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

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

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

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка автоматизированной информационной системы для обработки статистических данных в ГБУЗ АО «АМИАЦ»

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

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

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

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

Благовещенск 2022

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

Факультет математики и информатики
Кафедра информационных и управляющих систем

ЗАДАНИЕ

К выпускной квалификационной работе студента Ушаковой Виолетты Алексеевны

1. Тема выпускной квалификационной работы: Разработка автоматизированной информационной системы для обработки статистических данных в ГБУЗ АО «АМИАЦ»

(утверждена приказом от)

2. Срок сдачи студентом законченной работы (проекта): 21.06.2022 г.

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

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

5. Перечень материалов приложения (наличие чертежей, таблиц, графиков, схем, программных продуктов, иллюстративного материала и т.п.): схема организационной структуры предприятия, диаграммы внешнего и внутреннего

документооборота, логическая модель БД, физическая модель БД, алгоритм работы и структура программного продукта, экранные формы.

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

7. Дата выдачи задания: 20.02.2022 г.

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

Задание принял к исполнению (20.02.2022): _____

(подпись студента)

РЕФЕРАТ

Бакалаврская работа содержит 69 с., 19 рисунков, 9 таблиц, 2 приложения, 22 источника.

ГБУЗ АО «АМИАЦ», АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА, ДОКУМЕНТООБОРОТ, ER-ДИАГРАММА, ИНФОЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ, ЛОГИЧЕСКАЯ МОДЕЛЬ, ФИЗИЧЕСКАЯ МОДЕЛЬ

Разработана автоматизированная информационная система для обработки статистических данных в ГБУЗ АО «АМИАЦ».

Цель работы заключается в создании автоматизированной информационной системы для обработки статистических данных в ГБУЗ АО «АМИАЦ». Данная система предназначена снизить трудоемкость выполнения ручных операций по выборке статистических данных и проведения анализа обработки данных в целом.

Приложение имеет простой и интуитивно понятный интерфейс, удобную навигацию и приятный дизайн для всей целевой аудитории разработанного проекта. Результатом работы является автоматизированная информационная система для обработки статистических данных в ГБУЗ АО «АМИАЦ».

Область применения разработки: отдел медицинской статистики, сбора, обработки и анализа медико-статистической информации, а также отдел технического обеспечения, программного сопровождения и телемедицинских технологий.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС – автоматизированная информационная система;

БД – база данных;

ВКР – выпускная квалификационная работа;

ПК – персональный компьютер;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина;

СУБД – система управления базами данных;

ВВЕДЕНИЕ

В современном мире большую роль играет автоматизация в сфере здравоохранения. Медицинские учреждения обрабатывают и хранят огромные объемы данных о пациентах. Жизнь абсолютно каждого человека зависит от развития медицинских информационных систем. От того, насколько грамотно и эффективно они используются медицинскими работниками, зависит качество медицинского обслуживания, общий уровень жизни населения, уровень развития страны в целом.

Работа над вопросом развития в сфере здравоохранения началась уже давно, но глобально этот вопрос был рассмотрен 24 декабря 2018 года на заседании президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам. На данном заседании был утвержден паспорт национального проекта «Здравоохранения» о реализации «Создания единого цифрового контура здравоохранения на основе ЕГИСЗ»

До недавнего времени в российском здравоохранении практически не было признаков автоматизации. Карточки, выписка льгот, протоколы процедур, карты больных, лекарства - все велось на бумаге. Это сказывалось на скорости, а, следовательно, и на качестве обслуживания пациентов, затрудняло работу медицинского персонала, что приводило к врачебным ошибкам, длительному заполнению карт, составлению отчетов.

В настоящее время это и привело к созданию медицинских информационных систем в сфере здравоохранения.

1 АНАЛИЗ ДЕЯТЕЛЬНОСТИ УЧРЕЖДЕНИЯ

1.1 Цели и задачи учреждения

Предметом исследования является государственное бюджетное учреждение здравоохранения Амурской области «Амурский медицинский информационно-аналитический центр»

Учреждение создано в соответствии с Гражданским Кодексом Российской Федерации, нормативными правовыми актами на основании приказа управления здравоохранения Администрации Амурской области от 19.04.1994 г.

Медицинский информационно-аналитический центр выступает центральным звеном в организации сбора, обработки информации и показателей медицинской статистики, медико-демографической, финансовой, кадровой составляющих здравоохранения Амурской области.

Учреждение создано для формирование единой информационной системы здравоохранения Амурской области путем организации современных компьютерных технологий межотраслевой системы сбора, обработки, хранения и представления информации, обеспечивающей динамическую оценку состояния здоровья населения области, материально-технической базы учреждений здравоохранения области, а также обеспечение информационной поддержки мероприятий по дополнительному лекарственному обеспечению.

1.2 Организационная структура учреждения

Учреждение состоит из нескольких взаимодействующих между собой подразделений, приведенных на рисунке 1.

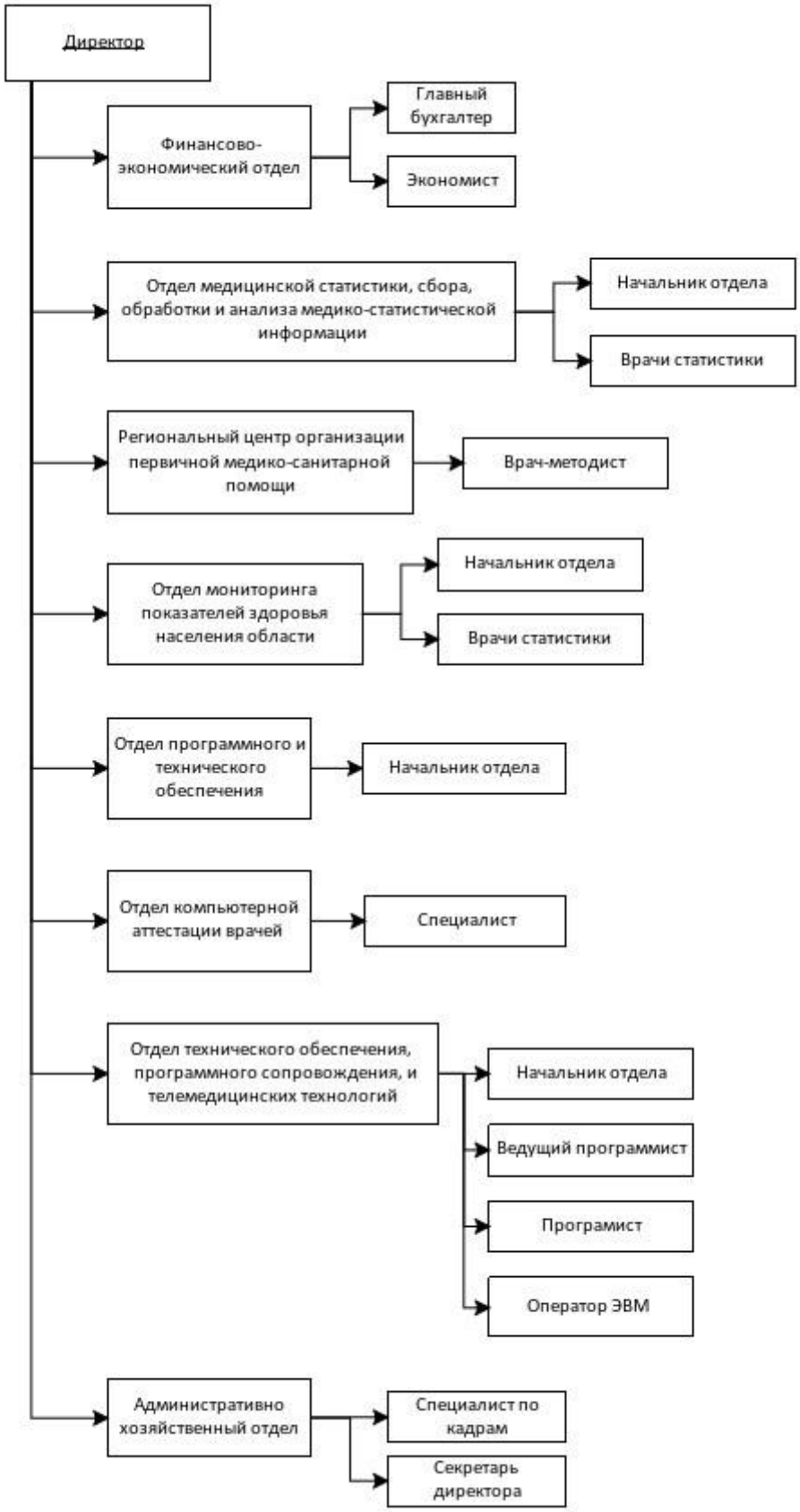

Рисунок 1 – Организационная структура ГБУЗ АО «АМИАЦ»

Во главе учреждения стоит директор, в подчинении которого находятся:

- финансово-экономический отдел;
- отдел медицинской статистики, сбора, обработки и анализа медико-статистической информации;
- региональный центр организации первичной медико-санитарной помощи;
- отдел мониторинга показателей здоровья населения области;
- отдел программного и технического обеспечения;
- отдел компьютерной аттестации врачей;
- отдел технического обеспечения, программного сопровождения, и телемедицинских технологий;
- административно хозяйственный отдел.

Подразделения выполняют следующие операции, приведенные ниже.

Директор организует работу учреждения, утверждает структуру и штаты, устанавливает размеры должностных окладов, подписывает финансовые и иные документы, осуществляет прием на работу сотрудников, контролирует работу и обеспечивает эффективное взаимодействие структурных подразделений, обеспечивает соблюдение законности в деятельности учреждения, осуществляет иные полномочия (функции), соответствующие уставным целям учреждения и не противоречащие федеральному и областному законодательству.

Финансово-экономический отдел ведет первичный бухгалтерский учет, производит расчет окладов и начисление заработной платы сотрудникам, выполняет расчет налоговых отчислений.

Отдел медицинской статистики, сбора, обработки и анализа медико-статистической информации занимается сбором, обработкой и анализом данных поступающих с медицинских организаций, а так же ведут отчетность для отдела мониторинга показателей здоровья населения Амурской области.

Региональный центр организации первичной медико-санитарной помощи занимается внедрением модели бережливой поликлиники.

Отдел мониторинга показателей здоровья населения Амурской области занимается сбором и обработкой информации по показателем здоровья населения, подготавливает еженедельные отчеты и доклады.

Отдел программного и технического обеспечения отвечает за работу программного и технического обеспечения учреждения. Ведения отчетности, изготовления электронных цифровых подписей, а также работу технической поддержки для медицинских организаций и для пациентов при электронной записи на прием к врачу и получению льгот.

Отдел компьютерной аттестации врачей производит один из видов аттестации на подтверждение квалификационной категории.

Отдел программного и технического обеспечения телемедицинских технологий внедряет информатизацию в медицинские организации, предоставляет платное техническое обеспечение.

Административно хозяйственный отдел осуществляет подбор персонала, подготовку отчетов по трудовой деятельности.

1.3 Анализ документооборота

Внешний документооборот – это движение документов, исходящих и входящих, которые подлежат возврату или отправке за пределы предприятия..

Диаграмма внешнего документооборота представляет собой контекстную диаграмму, построенную в нотации DFD (рисунок 2).

В состав диаграммы внешнего документооборота входят:

- процесс – ГБУЗ АО «АМИАЦ»;
- внешние сущности – ОПФР по Амурской области, УФСН по Амурской области, банк, граждане, Министерство здравоохранения РФ, Министерство здравоохранения АО, Правительство АО, служба технической поддержки, фонд социального страхования, Загс, медицинские организации, разработчики аппаратного обеспечения, аптечные организации;

– потоки документов, которые обеспечивают взаимодействие процесса с внешними сущностями – отчеты, письма, налоги, счета, законы и нормативные документы, различные запросы и прочее.

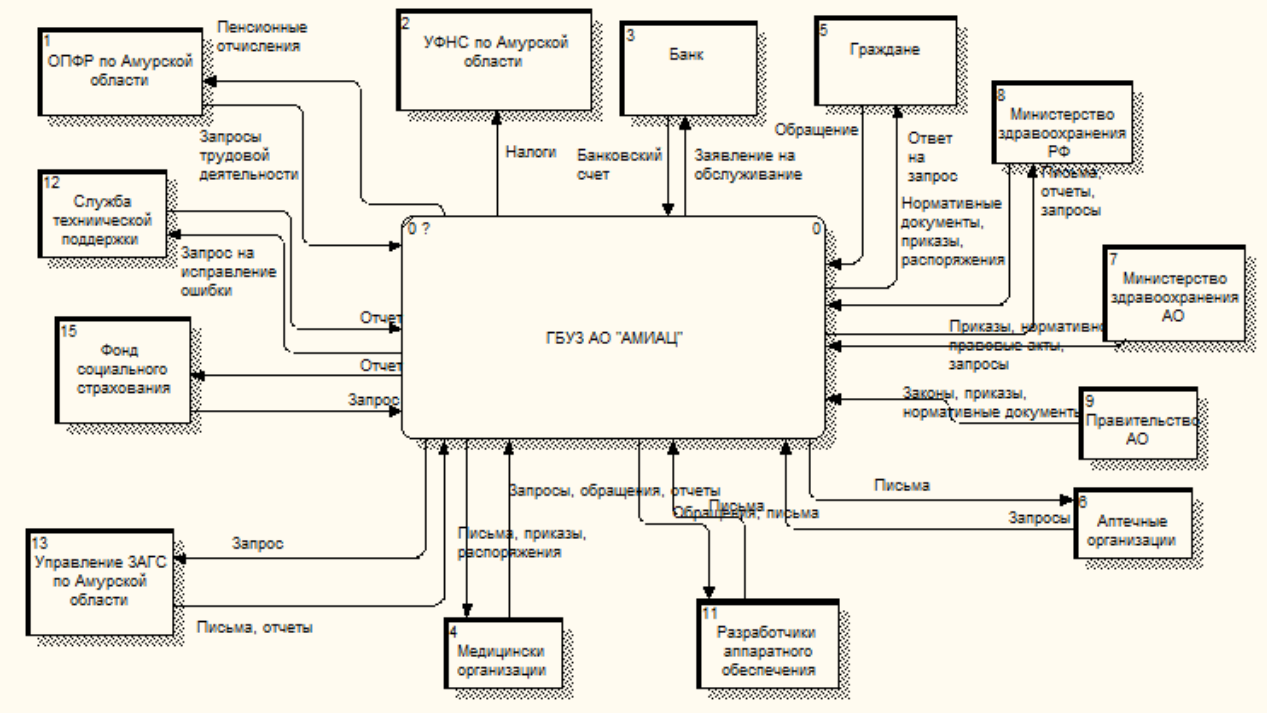

Рисунок 2 – Внешний документооборот предприятия

Внутренний документооборот – это движение документов внутри предприятия или организации, которые регулируются ведомственными или корпоративными нормативными правовыми актами.

Диаграмма внутреннего документооборота, построенная в нотации DFD, приведена на рисунке 3.

В состав диаграммы входят директор и все отделы предприятия – финансово экономический отдел, отдел компьютерной аттестации врачей, региональный центр организации первичной медико-санитарной помощи, административно-хозяйственный отдел, отдел технического обеспечения, программного

сопровождения и телемедицинских технологий, отдел медицинской статистики, сбора, обработки и анализа медико-статистической информации, отдел монито

ринга показателей здоровья населения области, отдел программного и технического обеспечения, а также внутренние документы, используемые внутри предприятия. Это могут быть приказы, распоряжения, отчеты разной формы, нормативные документы и так далее.

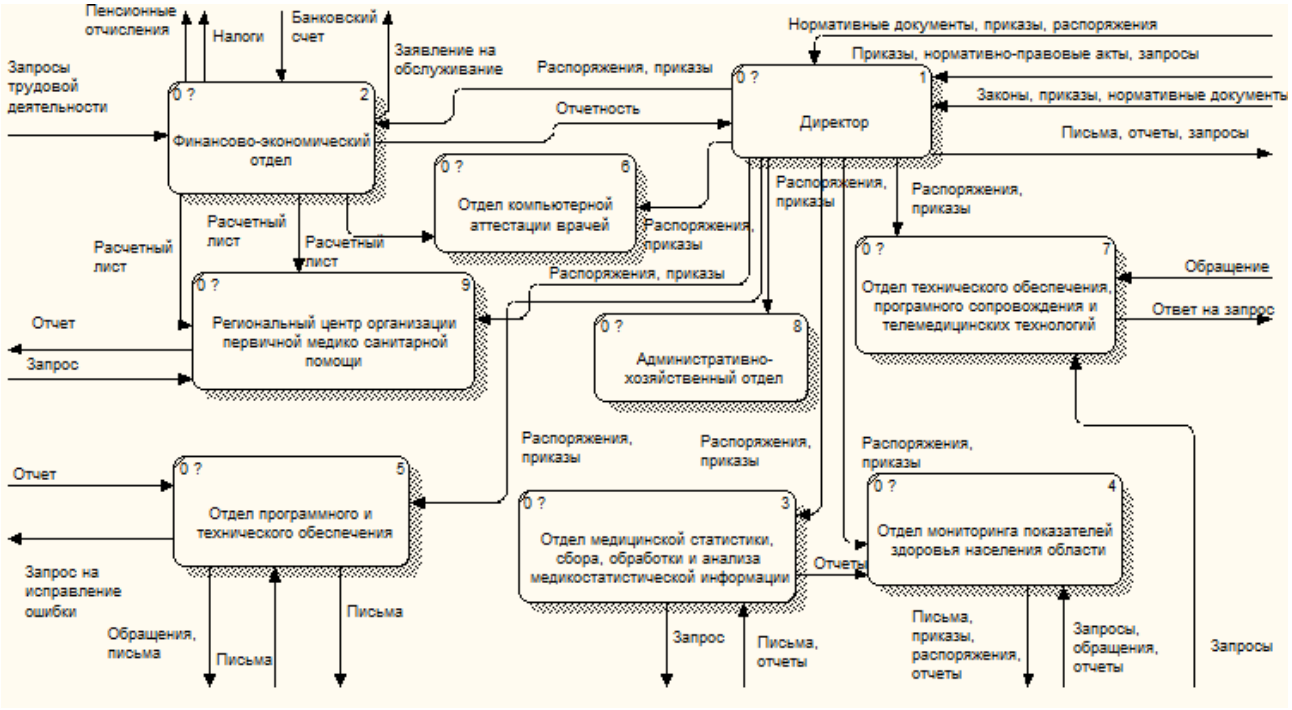

Рисунок 3 – Внутренний документооборот предприятия

1.4 Анализ программного и аппаратного обеспечения предприятия

В ГБУЗ АО «АМИАЦ» все рабочие места оборудованы персональными компьютерами, многофункциональными устройствами и источниками бесперебойного питания. Каждый компьютер имеет выход в Интернет.

В учреждении используется топология локальной сети «Звезда», При топологии «звезда» все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту, именуемому концентратором. Сигналы от передающего компьютера поступают через концентратор ко всем остальным. Эта топология возникла на заре вычислительной техники, когда компьютеры были подключены к центральному, главному, компьютеру.

Достоинства топологии локальной сети «звезда»:

– выход из строя одной рабочей станции не отражается на работе всей сети в целом;

– масштабируемость сети;

– лёгкий поиск неисправностей и обрывов в сети;

– высокая производительность сети (при условии правильного проектирования);

– гибкие возможности администрирования.

Недостатки топологии локальной сети «звезда»:

– выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;

– для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;

– конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

Программное обеспечение – совокупность программных и документальных средств для создания и эксплуатации систем, обработки данных.

В учреждении на всех ПК установлена операционная система Windows 10/11.

На всех ПК установлена антивирусная защита – Dr.Web и браузер для выхода в Интернет – Google.

Сотрудники обрабатывают данные с помощью офисного пакета Microsoft Office 2019.

В учреждении используется такая программа как «Медведь». «Медведь» – это программное решение, которое позволяет собирать и анализировать данные из медицинских систем, а также передавать их в любых форматах, тем самым обеспечивая интеграцию информационных систем между собой и с сервисами федерального уровня.

ТМ:ЦОД используется для централизованной обработки данных и информационного взаимодействия субъектов региональной системы здравоохранения. ТМ:ЦОД собирает данные о рецептах, направлениях свидетельствах о смерти, всю электронную медицинскую документацию, программа аккумулирует их и преобразует в отчеты.

Сервис «Управление потоками пациентов» осуществляет подключение государственных и муниципальных медицинских учреждений, к централизованной подсистеме «Управление потоками пациентов». Сервис позволяет решать следующие задачи:

– приём звонков, поступающих от населения;

– создание информационной карты вызова;

– ведение типовых сценариев диалога и информационной базы;

– ведение базы заданий, предусмотренных повседневной деятельностью медицинского персонала: обзвон граждан, подготовка отчётности и пр.

– хранение записей телефонных разговоров;

– ведение отраслевой отчётности;

– информационный обмен с существующими медицинскими информационными системами (работа с расписанием, база пациентов).

РАМИ – региональный архив медицинских изображений. Для организации единого информационного пространства службы лучевой диагностики целесообразно использование региональной радиологической информационной системы (РРИС), которая позволяет реализовать распределенную модель хранения МИ. Посредством системы на региональном уровне обеспечивается доступ к локальным архивам МИ (PACS медицинских организаций) на основе кроссплатформенного веб-браузера.

Ассистент используется учреждением для обеспечения доступа к удалённым компьютерам.

В финансово-экономическом отделе установлена программа 1С: Бухгалтерия.

С недавних пор сотрудники АМИАЦ начинают переходить на систему электронного документооборота. СЭД «Дело» - это система автоматизации работы с документами на протяжении всего их жизненного цикла (создание, изменение, хранение, поиск, классификация и пр.), а также процессов взаимодействия между сотрудниками. Основными объектами автоматизации в таких системах являются документы.

В отделе медицинской статистики, сбора, обработки и анализа медико-статистической информации и в отделе мониторинга показателей здоровья населения области работают в программе «Парус». Используют ее для сбора сводной отчетности из медицинских организаций. Так же в этих отделах используют программу МедСтат и МедСС.

МедСтат – информационная система, позволяющая автоматизировать обработку медико-статистической информации. Программа предназначена для формирования, анализа и хранения отчетно-статистической информации согласно годовым отчетным формам медицинской статистики.

Программа «Медицинское свидетельство о смерти» предназначена для заполнения и печати медицинских свидетельств о смерти, ведения журнала умерших, автоматического создания посмертных эпикризов, создания отчетов по смертности на основании внесенных данных, печати бланков свидетельств о смерти.

КриптоПро используется сотрудниками АМИАЦ для шифрования, защиты информации, а также хранения секретных ключей.

Crypto+ DE — это программное обеспечение управления электронной подписью и шифрованием.

Модуль криптографической защиты информации для рабочего места пользователя

2 ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Информационная система (ИС) – это организационная совокупность технических и обеспечивающих средств, технологических процессов и кадров, реализующих функции сбора, хранения, обработки, поиска, выдачи и передачи информации.

2.1 Цель и задачи проектирования

Основная цель проектирования информационной системы – разработка АИС для удовлетворения информационных потребностей пользователей системы путем предоставления необходимой им информации на основе хранимых данных.

При проектировании необходимо решить следующие задачи:

– проектирование и создание БД;

– выбор среды разработки;

– реализация программного продукта.

Для разрабатываемой автоматизированной информационной системы составлено техническое задание, приведенное в приложении А.

2.2 Обоснование необходимости создания АИС.

Рассматриваемая организация осуществляет как традиционное хранение документации (в бумажном виде), так и в сетевых папках или на ПК. Большой объем электронной статистической информации проходит через каждого сотрудника, обработка которой занимает долгое время. Помимо этого существует шанс человеческой ошибки. Поэтому необходимо разработать автоматизированную информационную систему для обработки статистических данных в ГБУЗ АО «АМИАЦ», которая:

– будет автоматически рассчитывать процент и количество умерших людей в разрезе по нозологиям, возрасту, годам и районам;

– будет иметь базу данных, благодаря которой можно посмотреть данные за определенный период;

– будет показывать количество умерших по определенному диагнозу;

– будет обеспечивать ввод новых данных, просмотр и изменение уже имеющихся в базе;

– будет позволять вывести на печать данные из таблиц базы данных, а также экспортировать данные в Excel.

Преимуществом создания автоматизированной информационной системы является то, что ее функционал будет разработан специально для исследуемого предприятия, основываясь на его запросах и требованиях, будет включать только те функции и модули, которые будут необходимые для работы предприятия.

2.3 Характеристика обеспечивающих подсистем

2.3.1 Требования к пользователям

Для обслуживания необходим один администратор, обладающий высокими навыками владения ПК, имеющий опыт работы с базами банных и Microsoft SQL Server, программными продуктами.

Количество персонала, работающего с разработанной информационной системой, не ограничено. Пользователь должен иметь навыки работы с ПЭВМ, быть уверенным пользователем.

2.3.2 Требования к организационному обеспечению

Для обеспечения корректной работы информационной системы необходимо разработать руководство пользователя и провести инструктаж сотрудников. Для администратора системы создается отдельное руководство, так как он обеспечивает контроль правильного функционирования системы.

2.3.3 Требования к методическому обеспечению

Разработанная информационная система должна отвечать требованиям надежности:

– иметь окно авторизации для идентификации и аутентификации пользователя;

– иметь защиту от некорректных действий пользователей.

Окно авторизации предотвращает беспрепятственный доступ к данным информационной системы по учету заказов.

На восстановление отказа нужно несколько секунд времени, восстанавливает исправное функционирование пользователь самостоятельно, заполнив обязательные поля или удалив некорректно внесенные данные.

2.3.4 Требования к техническому обеспечению

Необходимый состав технических средств: персональный компьютер, источник бесперебойного питания для обеспечения устойчивой работы оборудования при сбоях в сети электропитания, локальная сеть.

Требуемые технические характеристики ПК:

– Процессор Intel, 64-разрядный;

– Оперативная память не менее 2 Гбайт;

– Монитор с расширением от 800x600 пикселей;

– Свободное место на жёстком диске не менее 6 Гбайт.

2.3.5 Требования к математическому обеспечению

Должен производиться правильный медико-статистический анализ и обработка данных.

2.3.6 Требования к программному обеспечению

Для работы программы на ПК сотрудников, использующих ее, должна быть установлена операционная система Windows не ниже 7.

На сервере предприятия установлен Microsoft SQL Server (версия не ранее 2017 года).

2.3.7 Требования к лингвистическому обеспечению

Лингвистическое обеспечение информационной системы подразумевает совокупность применяемых языковых средств, единый логический интерфейс системы.

Лингвистическое обеспечение включает:

– языки описания, управления и манипулирования данными в СУБД;

– алгоритмические языки, используемые при разработке модуля;

– системы диалогового взаимодействия пользователей и ПЭВМ.

В качестве СУБД выбран Microsoft SQL Server 2017.

Выбран язык запросов SQL и язык программирования C#.

Программное обеспечение программного продукта для организации взаимодействия с пользователем использует русский язык.

2.4 Выбор и обоснование средств разработки

Автоматизированная информационной системы по учету заказов для предприятия будет создаваться с помощью следующих программных средств:

а) Microsoft SQL Server Management Studio 2017

Microsoft SQL Server – это клиент-серверная система управления реляционными базами данных, ориентированная на работу под управлением систем Microsoft Windows.

б) Microsoft Visual Studio 2017

Microsoft Visual Studio 2017 – полнофункциональная, расширяемая и бесплатная интегрированная среда разработки для создания современных приложений Android, iOS и Windows, а также веб-приложений и облачных служб.

в) Язык SQL

Язык SQL – основа многих СУБД, поскольку отвечает за физическое структурирование и запись данных на диск, а также чтение данных с диска. Он также позволяет принимать SQL-запросы от других компонентов СУБД и пользовательских приложений.

г) Язык программирования C#

C# – один из самых популярных языков программирования. Его преимущества по сравнению с другими языками программирования:

2.5 Проектирование базы данных

Проектирование структуры базы данных автоматизированной информационной системы включает в себя инфологическое, логическое и физическое проектирование.

2.5.1 Инфологическое проектирование

В разрабатываемой БД были выбраны сущности «Пользователях», «Пациенты», «Диагноз», «Регион»

– Сущность «Пользователи» содержит данные о сотрудниках;

– Сущность «Пациенты» содержит информацию об умерших;
– Сущность «Диагноз» содержит виды нозологий;
– Сущность «Регион» содержит субъекты Амурской области;

Сущности имеют спецификацию атрибутов, указанную в таблицах 1-4.

Таблица 1 – Спецификация атрибутов сущности «Пользователи»

Наименование атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример
1	2	3	4	5
Фамилия сотрудника	фамилия сотрудника	текст	–	Иванова
Имя сотрудника	имя сотрудника	текст	–	Татьяна
Отчество сотрудника	отчество сотрудника	текст	–	Ивановна
Логин	логин по которому будет входить пользователь	текст	–	admin
Пароль	пароль по которому будет входить пользователь	текст	–	qwerty

Таблица 2 – Спецификация атрибутов сущности «Пациенты»

Наименование атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример
1	2	3	4	5
Снилс	код, однозначно определяющий пациента	числовой	>0	123-456-789 10
Дата рождения	дата рождения	дата	< текущей даты	04.02.2021
Пол	пол пациента	текст	–	женский
Дата смерти	дата смерти пациента	дата	< текущей даты	06.02.2021
Место смерти	место смерти пациента	дата	< текущей даты	06.02.2021
Причина смерти	место где наступила смерть	текст	–	стационар
Диагноз по МКБ	Диагноз изза которого наступила смерть	текст	–	Covid-19

Таблица 3 – Спецификация атрибутов сущности «Диагноз»

Наименование атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример
1	2	3	4	5
код диагноза	Сокращенное название диагноза	текст	–	U07.2
диагноз	Наименование диагноза	текст	–	Covid-19

Таблица 4 – Спецификация атрибутов сущности «Регион»

Наименование атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример
1	2	3	4	5
код региона	Сокращенное название региона	текст	–	28
регион	Наименование регион	текст	–	Амурская область

В качестве первичных ключей для каждой выделенной сущности были предусмотрены специальные атрибуты-идентификаторы, которые однозначно определяют каждую запись таблицы.

Каждая сущность имеет следующие первичные ключи:

– Фамилия сотрудника – для сущности «Пользователь», определяется один раз и не изменяется;

– Снилс – для сущности «Пациент», определяется один раз и не изменяется;

– Код диагноза – для сущности «Диагноз», определяется для каждого вида нозологии и не изменяется;

– Код региона – для сущности «Регион», определяется для каждого вида субъекта и не изменяется;

Между сущностями установлены связи, представленные в виде диаграмм в нотации Чена.

Между сущностями «Пользователь» и «Диагноз» установлена связь «один-к-одному» (рисунок 4).

Рисунок 4 – Связь «Пациент-Диагноз»

Рисунок 5 – Связь «Заказ-Клиент»

2.6 Логическое проектирование

На первом этапе логического проектирования рассматривается каждая связь между сущностями.

1 Связь «Пациент-Диагноз»

Между сущностями установлена связь «один-к-одному» (рисунок 6).

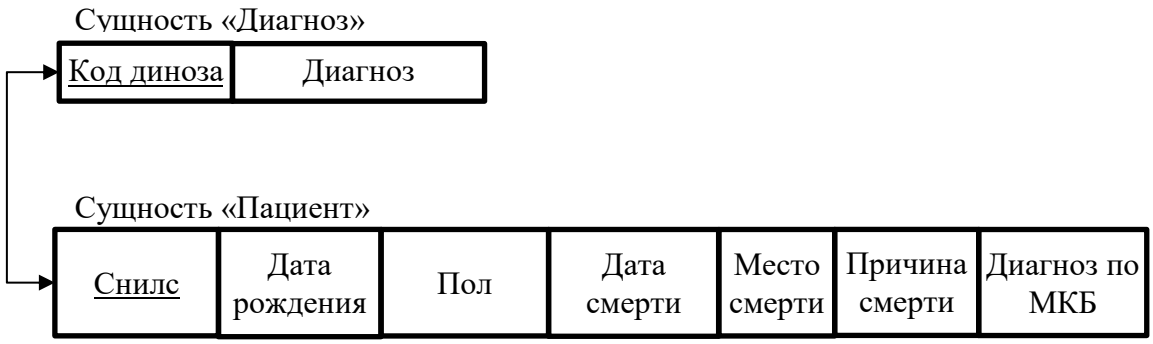

Рисунок 6 – Связь «Пациент-Диагноз»

2 Связь «Пациент-Регион»

Между сущностями установлена связь «один-к-одному» (рисунок 7).

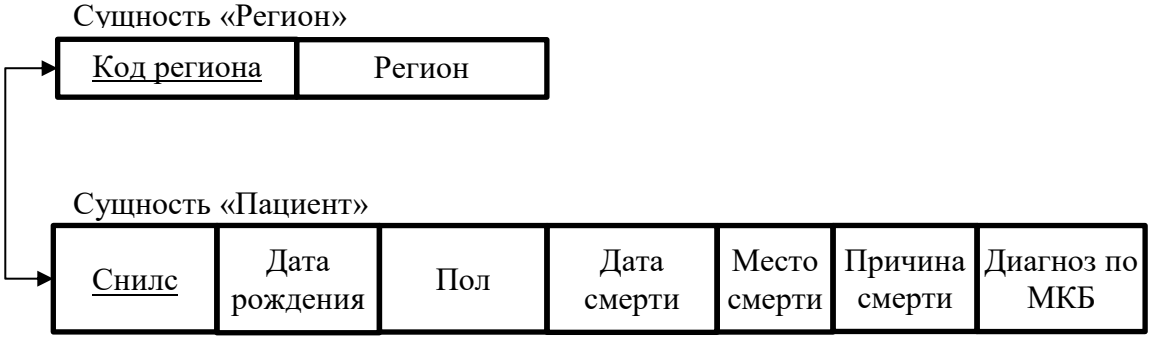

Рисунок 7 – Связь «Пациент-Регион»

Отношение 1 (Пациент)

Снилс	Код диагноза

Отношение 2 (Регион)

Снилс	Код региона

Отношение 3 (Диагноз)

Код диагноза	Диагноз

Отношение 4 (Регион)

Код региона	Регион

Отношение 5 (Пациент)

Снилс	Дата рождения	Пол	Дата смерти	Место смерти	Причина смерти	Диагноз по МКБ	Код Диагноза (FK)

Отношение 6 (Пациент)

Снилс	Дата рождения	Пол	Дата смерти	Место смерти	Причина смерти	Диагноз по МКБ	Код региона (FK)

Рисунок 8 – Множество отношений, полученных в результате анализа связей

На втором этапе логического проектирования выполняется анализ полученных на первом этапе проектирования отношений на соответствие 1НФ, 2НФ, 3НФ с целью удаления избыточности. Для проведения нормализации отношений строятся функциональные зависимости (рисунок 9).

Рисунок 9 – Функциональные зависимости отношений 1-4

Все отношения, представленные на рисунке 9, находятся в первой нормальной форме, и каждый атрибут, не являющийся ключевым атрибутом, в этих отношениях функционально полно зависит от первичного ключа.

Исследуемые отношения являются отношениями во второй нормальной форме – все не ключевые атрибуты функционально полно зависят от первичного ключа.

Все отношения находятся в третьей нормальной форме, так как они находятся во второй нормальной форме и все атрибуты, которые не являются ключевыми, не имеют транзитивной зависимости от ключевых атрибутов.

Логическая модель, построенная в виде диаграммы в методологии IDEF1X, приведена на рисунке 10.

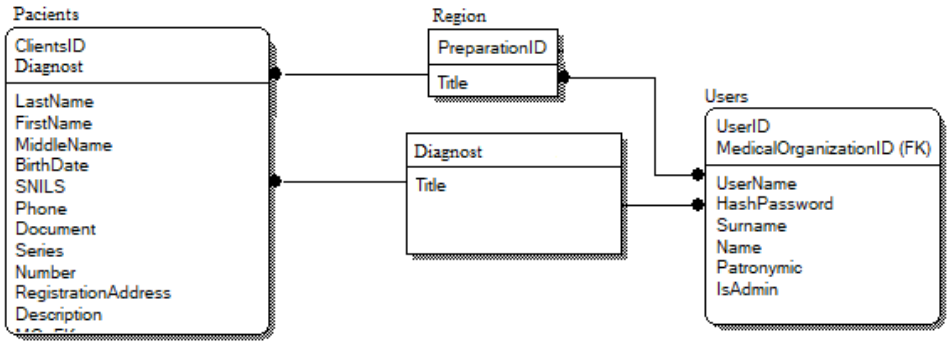

Рисунок 10 – Логическая модель БД

2.7 Физическое проектирование

На основании логической модели проектируется физическая модель БД. Проектирование структуры данных состоит в построении для каждого отношения таблицы «Физическая структура данных» (таблицы 5-8).

Таблица 5 – Физическая структура данных отношения 1 (Пациент)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
Снилс	числовой	Не NULL	Int()	Primary key
Дата рождения	дата	Не NULL	Date()	
Пол		Не NULL	Int()	
Дата смерти	дата	Не NULL	Date()	
Место смерти	текст	Не NULL	Int()	
Причина смерти	текст	Не NULL	Int()	
Диагноз по МКБ	текст	Не NULL	Int()	
Диагноз	числовой	Не NULL	Int()	Foreign key

Таблица 6 – Физическая структура данных отношения 2 (Пациент)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
Снилс	числовой	Не NULL	Int()	Primary key
Дата рождения	дата	Не NULL	Date()	
Пол		Не NULL	Int()	
Дата смерти	дата	Не NULL	Date()	
Место смерти	текст	Не NULL	Int()	
Причина смерти	текст	Не NULL	Int()	
Диагноз по МКБ	текст	Не NULL	Int()	
Регион	числовой	Не NULL	Int()	Foreign key

Таблица 7 – Физическая структура данных отношения 3 (Диагноз)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
Код диагноза	числовой	Не NULL	int	Primary key
Диагноз	текст	Не NULL	nvarchar(126)	

Таблица 8 – Физическая структура данных отношения 4 (Регион)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
Код региона	числовой	Не NULL	int	Primary key
Регион	текст	Не NULL	nvarchar(126)	

Физическое проектирование также предусматривает построение структуры физической модели данных в методологии IDEF1X (рисунок 11).

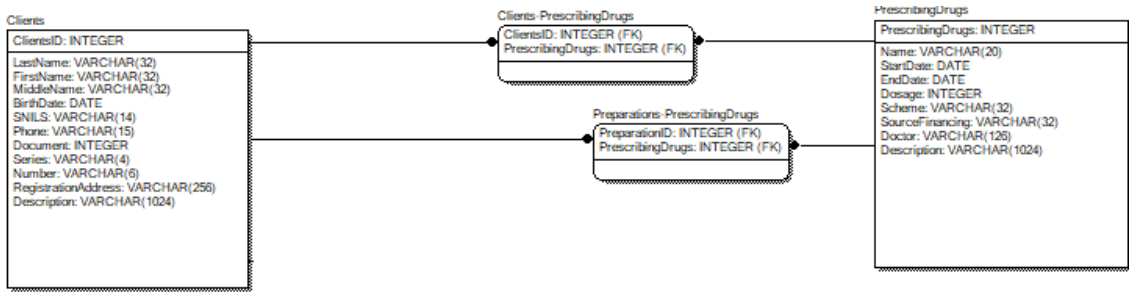

Рисунок 11 – Физическая модель БД

2.8 Требования информационной безопасности

Чтобы исключить неправомерный доступ к информации применяют такие средства, как идентификация и аутентификация. Их алгоритм работы заключается в том, чтобы получить от субъекта информацию, удостоверяющую его личность, проверить ее подлинность и предоставить (или не предоставить) этому субъекту возможность работы с системой.

Наличие процедур идентификации и/или аутентификации пользователей – обязательное условие любой защищенной системы.

Идентификация – это механизм присвоения собственного уникального имени или образа пользователю, взаимодействующего с информацией.

Аутентификация (установление подлинности) – это система способов проверки совпадений пользователя с тем паролем или образом, которому разрешен доступ.

3 РАЗРАБОТКА ПРОГРАММНОГО ПРОДУКТА

3.1 Общие сведения

Наименование программного продукта «Автоматизированная информационная системы для обработки статистических данных в ГБУЗ АО «АМИАЦ»».

Программный продукт написан на языке C# с использованием языка запросов SQL.

Данная информационная система разработана для автоматизированной обработки больших объемов информации о количестве смертей в разрезе по нозологиям, возрасту, месту смерти. Разработанный программный продукт, позволяет работать с данными, загружать базы, редактировать, удалять и сохранять новые данные, формировать дашборды, выводить их на печать и экспортировать в Excel.

Структура программного продукта представлена на рисунке 12.

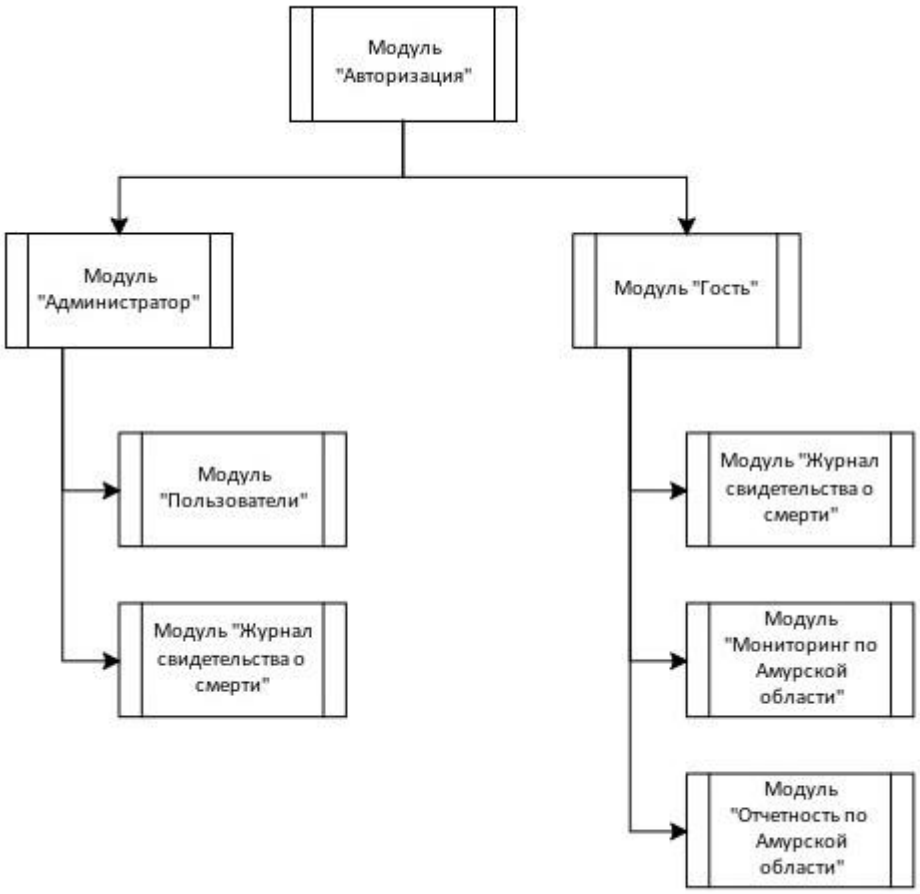

Рисунок 12 – Структура программного продукта

Модуль «Авторизация» (рисунок 13) предназначен для идентификации и аутентификации пользователя, открывается сразу после запуска программного продукта. Пользователь может войти в систему только под своим логином и паролем. Если авторизация прошла успешно, открывается модуль Администратор или Гость.

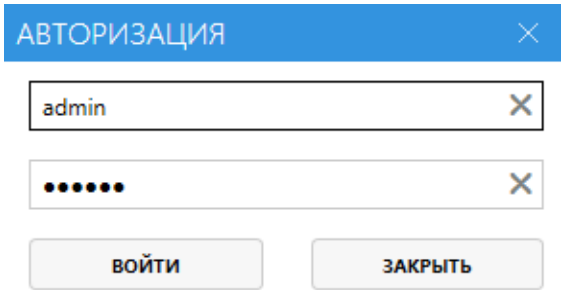

Рисунок 13 – Окно авторизации

Модуль «Администратор» (рисунок 14) предназначен для перехода в модули Журнал «свидетельства о смерти» и пользователи.

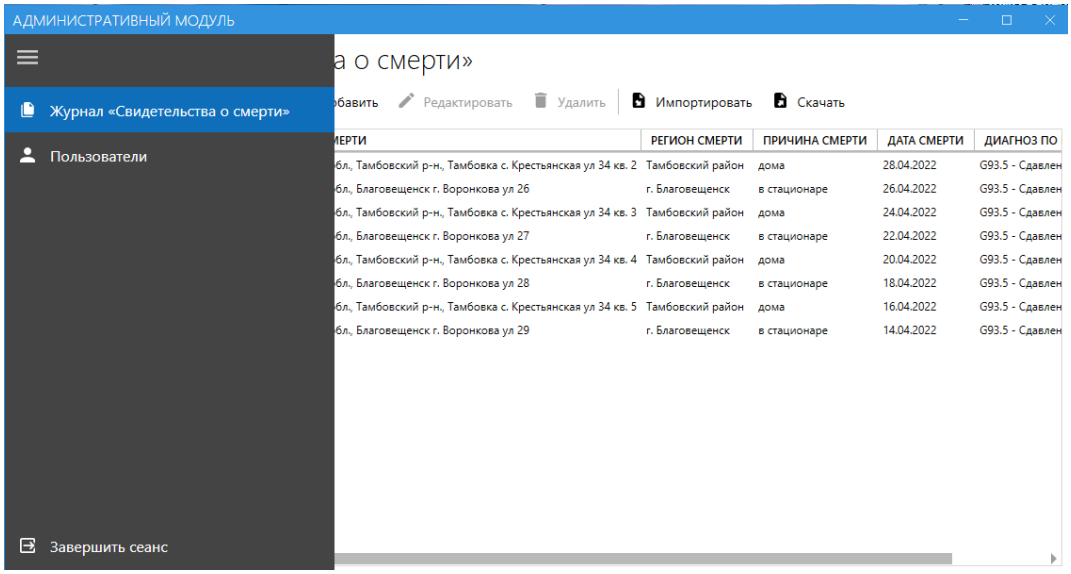

Рисунок 14 – Модуль «Администратор»

При выборе пункта вкладка Журнал «Свидетельства о смерти» появляется окно с информацией об уже выгруженных пациентах (рисунок 15), а так же имеет функцию сброса, фильтрации, добавления, редактирования, удаления, импорта и скачивания файла в формате EXEL.

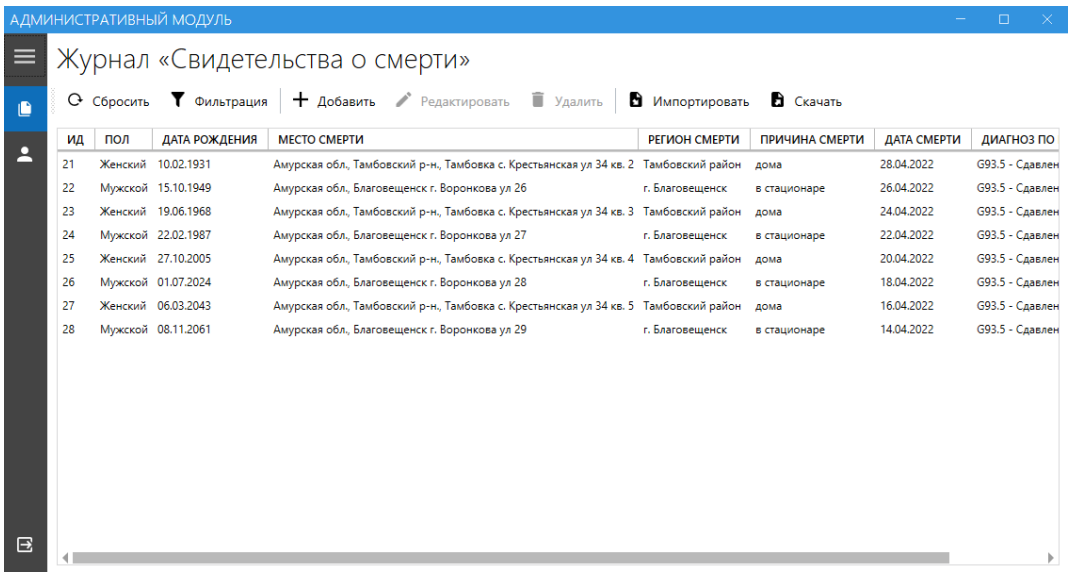

Рисунок 15 – вкладка Журнал «Свидетельства о смерти»

Для добавления пациента вручную необходимы следующие данные (рисунок 16):

– Снилс
– Дата рождения
– Пол
– Дата смерти
– Место смерти
– Причина
– Диагноз по МКБ

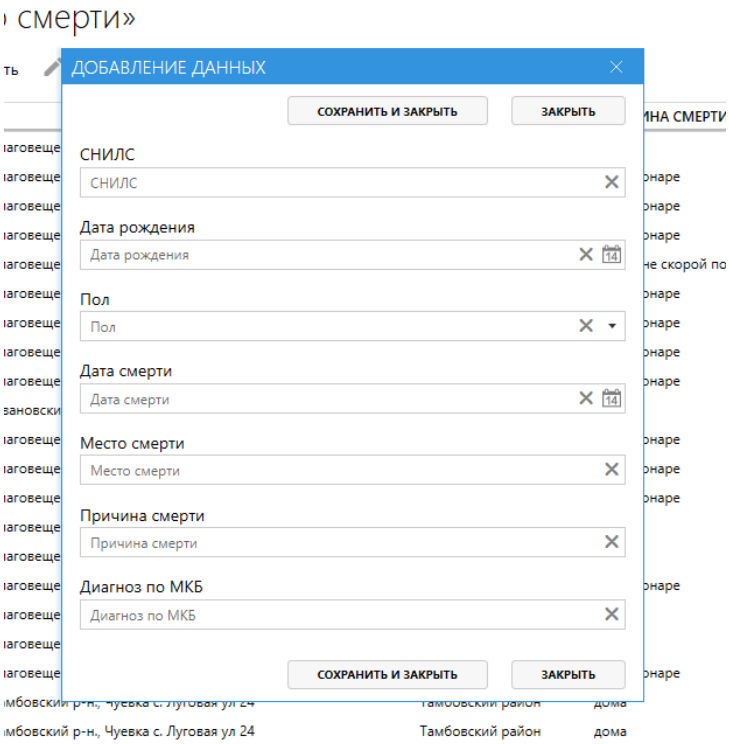

Рисунок 15 – окно «Добавление данных»

Окно импорта таблицы в программу представлено на рисунке 16. В данном окне мы видим количество доступных к импорту строк.

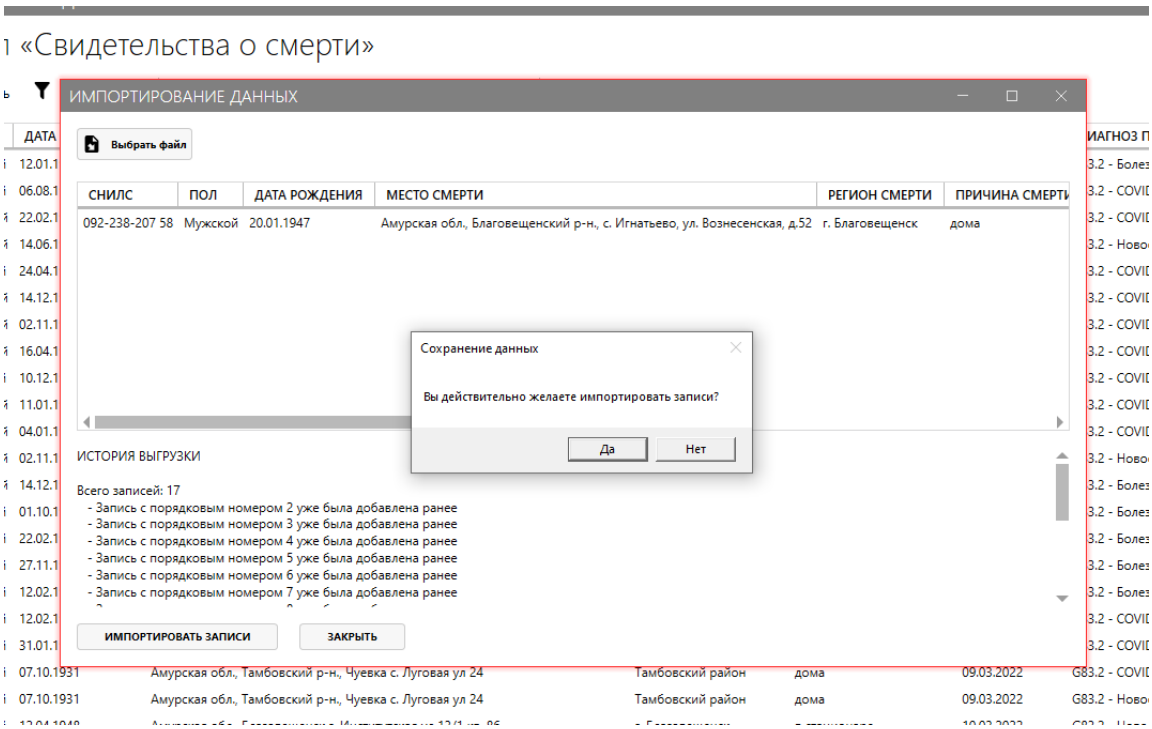

Рисунок 16 – окно «Импорт данных»

При выборе вкладки Пользователи появляется возможность добавить нового пользователя, редактировать ранее добавленных, а так же удалять. Для любого из пользователей выбираются полномочия (рисунок 17).

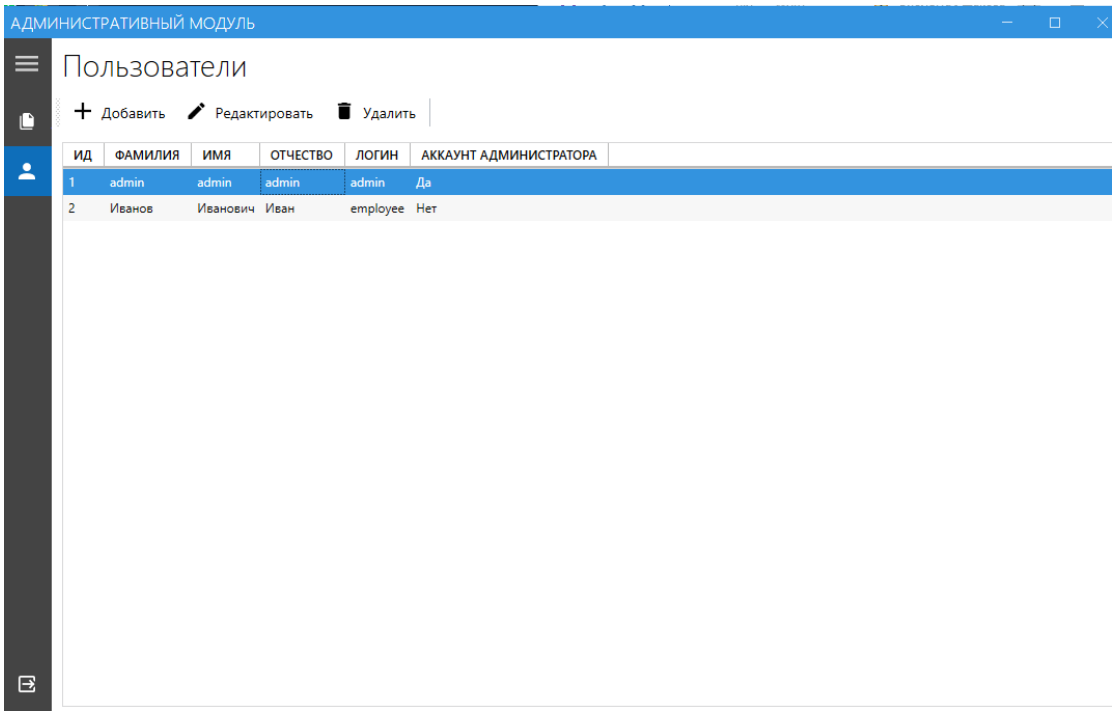

Рисунок 17 – вкладка «Пользователи»

Окно добавления пользователя представлено на рисунке 18. Необходимые данные для регистрации пользователя:

– Фамилия
– Имя
– Отчество
– Логин
– Пароль
– Повтор пароля
– Подтверждение аккаунта администратора

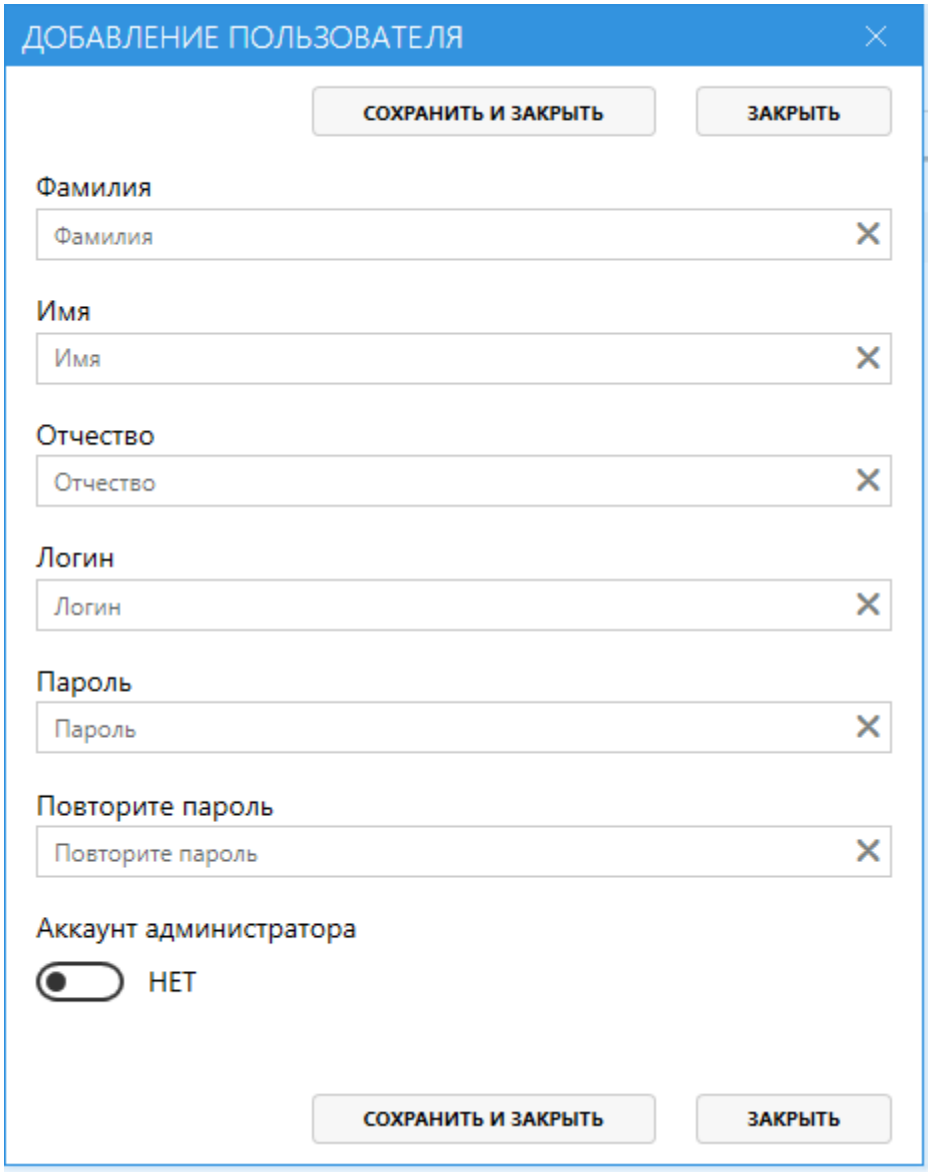

Рисунок 18 – Окно «Добавления пользователя»

Модуль «Мониторинг по Амурской области» (рисунок 19) содержит в себе диаграммы с возможностью выбора за какой период нужны данные, по какому субъекту и от какого диагноза. Диаграммы показывают общую смертность, разделение по полу, по нозологиям, и в разрезе по возрасту.

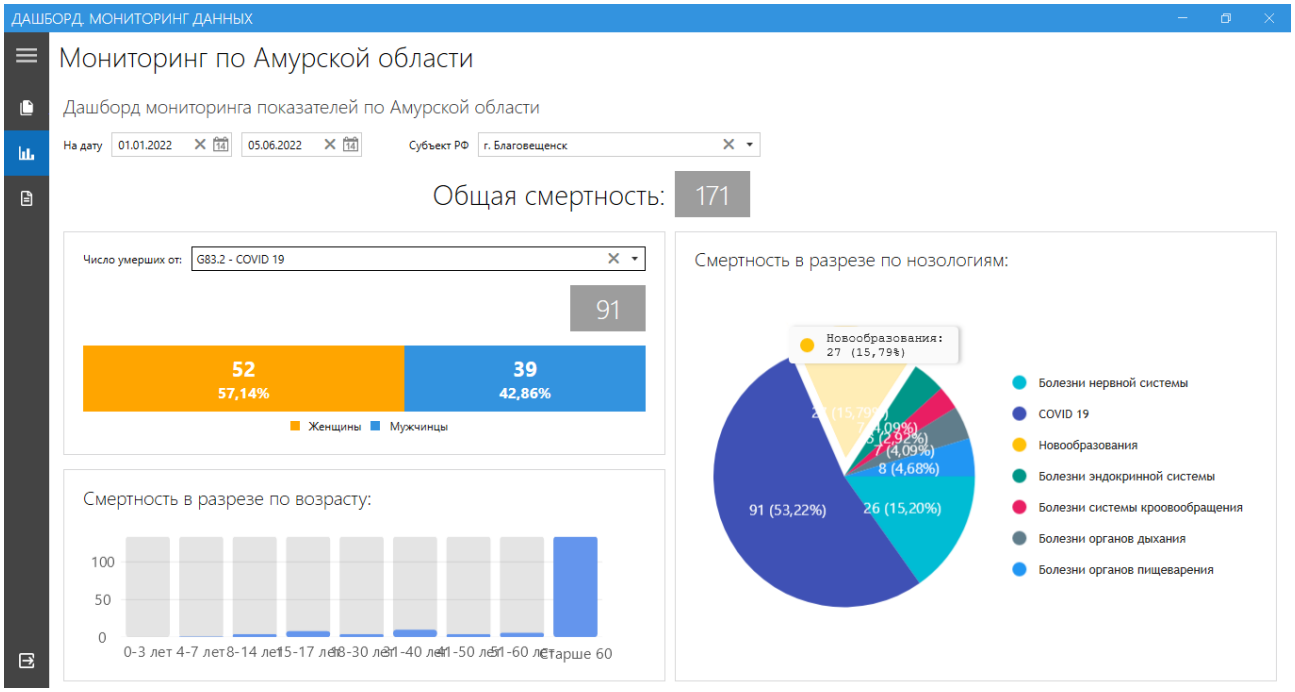

Рисунок 19 – Модуль «Мониторинг по Амурской области»

Модуль «Отчетность по Амурской области» (рисунок 20) содержит в себе диаграммы-отчеты по месяцам в сравнении 2019-2021 года.

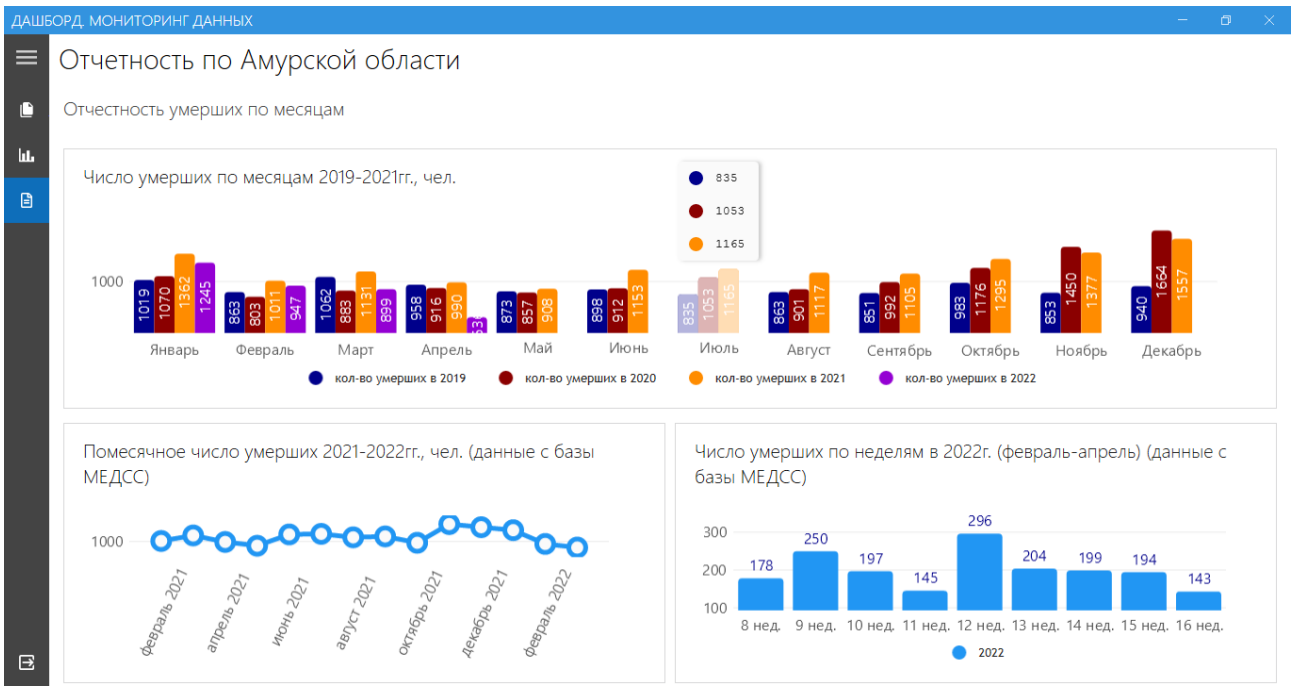

Рисунок 19 – Модуль «Отчетность по Амурской области»

3.2 Защита информации

Приложение хранит в БД данные клиентов, подлежащие защите от возможных утечек, неправомерных изменений и т.д.

3.3 Информация, требующая защиты

Данными, подлежащие защите являются: паспортные данные пациентов, снилс, полис, дата смерти и диагноз.

Защита представленных выше данных производится обезличиванием.

3.4 Модель нарушителя

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным системам либо защищаемой информации.

По признаку принадлежности к ИС все нарушители делятся на две группы:

– внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой

размещается оборудование ИС, внутренними нарушителями могут являться работники разных уровней доступа к данным.

– внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС, внешними являются все остальные лица, взаимодействующие с компанией: клиенты, сторонние организации и тд.

3.5 Угрозы ИБ

Для ИС выделяются следующие основные категории угроз безопасности информации:

- угрозы от утечки по техническим каналам;
- угрозы несанкционированного доступа к информации:

3.6 Мероприятия по защите от угроз ИБ

На основе имеющихся технических и организационных средств защиты информации ГБУЗ АО «АМИАЦ», производится оценка эффективности защиты, при неэффективной защите выявляются все возможные места потери информации в целом, ее достоверности, целостности.

Определятся угрозы, возможные нарушители для компании

Производится расчет ущерба от возможной реализации угрозы и организация защиты по уменьшению экономического ущерба.

Для компании наиболее экономически невыгодной является угроза потери доступа к банковским счетам, документов, подтверждающих право собственности, персональные данные клиентов.

Основная часть данных находится в главном офисе компании на ПК сотрудников, для их защиты необходимо использовать современные ПО для защиты от вирусов, перенос и хранение данных на отдельном сервере в защищенной комнате, организация доступа к серверу, а также компьютерам – терминалам, работающим с данными сервера

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

Вопрос безопасности и защищенности человека в критических и непредвиденных случаях остается одним из важнейших аспектов человеческой жизни.

Безопасность жизнедеятельности (БЖД) как научно-техническая дисциплина изучает опасности, угрожающие человеку в среде обитания, и закономерности их проявления в целях разработки комплексной системы мер по защите человека и среды обитания от опасностей, природных или формируемых в процессе деятельности человека [10].

В данной главе рассмотрим безопасность, экологичность и возможные чрезвычайные ситуации для офисного помещения предприятия ГБУЗ АО «АМИАЦ»

4.1 Безопасность

Безопасность – это такое состояние деятельности, при котором с определенной вероятностью исключаются потенциальные опасности, влияющие на жизнь и здоровье человека. Опасности, создаваемые деятельностью человека, имеют два важных для практики качества: потенциальный характер опасностей, т.е. опасности могут быть, но не приносить вреда, и проявляться при определенных условиях; зона действия опасности ограничена.

БЖД – система знаний, направленных на обеспечение безопасности и сохранение здоровья человека в производственной и непроизводственной среде с учетом влияния человека на среду обитания [10].

4.1.1 Условия труда

В соответствии с Федеральным законом № 197-ФЗ «Трудовой кодекс Российской Федерации» (статья 219) и в соответствии с Федеральным Законом № 181-ФЗ «Об основах охраны труда в Российской Федерации» каждый работник имеет право:

– на рабочее место, соответствующее требованиям охраны труда;

- на получение достоверной информации от работодателя об условиях труда, о риске повреждения здоровья, а также о мерах защиты от воздействия вредных и (или) опасных производственных факторов;
- на отказ от работы в случае опасности для жизни и здоровья из-за нарушения требований охраны труда;
- на обеспечение средствами индивидуальной и коллективной защиты, обучение безопасным приемам труда за счет средств работодателя;
- на запрос о проведении проверки условий труда на рабочем месте органами государственного надзора и контроля;
- на внеочередной медицинский осмотр (обследование) и компенсации, установленные законодательством, коллективным договором (соглашением) и трудовым договором (контрактом), если работник занят на тяжелых работах или работах с вредными и (или) опасными условиями труда.

В ГБУЗ АО «АМИАЦ» производственное оборудование и рабочие столы должны имеют пространство для размещения ног высотой не менее 600 мм, глубиной – не менее 450 мм на уровне колен и 600 мм на уровне стоп, шириной не менее 500 мм. Для пользователей персональных ПК/ноутбуков с жидкокристаллическим или плазменным экраном – размер кабинета составляет не менее 4,5 кв. м.

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

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

Производится ознакомление при приеме на работу с условиями трудового договора, в котором указывают трудовые права работника и информацию об

условиях труда (ст. 57 ТК РФ). На стенах учреждения руководство информирует работников о рисках получения профессиональных заболеваний с помощью визуальной и печатной формы информирования.

В связи с пандемией были с 2020 года были приняты меры, включающие проверку температуры на контрольно-пропускном пункте, ношение масок, соблюдение дистанции, а также обеспечение доступа каждого сотрудника к средствам обработки рук.

Более 90 % рабочего времени сотрудники ГБУЗ АО «АМИАЦ» проводят сидя, что сказывается на их здоровье. Мебель закуплена под средние параметры человека, которая чаще подходит большинству сотрудников.

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

Наибольшая нагрузка на глаза возникает при вводе информации в компьютер, а более сильное общее утомление вызывает работа в режиме диалога. Это усугубляется, если экран монитора небольшой, а плотность изображения высокая.

К работе 1 категории допускаются лица, у которых острота зрения с коррекцией не менее 0,4 хотя бы на одном глазу. Это позволяет без напряжения читать стандартный шрифт с расстояния 60-70 см. При худшем зрении увеличивается размер шрифта.

К работе 2 категории не допускаются лица с глаукомой.

К работе 3 категории предъявляют повышенные требования к органу зрения. Здесь обязательно бинокулярное зрение.

К работам 2 и 3 категории не рекомендуется допускать лиц, страдающих воспалительными и аллергическими заболеваниями глаз, сопровождающимися слезоточением, светобоязнью и т.д., а также заболеваниями сечатки и зрительного нерва.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с ПЭВМ, которые определяются: для группы А – по

суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену; для группы Б – по суммарному числу считываемых или вводимых знаков за рабочую смену, но не более 40 000 знаков за смену; для группы В – по суммарному времени непосредственной работы с ПЭВМ за рабочую смену, но не более 6 ч за смену.

В зависимости от категории трудовой деятельности и уровня нагрузки за рабочую смену при работе с ПЭВМ устанавливается суммарное время регламентированных перерывов, приведенных в таблице 10.

Таблица 9 «Регламентные перерывы»

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

Рабочие столы размещены таким образом, что видео дисплейные терминалы ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

Искусственное освещение в помещениях для эксплуатации ПЭВМ осуществляется системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, применяются системы комбинированного освещения.

Освещенность на поверхности стола в зоне размещения рабочего документа (300-500) лк. Освещение не создает бликов на поверхности экрана. Освещенность поверхности экрана не более 300 лк.

Яркость светильников общего освещения в зоне углов излучения от 50 до 90 градусов с вертикалью в продольной и поперечной плоскостях составляет не более 200 кд/м^2, защитный угол светильников должен не менее 40 градусов.

Требования к микроклимату помещений.

В производственных помещениях, в которых работа с использованием ПЭВМ является основной и связана с нервно-эмоциональным напряжением, должны обеспечиваться оптимальные параметры микроклимата для категории работ 1а и 1б в соответствии с действующими санитарно-эпидемиологическими нормативами микроклимата производственных помещений. На других рабочих местах следует поддерживать параметры микроклимата на допустимом уровне, соответствующем требованиям указанных выше нормативов.

В помещениях, оборудованных ПЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ.

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

Также в офисе предприятия проводится озеленение помещений, которое имеет большое санитарно-гигиеническое и эстетическое значение, т.к. улучшает состав воздуха, снижает температуру в жаркое время года, повышает влажность. Запах, цвет, шелест листьев благоприятно влияют на трудоспособность человека. Во всех кабинетах сотрудников предусмотрены кондиционеры.

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

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

При выполнении работ с использованием ПЭВМ в производственных помещениях уровень вибрации не должен превышать допустимых значений

вибрации для рабочих мест в соответствии с действующими санитарно-эпидемиологическими нормативами.

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

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

Директору ГБУЗ АО «АМИАЦ» следует следить за соблюдением вышеперечисленных факторов, т.к. они влияют на работоспособность сотрудников. Также сотрудникам следует регулярно делать короткие перерывы и выполнять разминку для глаз, спины, шеи и рук.

4.1.2 Организация графического интерфейса

Графический интерфейс разработанной автоматизированной информационной системы для обработки статистических данных в ГБУЗ АО «АМИАЦ» разработана по требованиям эргономики программного обеспечения.

Цель создания эргономичного интерфейса – отобразить информацию настолько эффективно насколько это возможно для человеческого восприятия и структурировать отображение на дисплее таким образом, чтобы привлечь внимание к наиболее важным единицам информации. Основная же цель состоит в том, чтобы минимизировать общую информацию на экране и представить только то, что является необходимым для пользователя.

Разработанный интерфейс интуитивно понятный – работа с системой не должна вызывать у пользователя сложностей в поиске необходимых элементов интерфейса для управления.

Интерфейс непротиворечивый и не избыточный. В окнах «Импорт» и «Редактирование» используются одинаковые приемы работы, в окнах «Мониторинг по Амурской области» и «Отчетность по Амурской области» пользователь видит только минимальную информацию.

В процессе работы система обеспечивает пользователя необходимыми инструкциями. Например, при вводе неправильного логина и пароля, система выводит сообщение об ошибке.

Необходимо учитывать размещение информации на экране.

Количество информации, отображаемой на экране, называется экранной плотностью. Исследования показали, что чем меньше экранная плотность, тем отображаемая информация наиболее доступна и понятна для пользователя и наоборот, если экранная плотность большая, это может вызвать затруднения в усвоении информации и ее ясном понимании.

Разработанный интерфейс является гибким и подходит для пользователей со всеми уровнями подготовки, как новичку, так и опытному пользователю, также в окнах присутствует минимальное количество отображаемой информации, необходимой для работы.

Информация на экране сгруппирована и упорядочена в значимые части, это достигнуто с помощью цветового решения. Информационные элементы расположены таким образом, чтобы зафиксировать внимание пользователя в нужном направлении. Дизайн заголовков и полей выполнен о едином стиле. Заголовки краткие, знакомые и содержательные для пользователя.

4.2 Экологичность

Экология является научной базой охраны окружающей среды. Охрану окружающей среды можно определить как область знаний, разрабатывающую комплекс мероприятий, направленных на поддержание рационального взаимодействия между деятельностью человека и окружающей природной средой, обеспечивающих сохранение, восстановление природных богатств, рациональное использование природных ресурсов, предупреждающих вредное влияние результатов хозяйственной деятельности общества на природу и здоровье человека.

Разработанный программный продукт не оказывает влияния на окружающую среду, но это влияние оказывает техническое оборудование – ПК и МФУ, которое используется при работе с программным продуктом.

В случае выхода из рабочего состояния ПК или МФУ, если нет возможности устранить неполадки и продолжить использование оборудования, их необходимо утилизировать.

Старую технику нельзя считать обычным мусором, потому что в составе ее компонентов находятся вредные вещества – отходы высоких классов опасности, которые вредят здоровью и экологии.

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

За отказ от утилизации, соответственно, предумышленное загрязнение окружающей среды, предусмотрена административная ответственность и наложение на предприятие крупных штрафных санкций.

В ГБУЗ АО «АМИАЦ»:

– Юридические лица должны предварительно списать сломанную технику с баланса предприятия. Для списания необходимо точно определить остаточную ценность оргтехники и получить заключение о непригодности оргтехники к использованию. Такое заключение выдается только на основании экспертизы.

– Поиск компании в Амурской области, которая занимается непосредственной утилизации техники. Заключение договора с исполнителем.

– Вывоз оргтехники с предприятия.

– Исполнитель демонтирует, сортирует технику. Отделяет черный металл от цветного и драгметаллов. Полученное сырье отправляется на заводы для переработки. В дальнейшем из них будут сделаны новые продукты. Отходы классов повышенной опасности обезвреживаются и уничтожаются, либо их отвозят на легальные места захоронения.

Очень важно досконально проверить правильность документации об утилизации техники. В противном случае может оказаться, что работа не была

произведена по всем правилам, что грозит серьезными штрафными санкциями для юридических лиц.

На предприятии ведется журнал учета количества эксплуатируемых, замененных и утилизированных светильников. Не работающие люминесцентные лампы – источник загрязняющих веществ, и должны утилизироваться безопасными способами.

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

4.3 Чрезвычайные ситуации

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

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

Пожаром называют неконтролируемое горение, развивающееся во времени и пространстве, опасное для людей и наносящее материальный ущерб. Под пожарной и взрывной безопасностью понимают систему организационных и технических средств, направленную на профилактику и ликвидацию пожаров и взрывов.

Источниками возгорания могут служить случайные искры различного происхождения, нагретые тела, перегрев электрических контактов и др.

Основные причины пожаров на производстве – нарушение технологического режима работы оборудования, неисправность электрооборудования, плохая подготовка оборудования к ремонту, самовозгорание различных материалов, несоблюдение работниками правил пожарной безопасности, захламление помещений и др.

Чаще всего пожар возникает по вине человека из-за несоблюдения правил пожарной безопасности и неосторожного обращения с огнем.

Для защиты от пожара в здании офиса предприятия имеются противопожарные преграды (стены, перегородки, двери, окна и др.), т.е. конструкции с нормируемым пределом огнестойкости, препятствующие распространению огня из одной части здания в другую.

Также предусмотрен путь эвакуации сотрудников, т.е. путь, ведущий к эвакуационному выходу на случай возникновения пожара.

Для тушения пожара используют огнегасительные вещества, которые при введении в зону сгорания прекращают горение. Основные огнегасящие вещества и материалы – вода и водяной пар, химическая и воздушно-механическая пены, водные растворы солей, негорючие газы, сухие огнетушащие порошки. Наиболее распространенным веществом, применяемым для тушения пожара, является вода. Под первичными средствами пожаротушения понимают передвижные и ручные огнетушители, переносные огнегасительные установки, внутренние пожарные краны, ящики с песком, асбестовые покрывала, противопожарные щиты с набором инвентаря и др. [14].

В офисе организации имеются такие средства пожаротушения, как ручные углекислотные огнетушители, также установлена система автоматического пожаротушения, пожарные датчики и пожарная кнопка, также размещены схемы путей эвакуации. Все сотрудники прошли инструктаж по технике безопасности и поставили подпись в журнале по технике безопасности.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы был проведен анализ предметной области, построена организационная структура предприятия ГБУЗ АО «АМИАЦ», построены диаграммы внешнего и внутреннего документооборота.

Выполнен анализ программного и аппаратного обеспечения, используемого на предприятии.

Приведена характеристика функциональных и обеспечивающих подсистем, выбраны средства разработки.

Проведен анализ безопасности и экологичности предприятия и разработанного продукта.

Спроектирована база данных. В ходе инфологического проектирования построена диаграмма, отражающая связи между сущностями. Разработаны и построены логическая и физическая модели базы данных.

Главным результатом выполнения работы стала структура БД, разработанная в Microsoft SQL Server 2017 и программный продукт, разработанный в Visual Studio 2017 на языке C# для предприятия ГБУЗ АО «АМИАЦ»

Созданная автоматизированная информационная система позволяет просматривать и обрабатывать данные, автоматизировать деятельность предприятия по обработке статистических данных.

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

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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

2 Баженова, И. Ю. SQL и процедурно-ориентированные языки / И. Ю. Баженова. – 2-е изд. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 166 с.

3 Башлы, П. Н. Информационная безопасность и защита информации. Учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – М.: Евразийский открытый институт, 2012. – 311 с.

4 Документация по SQL Server [Электронный ресурс] – Режим доступа: https://docs.microsoft.com/ru-ru/sql/sql-server. – 01.03.2021.

5 Документация по Visual Studio [Электронный ресурс] – Режим доступа: https://docs.microsoft.com/ru-ru/visualstudio. – 02.03.2021.

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

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

8 Молдованова, О. В. Информационные системы и базы данных. Учебное пособие / О. В. Молдованова. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2014. – 178 с.

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

10 Основы информационной безопасности. Идентификация и аутентификация, управление доступом [Электронный ресурс] – Режим доступа: http:// citforum.ru/security/articles/galatenko/. – 24.05.2021.

11 Полякова, Л. Н. Основы SQL. Учебное пособие / Л. Н. Полякова. – 3-е изд. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 273 с.

12 Порядок утилизации старой оргтехники на предприятии [Электронный ресурс] – Режим доступа: https:// stop-othod. ru / recycling/ utilizaciya-orgtekhniki. html. – 03.06.2021.

13 Разработка приложений на C# в среде Visual Studio. Учебное пособие / А. М. Нужный [и др.]. – Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2019. – 89 с.

14 Руководство по программированию на C# [Электронный ресурс] – Режим доступа: https://docs.microsoft.com/ru-ru/dotnet/csharp/programming-guide. – 02.03.2021.

15 Руководство по программному пакету AllFusion Erwin Data Modeler [Электронный ресурс] – Режим доступа: http://emanual.ru/download/ www. eManual. ru_510.html. – 02.03.2021.

16 Руководство по программному пакету AllFusion Process Modeler [Электронный ресурс] – Режим доступа: https://itteach.ru/bpwin/. – 03.03.2021.

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

18 Стасышин, В. М. Разработка информационных систем и баз данных. Учебное пособие / В. М. Стасышин. – Саратов: Профобразование, 2020. – 100 с.

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

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

21 Шумилин, В. К. ПЭВМ. Защита пользователя / Шумилин В. К. – М.: Охрана труда и социальное страхование, 2015. – 214с.

22 Эргономика программного обеспечения [Электронный ресурс] – Режим доступа: https://studwood.ru/ 1589590/ informatika/ ergonomika_ programmno go_obespecheniya. – 03.06.2021.

ПРИЛОЖЕНИЕ А
Техническое задание

1 Введение

1.1 Наименование разрабатываемой системы: «Разработка автоматизированной информационной системы для обработки статистических данных в ГБУЗ АО «АМИАЦ»».

1.2 Краткая характеристика области применения

Автоматизированная информационная система разрабатывается для предприятия ГБУЗ АО «АМИАЦ», офис расположен по адресу город Благовещенск, ул.Воронкова 26. Юридический адрес: 675000, Амурская область, г. Благовещенск, ул. Воронкова, д.26.

Медицинский информационно-аналитический центр выступает центральным звеном в организации сбора, обработки информации и показателей медицинской статистики, медико-демографической, финансовой, кадровой составляющих здравоохранения Амурской области. Разработанная система выполнена в учебных целях и предназначена, в первую очередь, для отдела мониторинга показателей здоровья населения Амурской области.

2 Основание для разработки

2.1 Разработка ведётся на основе устава организации, документов и различных отчетов организации.

Дата начала разработки – апрель 2021 года.

Дата утверждения технического задания – 10 апреля 2021 года.

2.2 Наименование темы разработки «Разработка автоматизированной информационной системы для обработки статистических данных в ГБУЗ АО «АМИАЦ»».

Продолжение ПРИЛОЖЕНИЯ А

3 Назначение разработки

Разрабатываемая система хранит данные о пациентах, и производит статистическую обработку информации. Разрабатываемая система направлена на уменьшение избыточности информации и времени на обработку данных по учету заказов.

Администратор вносит данные в ручном или табличном виде , добавляет новых пользователей и редактирует полномочия уже имеющихся.

Врач-статистик имеет доступ уже к готовым диаграммам и дашбордам, где имеет возможность выбрать период, диагноз, район, возраст и нозологию по которой необходим отчет, который можно скачать в формате Exel.

4 Требования к программе или программному изделию

4.1 Требования к функциональным характеристикам

Все данные должны находиться в одной базе.

Система должна обеспечивать ввод новых данных, просмотр и изменение уже имеющихся в базе. Для изменения или обработки данных необходимо разработать соответствующие запросы на языке SQL.

Входными данными являются данные пациентах, в которые входит дата рождения, пол, дата смерти, диагноз, дата и место смерти.

Выходные данные – дашборды мониторинга с функцией выбора периода, региона, и диагноза. Результаты обработки данных выводятся в формате Excel с обезличенными персональными данными.

4.2 Требования к надежности

Разработанная система должна отвечать требованиям надежности – иметь защиту от некорректных действий пользователей.

Для надежности функционирования системы и исключения ошибок персонала при вводе для каждого атрибута определён тип данных, предусмотрен автоматический ввод идентификатора. Для обязательных полей запрещено

значение NULL, для обновления информации в базе необходимо заполнить все обязательные поля. На восстановление отказа нужно несколько секунд времени, восстанавливает исправное функционирование пользователь самостоятельно, заполнив обязательные поля или удалив некорректно внесенные данные.

4.3 Требования к условиям эксплуатации

Система должна быть рассчитана на эксплуатацию в составе программно-технического комплекса Заказчика.

Для обслуживания необходим один администратор, обладающий высокими навыками владения ПК, имеющий опыт работы с базами банных и Microsoft SQL Server.

Количество персонала, работающего с разработанной информационной системой, не ограничено. Пользователь должен иметь навыки работы с ПЭВМ, быть уверенным пользователем.

Необходимый состав технических средств: персональный компьютер, источник бесперебойного питания для обеспечения устойчивой работы оборудования при сбоях в сети электропитания, локальная сеть.

Требуемые технические характеристики ПК:

– Процессор Intel, 64-разрядный;

– Оперативная память не менее 2 Гбайт;

– Монитор с расширением от 800x600 пикселей;

– Версия Windows от 8;

– Свободное место на жёстком диске не менее 6 Гбайт.

Требования к совместимости: система должна быть совместима с Microsoft SQL Server (версия не ранее 2017 года), установленного на сервере Заказчика.

4.4 Требования к маркировке и упаковке

Требования к маркировке и упаковке не предъявляются.

Заказчик должен обеспечить размещение БД на сервере и установку программного продукта на ПК пользователей, размещённых в соответствии с санитарными нормами и требованиями к пожарной безопасности, и исключить возможность бесконтрольного доступа и проникновения к ПК посредством установления парольной защиты на ПК и сервер.

5 Требования к программной документации

Состав программной документации согласовывается с Заказчиком. Заказчику предоставляется руководство пользователя и техническое задание по ГОСТ 19.102-78.

6 Технико-экономические показатели

6.1 Экономическая эффективность от внедрения

6.2 Предполагаемая годовая потребность

Годовая потребность составит 250 рабочих дней при условии использования разработанного модуля ежедневно при пятидневной рабочей неделе.

6.3 Экономические преимущества разработки по сравнению с аналогами

По сравнению с аналогами разработанная автоматизированная информационная система является бесплатной для установки и использования и разрабатывается в соответствии с требованиями Заказчика.

7 Стадии и этапы разработки

Разработка автоматизированной информационной системы включает следующие стадии:

– Составление технического задания для выяснения требований Заказчика к разрабатываемой системе;

– Эскизный проект. Проводится анализ предметной области, документооборота и деятельности предприятия. По окончании этапа будут разработаны диаграммы внутреннего и внешнего документооборота, диаграммы деятельности;

– Технический проект. Выполняется проектирование концептуальной, логической и физической модели базы данных. По окончании этапа будут разработаны концептуально-инфологическая модель БД, логическая и физическая модели;

– Рабочий проект. Создается структура базы данных на языке SQL и программный продукт. Проводится тестирование разработанного программного продукта. По окончании этапа будут разработаны база данных, программный продукт и руководство пользователя.

Сроки разработки с апреля по июнь 2021 года.

Исполнитель: студент группы 855-об Амурского государственного университета Ушакова Виолетта Алексеевна.

8 Порядок контроля и приемки

Сдача разработанной информационной системы предприятия производится в соответствии с календарным планом.

При приёмке Заказчик проверяет соответствие разработанной системы техническому заданию в присутствии Исполнителя.

При приёмке Заказчик ознакамливается с руководством пользователя.

Производятся следующие виды испытаний:

– запуск разработанного программного продукта;

– авторизация пользователя;

– ввод новых данных в таблицы БД;

– изменение и удаление данных в базе;

– проверка правильности работы запросов;

– ввод данных о новом заказе;

– ввод данных о доставке.

ПРИЛОЖЕНИЕ Б
Концепция ИБ предприятия

1 Общие положения

1.1 Назначение концепции по обеспечению информационной безопасности

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению ИБ в, а также нормативных и методических документов, обеспечивающих её реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности информации;

– принятия управленческих решений и разработки практических мер по воплощению политики безопасности, и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз;

– координации деятельности структурных подразделений при проведении работ по развитию и эксплуатации ИС с соблюдением требований обеспечения безопасности информации;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности в ИС.

Основной целью создания СЗПДн является минимизация ущерба от возможной реализации угроз безопасности информации.

1.1 Цели системы информационной безопасности

Основными целями обеспечения информационной безопасности являются:

− предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию;

− повышение качества оказания населению государственных и муниципальных услуг в электронном виде в сфере здравоохранения;

− повышение эффективности использования современных информационных технологий;

− соответствие применяемых мер защиты информации действующему законодательству Российской Федерации, нормативным и методическим документам уполномоченных органов

1.2 Задачи системы информационной безопасности

Задачами деятельности по обеспечению информационной безопасности являются:

– формирование и проведение единой политики в области обеспечения защиты информации в АМИАЦ;

– формирование единых требований к АРМ пользователей ЕМИСЗ РК;

– координация деятельности МО при разработке организационно-распорядительной документации по защите информации, содержащейся в АМИАЦ.

– поддержание системы информационной безопасности в состоянии, устойчивом к существующим и вновь выявляемым угрозам в информационной сфере;

– разработка и внедрение в информационную инфраструктуру МО современных методов и средств обеспечения информационной безопасности;

– организация контроля состояния и оценки эффективности системы информационной безопасности и реализация мер по её совершенствованию.

2. Проблемная ситуация в сфере информационной безопасности.

2.1 Объекты информационной безопасности

Объектами защиты в ГБУЗ АО «АМИАЦ» являются:

– обрабатываемая информация;

– программные, технические и программно-технические средства обработки информации;

– средства защиты информации;

– средства и системы связи и передачи данных;

– общесистемное, прикладное, специальное программное обеспечение

2.2 Определение вероятного нарушителя

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным системам либо защищаемой информации.

По признаку принадлежности к ИС все нарушители делятся на две группы:

– внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС;

– внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

2.3 Описание особенностей (профиля) каждой из групп вероятных нарушителей

Внутренними нарушителями могут являться работники разных уровней доступа к данным, внешними являются все остальные лица, взаимодействующие с учреждением: посетители, сторонние организации и тд.

2.4 Основные виды угроз информационной безопасности Предприятия

Для ИС выделяются следующие основные категории угроз безопасности информации:

– угрозы от утечки по техническим канала;

– угрозы несанкционированного доступа к информации:

– угрозы уничтожения, хищения аппаратных средств ИС, носителей информации путем физического доступа к элементам ИС;

– угрозы хищения, несанкционированной модификации или блокирования информации за счёт НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

– угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИС;

– угрозы в результате сбоев ПО, а также угрозы неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

– угрозы преднамеренных действий внутренних нарушителей;

– угрозы НСД по каналам связи.

2.5 Оценка потенциального ущерба от реализации угрозы

Потенциальный ущерб определяется как общий эффект воздействия на учреждение в связи с хищением информации, внедрения вредоносных ПО, диверсией, связанной с изменением информации и тд.

Продолжение ПРИЛОЖЕНИЯ Б

3 Механизмы обеспечения информационной безопасности предприятия

3.1 Принципы, условия и требования к организации и функционированию системы информационной безопасности

Построение системы обеспечения безопасности информации ИС в и её функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;

3.2 Основные направления политики в сфере информационной безопасности

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИС, использование ресурсов ИС, деятельность сотрудников и сторонних организаций, а также порядок взаимодействия пользователей с ИС таким образом,

чтобы в наибольшей степени затруднить или исключить возможность реализации угроз ИБ или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ИС, отражающую подходы к защите информации, и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности в ИС состоит из мер административного уровня и организационных (процедурных) мер защиты информации. К административному уровню относятся решения руководства, затрагивающие деятельность ИС в целом.

Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

– принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности информации, определение ответственных за её реализацию;

– принятие решений по вопросам реализации программы безопасности;

– обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

4 Мероприятия по реализации информационной безопасности предприятия

4.1 Организационное обеспечение информационной безопасности

Мероприятия по обеспечению информационной безопасности ГБУЗ АО «АМИАЦ» должны носить упреждающий характер и быть направлены на предотвращение инцидентов, реализующих угрозы безопасности информации.

При выборе мер защиты информации, обрабатываемой с применением средств автоматизации необходимо определить актуальные угрозы для данной

ИС, тип обрабатываемых данных, тип самой ИС, её класс защищённости и иные параметры, определяемые действующим законодательством в качестве основополагающих при выборе правил и мер защиты информации.

В целях нейтрализации угроз безопасности информации применяются организационные и технические меры защиты информации.

Организационные меры обеспечения информационной безопасности предусматривают:

- назначение ответственных за организацию обработки ПДн, за обеспечение безопасности информационной системы, за техническое обслуживание информационной системы, за проведение мероприятий по обезличиванию обрабатываемых ПДн, за хранение материальных носителей информации;
- ознакомление сотрудников с законодательством и внутренними документами МЗ в области информационной безопасности;
- обучение сотрудников, непосредственно осуществляющих обработку ПДн, правилам безопасной работы с персональными данными;
- повышение квалификации специалистов по защите информации и лиц, ответственных за организацию защиты информации;
- назначение ответственности сотрудников и руководителей всех уровней за выполнение установленных требований по защите информации;
- проведение контроля соблюдения сотрудниками требований по обеспечению информационной безопасности;
- обезличивание ПДн в случаях, когда не требуется определение субъекта персональных данных;
- прием и обработку обращений и запросов субъектов ПДн или их представителей;
- установление уровней защищенности ПДн в ИСПДн;
- установление класса защищенности ГИС;

- оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей по защите ПДн;
- уведомление уполномоченного органа по защите прав субъектов ПДн (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) о начале обработки ПДн в соответствии со ст.22 Федерального закона № 152-ФЗ;
- выявление угроз безопасности и разработку моделей угроз и нарушителя;
- управление доступом сотрудников к информационной системе;
- назначение минимально необходимых прав и привилегий пользователям;
- регистрацию всех действий пользователей;
- обучение пользователей и персонала, обслуживающего системы защиты информации, правилам и способам работы с подсистемой информационной безопасности;
- учет машинных носителей информации;
- применение средств защиты информации, прошедших обязательный контроль соответствия требованиям нормативных документов по защите информации;
- мероприятия по обеспечению физической безопасности средств вычислительной техники и материальных носителей информации;
- оценку эффективности реализованных мер по обеспечению безопасности ПДн (аттестация АМИАЦ и ее сегментов по требованиям безопасности информации);
- унификацию и стандартизацию средств защиты информации;

− проведение анализа эффективности и достаточности принятых мер по защите информации;

− разработку и реализацию предложений по совершенствованию систем защиты информации;

− выявление незарегистрированных технических устройств и программного обеспечения, в том числе имеющего признаки контрафактности;

− противодействие перехвату информации в каналах связи;

− организацию безопасного доступа к ресурсам сети Интернет;

− резервирование информации и ее восстановление в случае возникновения инцидентов безопасности информации;

− обеспечение гарантированной доступности информационных ресурсов информационных систем с помощью:

− резервирования оборудования и каналов связи;

− балансировки нагрузки на сервера и каналы связи;

− обеспечения гарантированного электропитания;

− контроль, в том числе с использованием программных технических средств, за действиями пользователей и реакцию на нарушение установленных мер защиты.

4.2 Техническое обеспечение информационной безопасности Предприятия

Технические меры обеспечения безопасности ПДн включают использование средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации и шифровальных (криптографических) средств защиты информации и должны решать следующие задачи:

- Предотвращение несанкционированного доступа;

- Возможность быстрого восстановления данных, утерянных или модифицированных;

- Введение в использование новейших средств защиты ПО;
- Техническая защита от перехвата данных.

4.3 Правовое обеспечение информационной безопасности Предприятия

Деятельность по обеспечению информационной безопасности, должна осуществляться в рамках действующего законодательства, руководящих документов уполномоченных государственных органов исполнительной власти, рекомендаций Министерства здравоохранения РФ, ведомственных документов МЗ и настоящей Концепции.

В части организации обработки и защиты персональных данных следует руководствоваться следующими документами:

– Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;

– Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства РФ №1119);

– Постановление Правительства РФ от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных

данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановление Правительства РФ от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальным органами»;

– Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008, утвержденная ФСТЭК РФ.