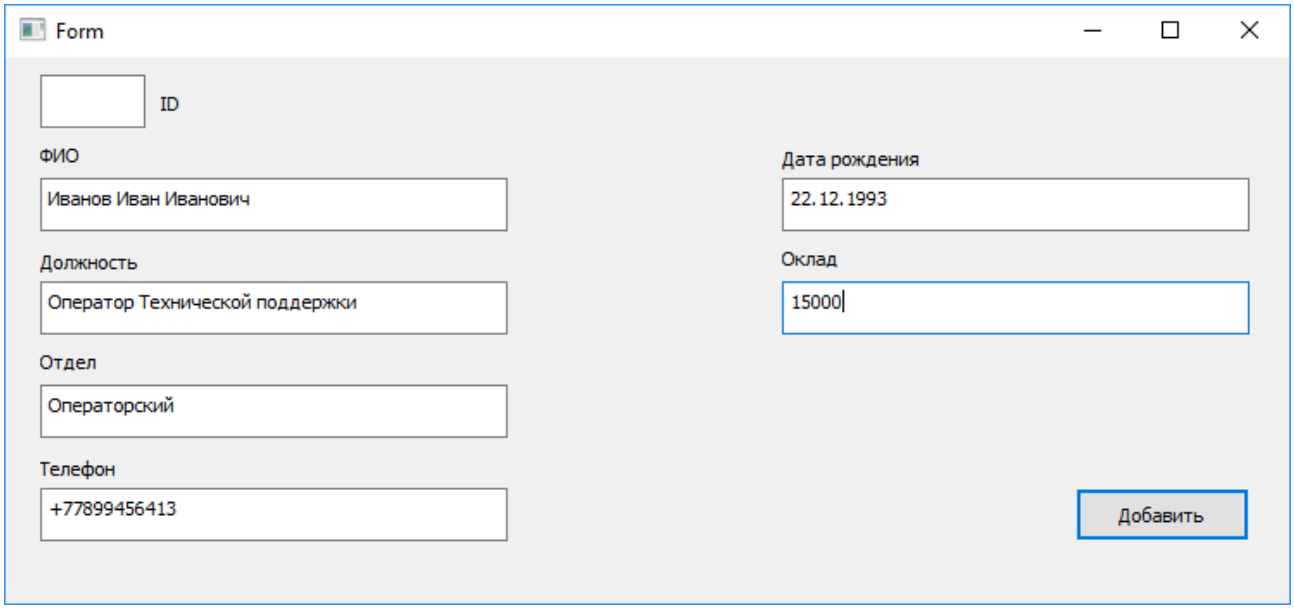


Рисунок 9 – Добавление нового сотрудника в базу данных

После нажатия кнопки «Добавить» происходит формировка запроса к базе данных, далее запрос проходит через «Криптомодуль», который шифрует данный запрос, он направляется на сервер, там проходит процесс дешифровки, сервер обращается к базе данных с запросом на добавление, если никаких ошибок не происходит, то запись добавляется. Проверить добавление можно с помощью кнопки «Поиск».

После выбора пункта меню «Редактор», далее «Добавить клиента», появляется диалоговое окно, предлагающее ввести информацию, которая указана на рисунке 10.

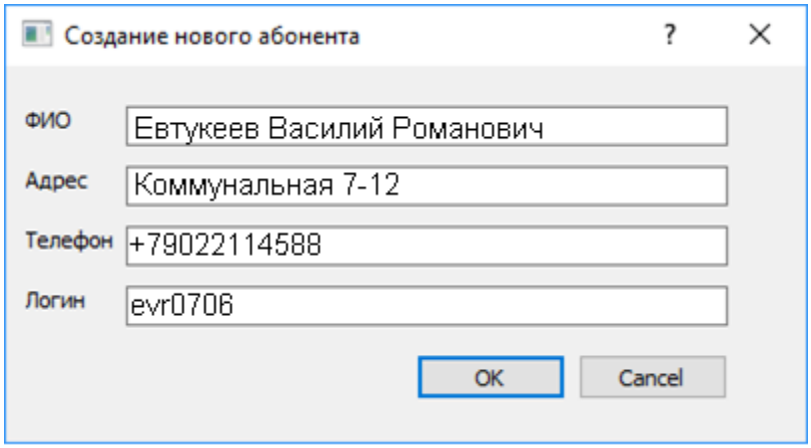
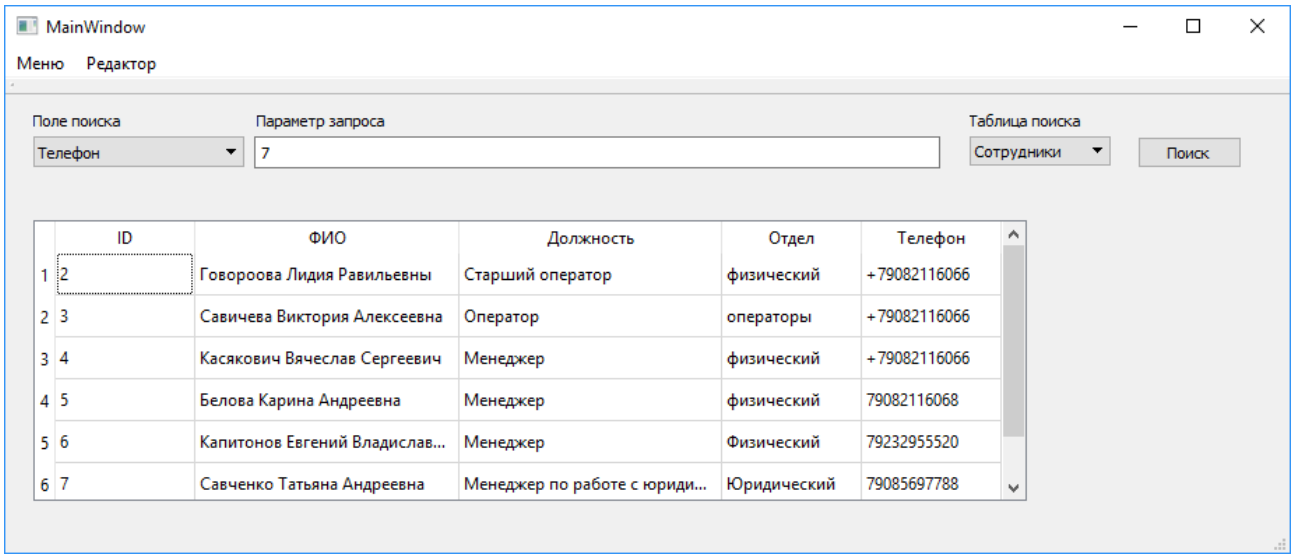


Рисунок 10 – Добавление клиента в базу данных

По нажатию кнопки «OK», происходит формировка запроса к базе данных, далее запрос проходит через «Криптомодуль», который шифрует данный запрос, он направляется на сервер, там проходит процесс дешифровки, сервер обращается к базе данных с запросом на добавление, если никаких ошибок не происходит, то запись добавляется. Проверить добавление можно с помощью кнопки «Поиск».

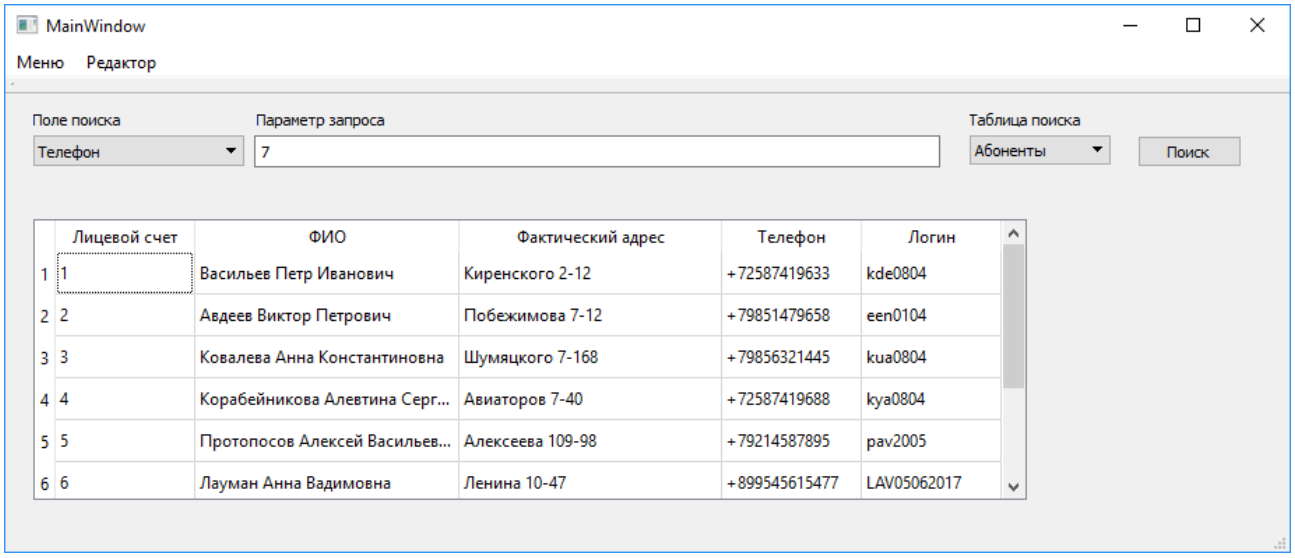
При нажатии кнопки поиск с введением, каких либо параметров, запрос передается в «Криптомодуль», в зашифрованном виде далее на сервер, сервер совершает дешифровку, делает запрос к базе данных, результат запроса направляется в «Криптомодуль», в зашифрованном виде передается клиенту,

клиент его расшифровывает и получает результат запроса, выводя его в таблицу. Итог вышеописанной операции можно видеть на рисунке 11 и рисунке 12.



	ID	ФИО	Должность	Отдел	Телефон
1	2	Говороова Лидия Равильевны	Старший оператор	физический	+79082116066
2	3	Савичева Виктория Алексеевна	Оператор	операторы	+79082116066
3	4	Касякович Вячеслав Сергеевич	Менеджер	физический	+79082116066
4	5	Белова Карина Андреевна	Менеджер	физический	79082116068
5	6	Капитонов Евгений Владислав...	Менеджер	Физический	79232955520
6	7	Савченко Татьяна Андреевна	Менеджер по работе с юриди...	Юридический	79085697788

Рисунок 11 – Результат запроса с полем поиска «Телефон» и параметром «7» к таблице «Сотрудники»



	Лицевой счет	ФИО	Фактический адрес	Телефон	Логин
1	1	Васильев Петр Иванович	Киренского 2-12	+72587419633	kde0804
2	2	Авдеев Виктор Петрович	Побежимова 7-12	+79851479658	een0104
3	3	Ковалева Анна Константиновна	Шумяцкого 7-168	+79856321445	kua0804
4	4	Корабейникова Алевтина Серг...	Авиаторов 7-40	+72587419688	kya0804
5	5	Протопосов Алексей Васильев...	Алексеева 109-98	+79214587895	pav2005
6	6	Лауман Анна Вадимовна	Ленина 10-47	+899545615477	LAV05062017

Рисунок 12 - Результат запроса с полем поиска «Телефон» и параметром «7» к таблице «Абоненты»

После двойного щелчка мышки по какой-либо из строк, полученного результата, будет сформирован другой запрос к базе данных по той же схеме. В зависимости от того на результат запроса к какой таблице кликает пользователь, откроется окно представленное либо на рисунке 13, если это «Сотрудники», либо на рисунке 14, если это «Абоненты».

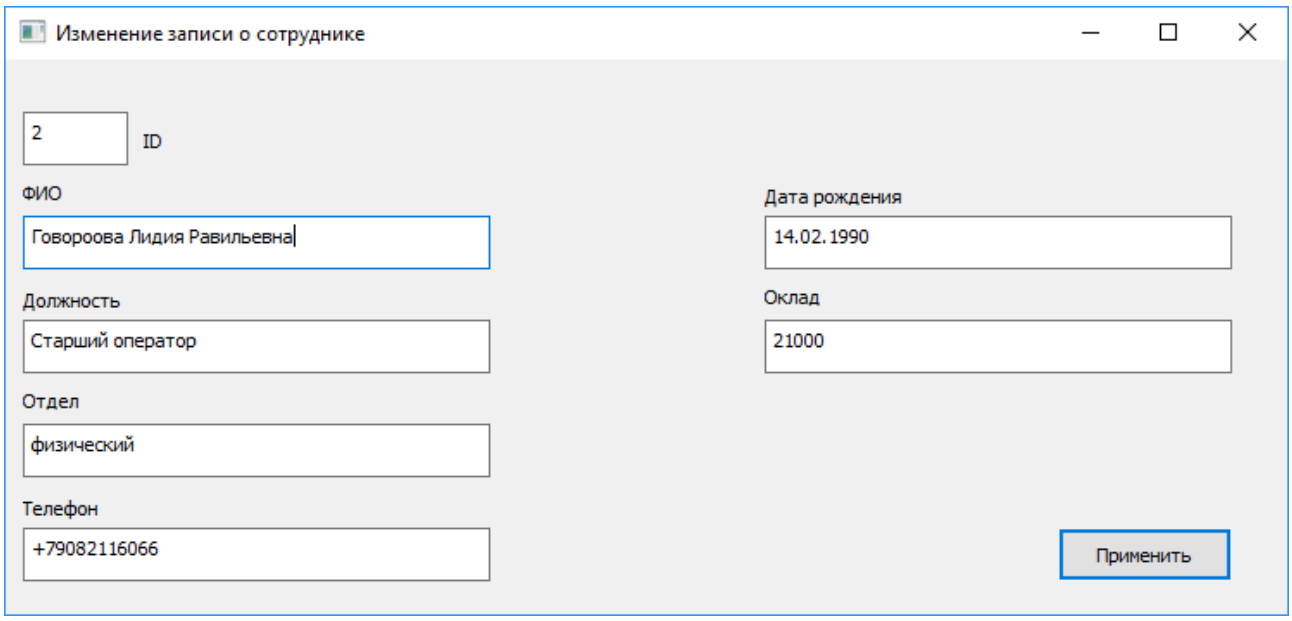


Рисунок 13 – Результат открытия окна изменения записи о сотруднике

Диалоговое окно, изображенное на рисунке 13, позволяет пользователю не только просмотреть записи о текущем сотруднике, но и изменить его. Достаточно изменить какую-либо строку и нажать кнопку «Применить».

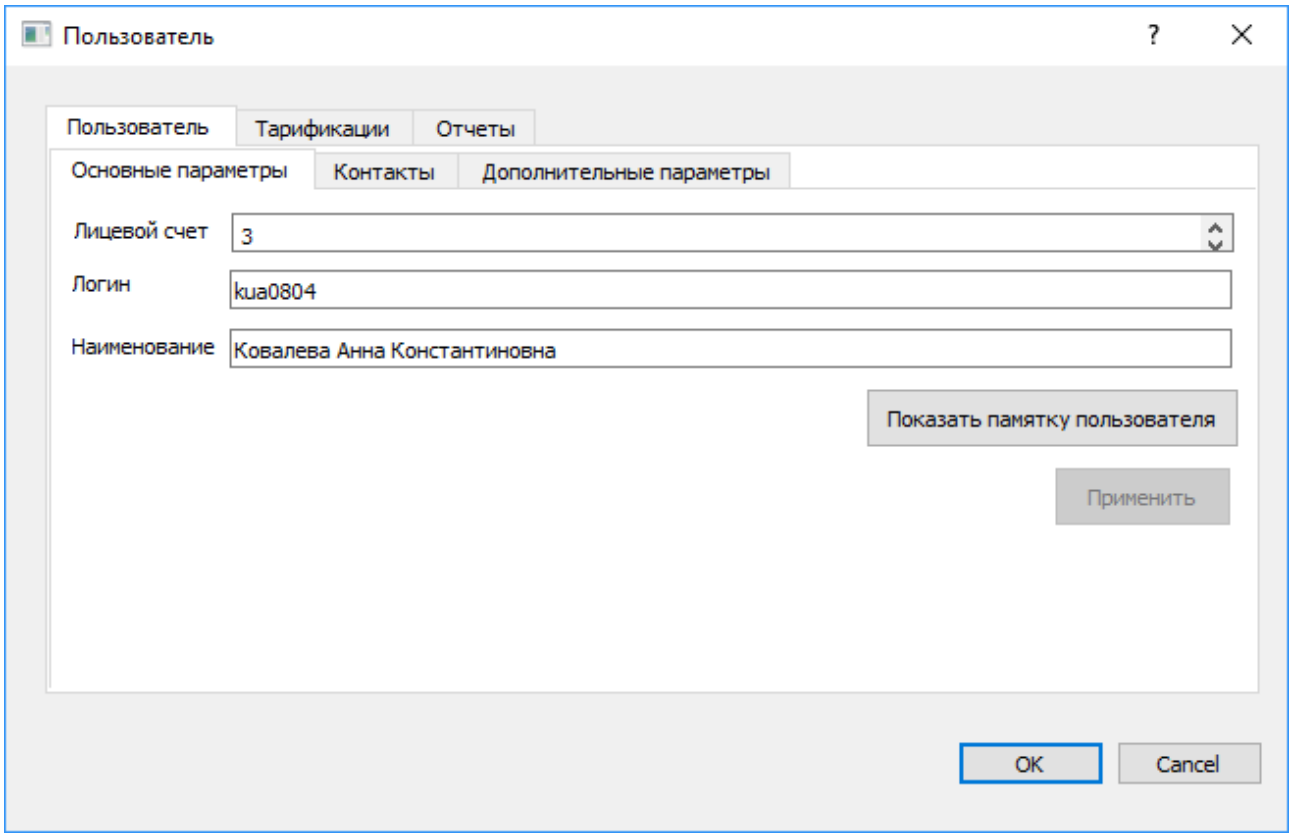


Рисунок 14 – Окно обзора учетной записи пользователя

На рисунке 14 изображено диалоговое окно, которое отображает всю информацию об абоненте. С помощью него есть возможность узнать лицевой счет абонента, логин для аутентификации в личный кабинет, фио, так же есть возможность распечатать «Памятку пользователя». Вся эта информация хранится во вкладке «Основные параметры». Вкладка «Контакты» содержит информацию по адресу проживания абонента, контактному номеру телефона, номеру подъезда и этажа. Данное окно представлено на рисунке 15.

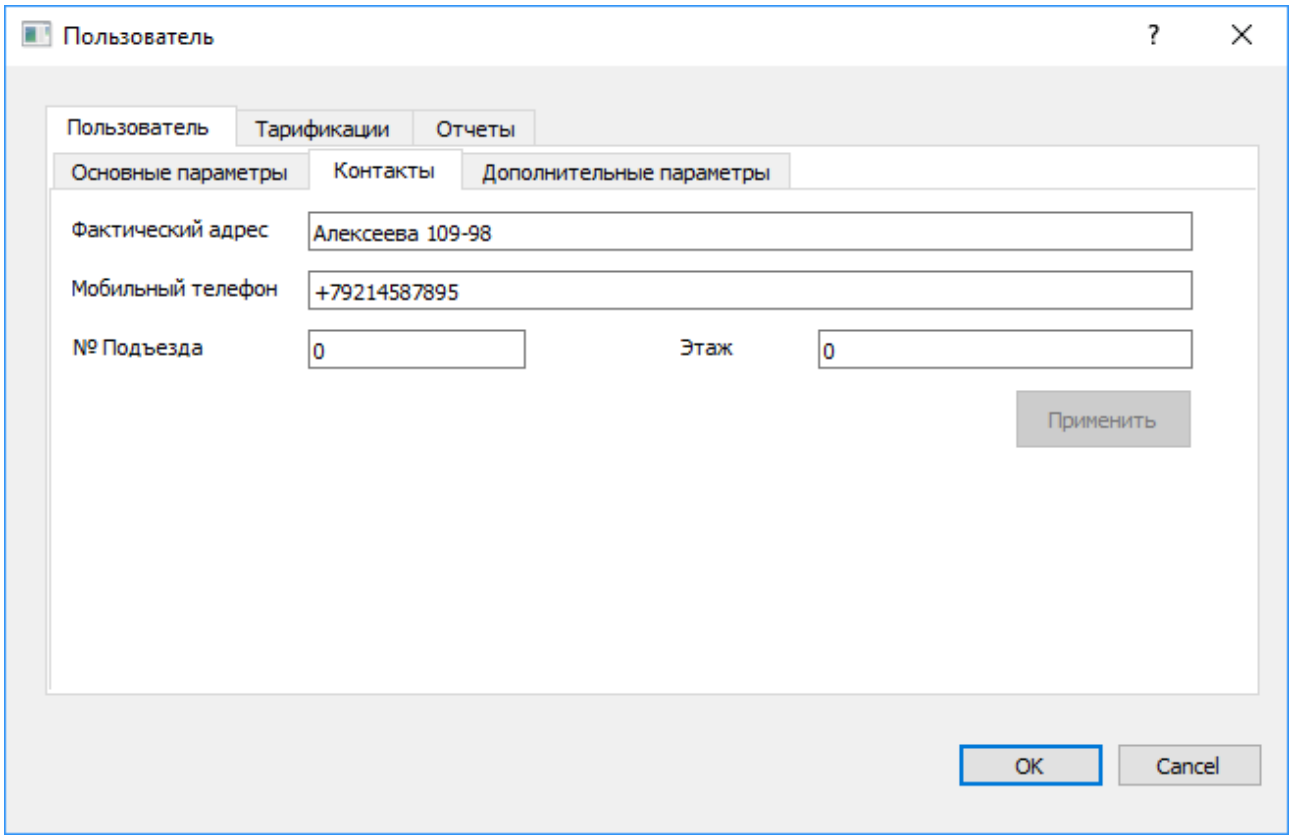


Рисунок 15 – Вкладка «Контакты»

Во вкладке «Дополнительные параметры» включает в себя: паспортные данные абонента, его ИНН, КПП, комментарии, сопутствующие учетной записи, IP-адрес свитча и номер порта, к которому подключен абонент. Пример такого окна показан на рисунке 16.

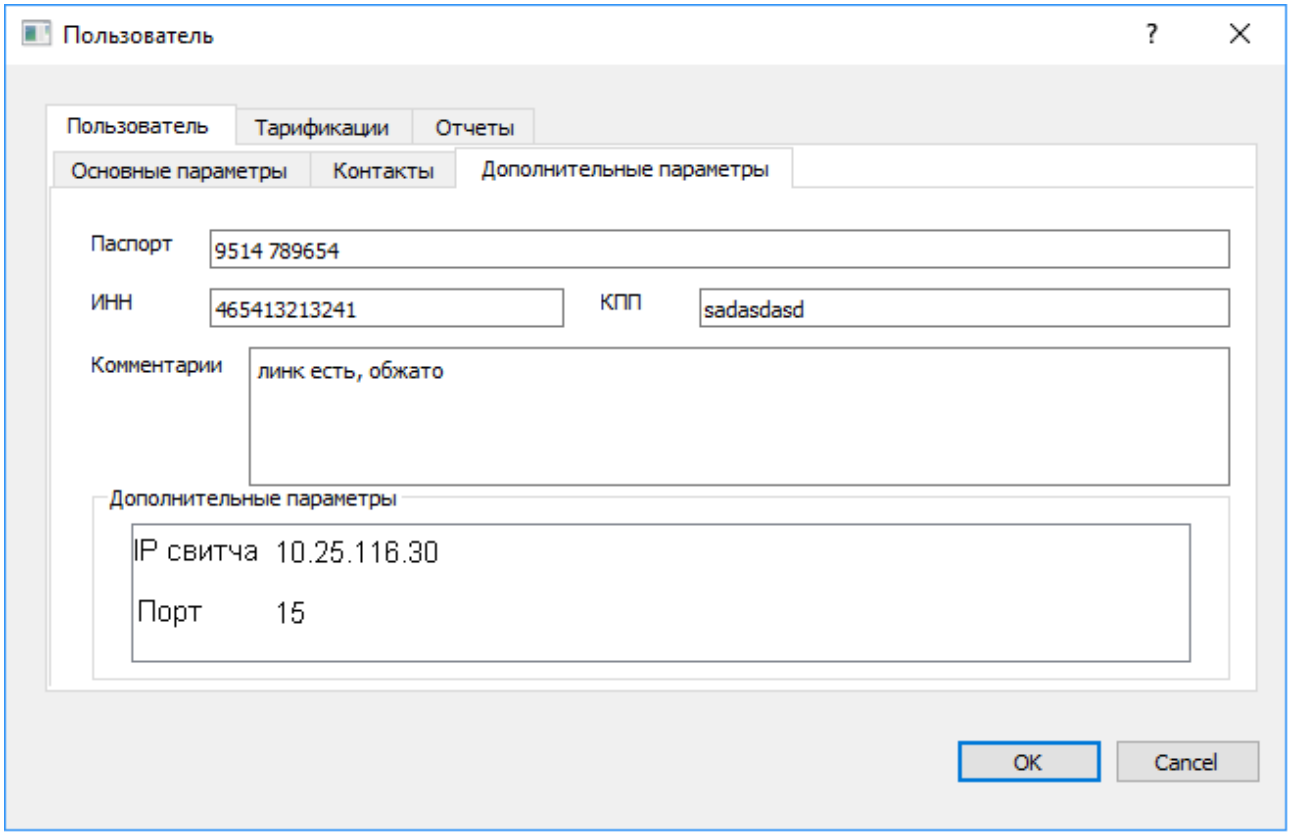


Рисунок 16 – Вкладка «Дополнительные параметры»

Одна из важнейших вкладок абонентской учетной записи – «Тарификации». Содержимое вкладки представлено на рисунке 17.

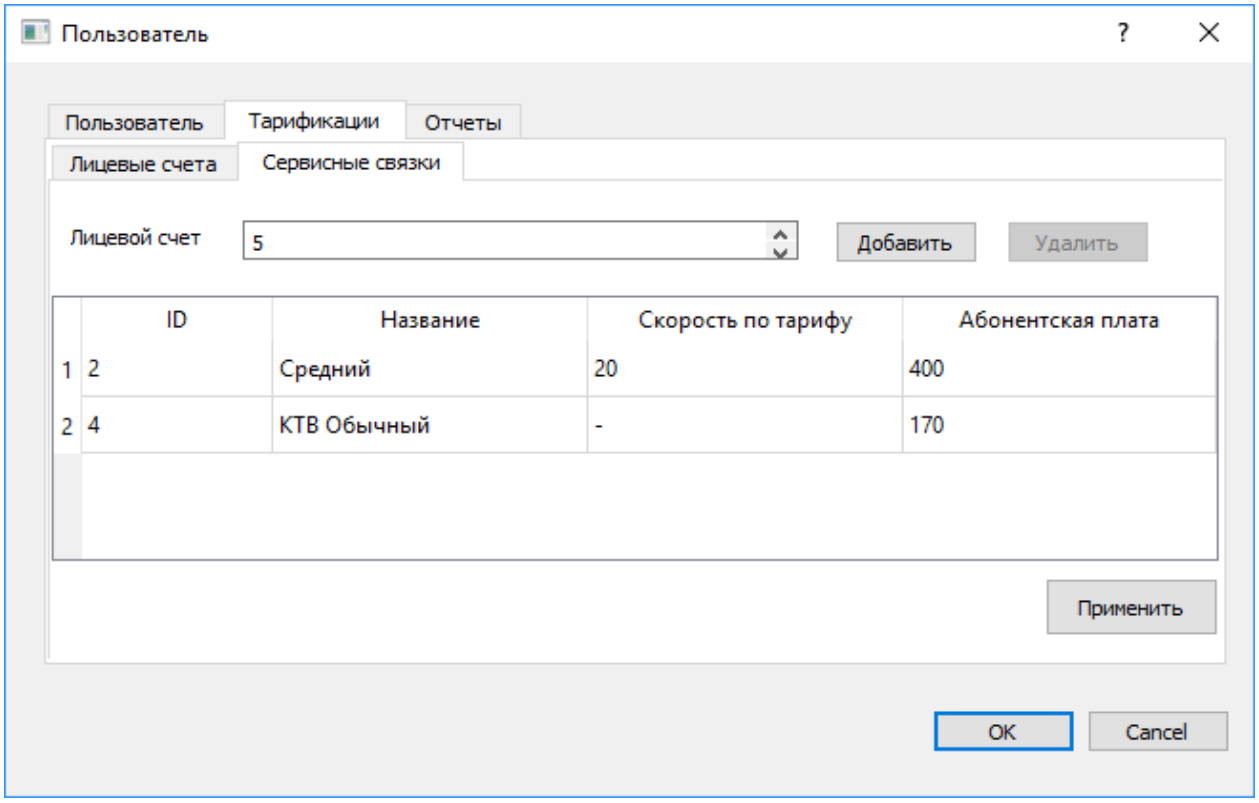


Рисунок 17 – Вкладка «Тарификации»

«Тарификации» содержат информацию по лицевым счетам абонента, в «Сервисных связках» есть возможность ознакомиться с услугами, к которым подключен абонент, его абонентскую плату за услуги, добавить тарифный план кнопкой «Добавить», окно добавления тарифного плана изображено на рисунке 18.

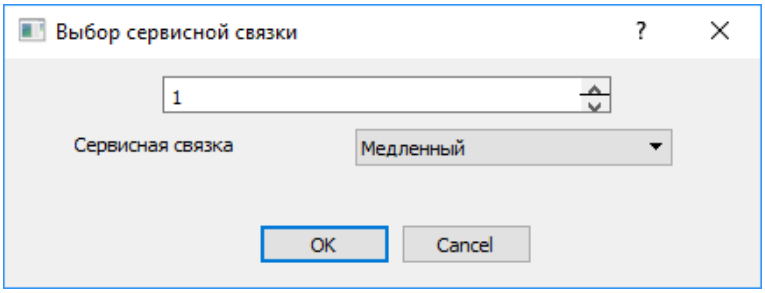


Рисунок 18 – Окно добавления тарифного плана

5.2 Серверная часть

В данном программном комплексе сервер выполняет функцию посредника, чтобы исключить взаимодействие клиента и базы данных напрямую. После запуска сервера, он начинает работать в фоновом режиме на машине вместе в паре с SQL – сервером. Сервер, как и клиент, имеет функции шифрации и дешифрации данных. Все запросы, зашифрованные клиентом, передаются серверу по средству TCP – сокета. После получения данных сервером, они расшифровываются, сервер делает запрос к базе данных, полученный результат снова шифруется и передается клиенту, где результат запроса дешифровывается и выводится на экран.

Сервер постоянно находится в состоянии прослушки заданного порта, пока очередной клиент не создаст запрос. После двустороннего обмена информацией, клиент освобождает выделенную под сокет память и соединение с сервером прекращается.

После запуска сервера появляется окно аутентификации. Принцип аутентификации, в данном случае, отличается от клиента. Если клиент проходит этот процесс на уровне обращения к базе данных, то сервер это делает на уровне SQL – server. То есть, чтобы серверная часть приложения запустилась без каких-либо проблем, необходим созданный пользователь, который может пройти авторизацию в SQL – сервер.

ЗАКЛЮЧЕНИЕ

В России законодательство в области персональных данных существует не так давно. Изучение нормативно – правовой базы в данной области дает существенное преимущество перед лицами не знакомыми с ней. На сегодняшний день существует достаточное количество организаций, в которых не считают обязательным защиту ПДн. Навыки, полученные в ходе выполнения данной работы, являются фундаментом в дальнейшем изучении различных областей информационной безопасности связанных с ПДн. Также по ходу работы был выработан четкий алгоритм организации системы защиты ПДн.

В процессе выполнения данной работы были выполнены все поставленные задачи: разработана структурная схема программного комплекса, выбран язык программирования, на основании установленных критериев, изучена структура базы данных провайдера.

Для разработки криптомодуля была реализована библиотека для работы с арифметикой чисел, которые выходят за границы стандартных типов данных, что помогло закрепить навыки в области программирования математических операций и криптографии.

В течение реализации программного комплекса получены неоценимые навыки разработки, принципов функционирования и реализации биллинговых систем, что позволит в следствии более качественно выполнять свои обязанности на занимаемой должности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. СУБД Cache. Объектно-ориентрированная разработка приложений: учебный курс / В. Кирстен, М. Иринге р, П. Шульпе, Б. Рериг. – Санкт-Петербург: Питер, 2001. – 384 с.

2. Хомоненко, А.Д. Базы данных: учебник для высших учебных заведений. – 4-е изд., доп. и перераб. / под ред. проф. А. Д. Хомоненко. – Санкт-Петербург: КОРОНА принт, 2004. – 736с.

3. Энциклопедия технологий баз данных / М.Р. Когаловский – Москва: Финансы и статистика, 2002. – 800 с.

4. DeveloperNetwork [Электронный ресурс] // Пошаговое руководство. Подключение к данным в базе данных MSSQL (WindowsForms): [сайт]. - 2014. Режим доступа: https://msdn.microsoft.com/ru-ru/library/ms171893.aspx.

5. Кузнецов С. Д. Основы баз данных: учебное пособие // С. Д. Кузнецов - 2-е изд., испр. - М.: Интернет-Университет Информационных Технологий; БИНОМ Лаборатория знаний, 2007. - 484 с., ил.

6. Бурмистров А.С., Данилова Т.С., Сальшин В.И., Умаров А.С., Зелепухина В.А., Тарасевич Ю.Ю. Особенности разработки информационных систем // Двадцатая международная конференция. Математика. Компьютер. Образование. г. Пущино, 28 января 2 февраля 2013 г. Тезисы - М., Ижевск: РХД, 2013.- С. 205.

7. Мартин Грабер. SQL– К.: Издательство «ЛОРИ», 2003, – 644 с.

8. Бойко В.В., Савинков В.М. Проектирование баз данных информационных систем. – М.: Финансы и статистика, 1989.

9. Томас М. Конноли, Каролин Е. Бегг Базы данных. Проектирование, реализация, сопровождение. Теория и практика. – Москва-Санкт-Петербург-Киев, 2007. – 1111 с.

10. О персональных данных [Электронный ресурс]: федер. закон от 08.06.2006 №152-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

11. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Постановление Правительства РФ от 01.11.2012 №1119// Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

12. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Приказ ФСТЭК от 18.02.2013 №21]// Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

13. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: Методический документ от 15.02.2008 // Официальная страница службы ФСТЭК России. – Режим доступа: http://www.fstec.ru

14. СТО 4.2-07-2014 Система менеджмента качества. Общие требования к построению и оформлюению документов учебной деятельности. – Введ. 30.12.2013 – Красноярск : ИПК СФУ, – 2014, – 60 с.

ПРИЛОЖЕНИЕ А

Акт об определении уровня защищенности

Состав комиссии	Ф.И.О.	Должность
Председатель	Волжанин К.В.	Генеральный директор
Члены комиссии	Петров А.В.	Главный инженер
	Безликих Н.А.	Ведущий системный администратор
	Егорова С.В.	Коммерческий директор
	Васильева С.Е	Главный бухгалтер

Комиссия рассмотрев исходные данные информационной системы персональных данных(ИСПДн) «Клиентская база» в соответствии с Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определила:

категории персональных данных, обрабатываемых в ИСПДн:

1. специальные категории персональных данных - информация касающаяся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья;
2. биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность;
3. общедоступные персональные данные;
4. иные категории персональных данных.

объем обрабатываемых персональных данных - свыше 100000 субъектов;

угрозы, актуальные для ИСПДн: угрозы связанные с наличием недекларированных возможностей в прикладном программном обеспечении, то есть угрозы 2-го типа;

тип субъектов персональных данных, обрабатываемых в ИСПДн: ИСПДн обрабатывает персональные данные сотрудников оператора, а также лиц, не являющихся сотрудниками оператора;

5) структура ИСПДн: комплекс автоматизированных рабочих мести локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа, то есть распределенная ИСПДн. Присутствует подключение к сетям общего пользования.

По результатам анализа исходных данных, а также основываясь на модели угроз безопасности персональных данных при их обработке в ИСПДн, требуется установить 1 уровень защищенности персональных данных.

Председатель комиссии: _____ /_____/

Члены комиссии: _____ /_____/

_____ /_____/

_____ /_____/

_____ /_____/

Дата:

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт Космических и Информационных Технологий

Информационные Системы

УТВЕРЖДАЮ
Заведующий кафедрой ИС
_____ С.А. Виденин
подпись инициалы, фамилия
«16» 06 2017 г.

БАКАЛАВРСКАЯ РАБОТА

09.03.02 Информационные системы и технологии

Организация системы защиты персональных данных

Руководитель	16.06.17	ст.преподаватель	Ю.В.Шмагрис
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	16.06.17		Л.В.Терскова
	подпись, дата		инициалы, фамилия
Консультант	16.06.17	к.т.н., доцент	И.А.Легалов
	подпись, дата	должность, ученая степень	инициалы, фамилия
Нормоконтролер	16.06.17		Ю.В. Шмагрис
	подпись, дата		инициалы, фамилия

Красноярск 2017