Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

Факультет (институт) информационных технологий
Кафедра информатика, вычислительная техника и информационная безопасность
Направление Информационная безопасность
Направленность (профиль) Организация и технология защиты информации

УДК 004.77

УТВЕРЖДАЮ
Заведующий кафедрой ИВТиИБ
А.Г. Якунин
“____”_____2020 г.

# БАКАЛАВРСКАЯ РАБОТА

**БР 10.03.01.04.000 ПЗ**
обозначение документа

«Проектирование защищенного комплекса средств автоматизации приема вызовов скорой медицинской помощи»
*тема бакалаврской работы*

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Студент группы ИБ-62 Липатов Владимир Алексеевич
*фамилия, имя, отчество*

Руководитель работы ст.преп. А.В. Циклаков
*должность, ученая степень* *инициалы, фамилия*

Барнаул 2020 г.

## Реферат

Бакалаврская работа посвящена созданию защищенной виртуальной частной сети на основе программно-аппаратного комплекса ViPNet и ОС Astra Linux.

В бакалаврской работе была разработана и внедрена защищенная виртуальная частная сеть на предприятии, позволяющая осуществлять безопасный обмен информацией между удаленными офисами и филиалами. Реализованы анализ обрабатываемой информации, подбор необходимых средств защиты, их установка и настройка для дальнейшей работы.

Ключевые слова – виртуальная частная сеть, безопасный обмен данными, программно-аппаратные средства защиты.

Бакалаврская работа содержит 70 страниц, 9 рисунков, 1 приложение.

## The abstract

The bachelor's work is devoted to creating a secure virtual private network based on the ViPNet software and hardware complex and the Astra Linux OS.

In the bachelor's work, a secure virtual private network was developed and implemented at the enterprise, allowing for secure exchange of information between remote offices and branches. Implemented analysis of the processed information, selection of necessary security tools, their installation and configuration for further work.

Keywords - virtual private network, secure data exchange, software and hardware protection.

The work contains 70 pages, 9 drawings, 1 apposition.

**Содержание**

Введение....4
1 Описание исследуемого объекта....6
1.1 Анализ функционального процесса....6
1.2 Анализ архитектуры автоматизированной системы....9
1.3 Информация, подлежащая защите, определение источников информации..14
2 Проектирование системы информационной безопасности....18
2.1 Анализ требований к автоматизированным системам....18
2.2 Модели угроз и возможных нарушителей....23
2.3 Состав и оценка эффективности проектируемой системы информационной безопасности....27
3Разработка защищенного комплекса....32
3.1 Структурно-функциональная схема проекта....32
3.2 Выбор целесообразных программно-технических средств и организационных мероприятий....39
3.2.1 Выбор общего программного обеспечения....39
3.2.2 Выбор программных средств виртуализации....43
3.2.3 Выбор средств доверенной загрузки для защиты средств вычислительной техники от несанкционированного доступа....46
3.2.4 Выбор сетевых экранов....48
3.2.5 Выбор средств обнаружения вторжений....49
3.3Функциональная оценка эффективности подсистемы компьютерной безопасности....51
3.4 Расчет технико-экономических показателей....55
3.4.1 Расчёт расходов на оборудование....56
3.4.2 Расчёт расходов на программное обеспечение....57
Заключение....58
Список использованных источников....59

# Введение

Создать идеальную систему защиты информации невозможно, но возможно отдалить во времени негативное событие, а также подготовиться к нему. Для предотвращения инцидента в ближайшей перспективе, либо подготовки к устранению его последствий нужны не только специалисты, но и ресурсы.

Быстрое развитие информационных технологий способствует появлению новых угроз и уязвимостей. В то же время уже зарекомендовавшие себя векторы атак используются более активно злоумышленниками. Проблемы и задачи в сфере информационной безопасности настолько глубоки и разнообразны, что требуют непрерывной подготовки специалистов высокого уровня.

Да и имеющиеся ресурсы для обеспечения информационной безопасности, либо ликвидации последствий далеко не безграничны. Желательно, чтобы руководство в сфере информационной безопасности уже с первого раза принимало верное решение, так как последствия от ошибочного или недальновидного решения могут быть критическими для организации, вплоть до её закрытия.

Актуальность выполненной работы в условиях угроз информационной безопасности высока.

При написании данной работы были использованы научная и учебно-методическая литература, стандарты в области защиты информации и информационных технологиях. Основными источниками, раскрывающими теоретические основы обеспечения комплексной защиты информации, являлись работы Астахова А. М., Баранова Е. К., Бирюкова А. А., Гришина Н.В., Денисова Ю., Лушникова Н. Д., Эпельфельда И. И. В данных источниках подробно рассмотрено понятие угроз информационной безопасности, а также информационных рисков организации.

Научная новизна работы заключается в обоснованном и оптимальном выборе современных средств защиты, а также в выработке организационных мер

для обеспечения информационной безопасности, соответствующих нормативной базе ФСТЭК России.

Объектом выполненной работы является центр обработки вызовов скорой помощи в с. Майма Республики Алтай.

Предметом выпускной квалификационной работы является обеспечение информационной безопасности средств автоматизации приема вызовов скорой медицинской помощи.

Целью данной работы является разработка проекта защищенного комплекса средств автоматизации приема вызовов скорой медицинской помощи.

Задачами выполненной работы являются:

– анализ функционального процесса;

– анализ архитектуры автоматизированной системы;

– определение источников информации, подлежащих защите;

– построение модели угроз и возможных нарушителей;

– проведение оценки эффективности проектируемой системы защиты информации;

– построение структурно-функциональной схемы проекта;

– выбор программно-аппаратных средств защиты и организационных мероприятий;

– функциональная оценка эффективности разработанной системы защиты информации.

Практическая значимость заключается в возможности применения выбранных средств защиты для создания объекта, отвечающего требованиям безопасности ФСТЭК России.

# 1 Описание исследуемого объекта

В данном разделе работы отражены сведения исследуемого объекта выполненной работы центра обработки вызовов скорой медицинской помощи в с. Майма Республики Алтай, раскрывающие структуру и анализ функционального процесса, архитектуры автоматизированной системы обработки вызовов. Обобщены и показаны источники информации, подлежащей защите.

## 1.1 Анализ функционального процесса

Система вызова скорой медицинской помощи заключается в виде деятельности дежурного персонала медицинской службы, действующего на территории Республики Алтай и обеспечивающего прием вызовов и направление бригад скорой медицинской помощи пострадавшим.

Прием вызовов скорой медицинской помощи осуществляется центрами обработки вызовов (далее – ЦОВ), которые создаются на базе дежурных диспетчерских служб (далее – ДДС) муниципальных образований.

В центре обработки вызовов скорой медицинской помощи циркулирует два типа информации:

– оперативная информация, к которой относятся данные о вызовах, сообщениях, происшествиях (обращения граждан с просьбой об оказании необходимой помощи; сообщения о происшествиях и чрезвычайных ситуациях; данные о ходе реагирования на принятый вызов (сообщение о происшествии); данные по управлению (контроль состояния) силами и средствами; данные об изменении режима функционирования ЦОВ и ДДС; данные о развитии обстановки при происшествиях и чрезвычайных ситуациях и о ходе работ по их ликвидации; данные о результатах реагирования на происшествия; данные о

действиях персонала скорой помощи медицинской службы при приеме сообщения о происшествии и реагировании на происшествия);

– текущая информация, представляющая обобщённые данные о вызовах, происшествиях и основных результатах реагирования на них (данные о результатах ликвидации происшествий и материальном ущербе; обобщённые данные о функционировании систем; данные о состоянии сил и средств; данные о состоянии и работоспособности программно-технических средств центра обработки вызовов.

В случае заведомо ложного вызова заявитель несёт ответственность в соответствии с действующим законодательством Российской Федерации.

С операторами ЦОВ скорой медицинской помощи взаимодействуют пользователи сетей фиксированной телефонной связи, подвижной радиотелефонной связи, комплексы взаимодействующих сигнальных систем.

Приём вызовов, являющихся сообщениями о происшествии, осуществляется операторами ЦОВ, которые вводят в базу данных информацию о происшествии, которая проходит процесс регистрации, анализа, и в зависимости от специфики происшествия к работе подключается диспетчер (фельдшер, радиотелефонист, дежурный и пр.) скорой медицинской службы.

Обобщенная схема процесса приема и обработки вызова скорой медицинской службы представлена на рисунке 1.




Рисунок 1 – Обобщенная схема процесса приема и обработки вызова скорой медицинской помощи

При поступлении вызова скорой медицинской службы:

1) дежурный оператор обязан осуществить прием вызова;

2) при наличии признаков чрезвычайной ситуации соединить с позвонившим лицом старшего оператора смены;

3) старший оператор смены обязан выполнить план мероприятий по оповещению соответствующих должностных лиц.

Если в момент поступления вызова все операторы заняты, вызов переходит в очередь на ожидание. Первый освободившийся оператор начинает приём и обработку вызова.

Обобщенная схема процесса приема вызова скорой медицинской помощи изображена на рисунке 2.

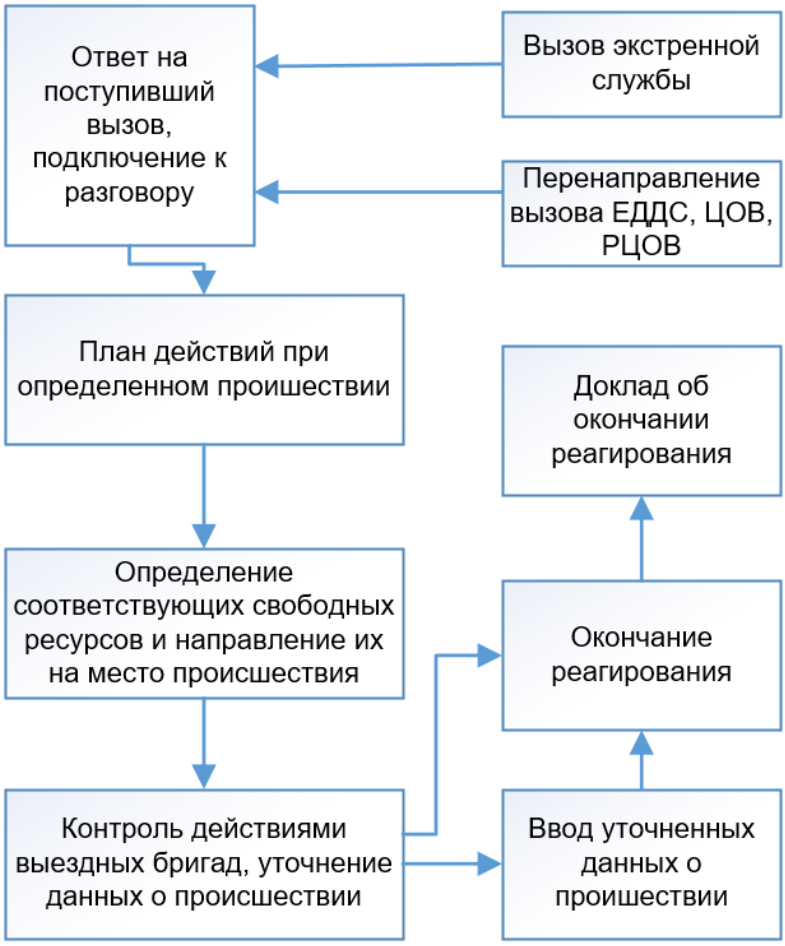



Рисунок 2 – Обобщенная схема процесса приема вызова

Решение об организации реагирования на вызов оператор принимает на основе оценки достоверности полученных данных с учётом возможной «необоснованности» вызова, типа происшествия, требований руководящих

документов и инструкций, условий обстановки, а также наличия сил и средств реагирования.

### 1.2 Анализ архитектуры автоматизированной системы

Прием и обработка вызовов службой скорой медицинской помощи осуществляется в установленном порядке в соответствии со «Статистическим инструментарием станций (отделений), больниц скорой медицинской помощи», утвержденным приказом Минздравсоцразвития России от 2 декабря 2009 г. № 942.

В составе операторского персонала основного и резервного центров обработки вызовов кроме дежурных специалистов могут быть предусмотрены также:

– старший смены;

– специалист - переводчик-лингвист;

– специалист психолог;

– ведущий инженер электроник.

Старший смены выполняет следующие функции:

– организация работы дежурных специалистов;

– координация взаимодействия операторов (при необходимости);

– сбор данных и формирование сводной отчетности по работе специалистов (операторов;

– выполнение функций дежурного оператора при повышенной нагрузке.

Специалист переводчик-лингвист выполняет следующие функции:

– обеспечение поддержки языков, отличных от русского, при общении операторов с позвонившим лицом;

– выполнение функций дежурного оператора при повышенной нагрузке.

Специалист психолог выполняет следующие функции:

– обеспечение психологической поддержки позвонившего лица (когда требуется его вмешательство) в двух режимах (с отключением оператора от разговора или с участием оператора в разговоре);

– выполнение функций дежурного специалиста при повышенной нагрузке.

Ведущий инженер электроник обеспечивает:

– надежное и своевременное предоставление информации об объектах связи, расположенных на территории Республики, различной степени детализации; обеспечение ее полноты, правильности, актуальности и необходимой конфиденциальности;

– возможность совместного использования разнородных данных, получаемых из различных источников (операторов связи, граждан), об объектах связи, расположенных на территории Республики;

– создание информационной основы для последующего решения аналитических задач;

– контроль актуальности и целостности баз данных;

– определение состава, структуры, внешнего вида компонентов системы обработки вызовов;

– внесение изменений в состав, структуру и логику работы системы обработки вызовов;

– контроль доступа к базам данных системы обработки вызовов или её компонентам пользователям системы в соответствии с их полномочиями;

– контроль корректности работы системы обработки вызовов и её компонентов;

– все виды работ с программными оболочками компонентов системы обработки вызовов, предусмотренные их разработчиками, в том числе настройку программно-технического комплекса пользователя, необходимую для нормального функционирования.

– выполнение функции дежурного оператора по приему и обработке вызовов.

Дежурный специалист (оператор) при приеме вызова выполняет следующие действия:

1) представляется позвонившему лицу;

2) производит первичный опрос позвонившего лица и регистрирует полученные сведения (информацию о происшествии) в базе данных (заполняет общую информационную часть (поля) унифицированной электронной формы учета события);

3) принимает решение о необходимости подключения к разговору переводчика, психолога.

Центр обработки вызовов скорой медицинской помощи в с. Майма Республики Алтай располагается в административном здании на 1 этаже. Схема расположения помещений представлена на рисунке 3.

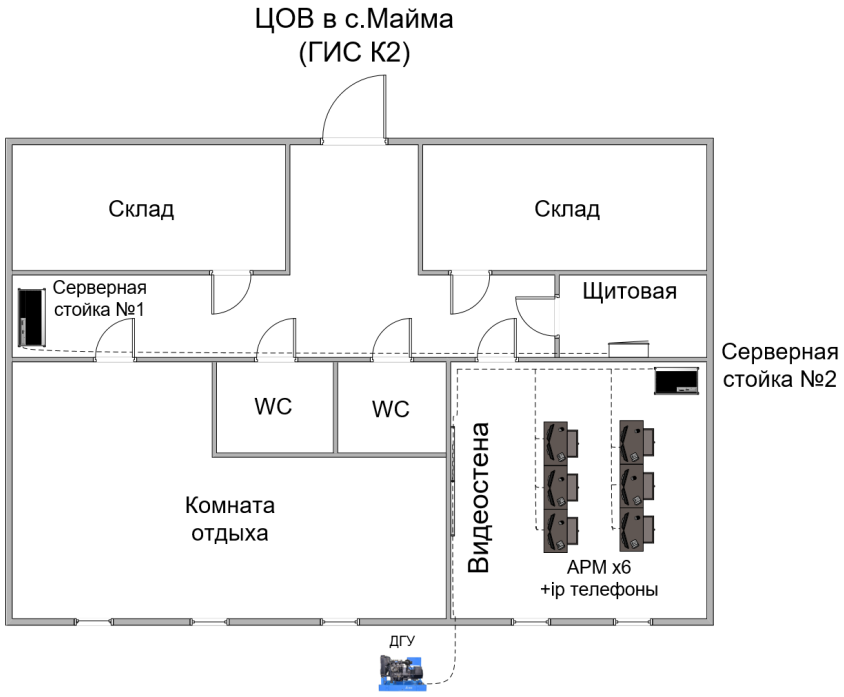



Рисунок 3 – Схема расположения помещений службы скорой медицинской помощи в с. Майма Республики Алтай

Локально-вычислительная сеть службы скорой медицинской помощи в с. Майма Республики Алтай состоит из диспетчерской службы медицинской помощи, рабочего места старшего смены, рабочего места, ведущего инженер электроника и специалиста психолога. Локально-вычислительная сеть ЦОВ

является сегментом сети взаимодействия оперативных служб системы 112 Республики Алтай.

В качестве пограничного с сетью Интернет оборудования выступает маршрутизатор D-Link DIR-841. С использованием программных фильтров пограничного маршрутизатора сетевое взаимодействие объектов ЦОВ службы скорой медицинской помощи в с. Майма Республики Алтай с ресурсами сети Интернет ограничено [9, 10].

Администрирование маршрутизаторов разрешено только из внутренней сети с IP-адреса компьютера ведущего инженера электроника.

В качестве коммутаторов уровня доступа применяются коммутаторы второго уровня TP-LINK TL-SF1016D. С целью повышения информационной безопасности локально-вычислительной сети, структурные подразделения организации вынесены в отдельные сегменты сети (VLAN), используя технологию 802.1Q реализованную коммутатором [9, 10].

Рабочие станции организации функционируют в рабочей группе – Workgroup со статической IP-адресацией из диапазона 172.16.9.0/24. Сетевое оборудование имеет статическую адресацию этого же диапазона.

Центр обработки данных (ЦОД) располагается в Республиканской больнице г. Горно-Алтайск на 3 этаже административного здания. ЦОД оснащен системами кондиционирования, пожарной и охранной сигнализацией. Доступ сотрудников больницы и посторонних лиц ограничен СКУД. Резервное электропитание оборудования осуществляется источниками бесперебойного электропитания. Схема ЦОД представлена на рисунке 4.

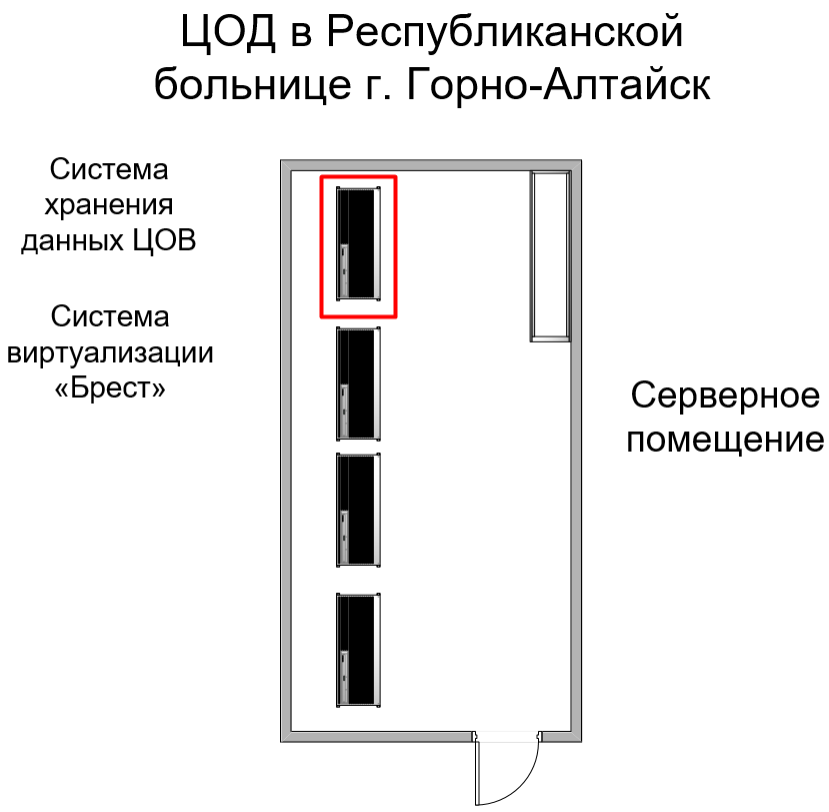



Рисунок 4 – Схема ЦОД в Республиканской больнице г. Горно-Алтайск

В качестве пограничного с сетью Интернет оборудования выступает маршрутизатор Cisco 3925, являющийся оборудованием провайдера ПАО «Ростелеком». С использованием программных фильтров пограничного маршрутизатора сетевое взаимодействие объектов ЦОД с ресурсами сети Интернет ограничено. Кроме того, настройками указанного маршрутизатора запрещено взаимодействие объектов сети Интернет, имеющих IP-адреса иностранных операторов связи, с объектами ИТС.

Для передачи голосового трафика используется голосовой шлюз Cisco VG204XM.

В качестве телекоммуникационного оборудования уровня доступа используется отказоустойчивый кластер из двух коммутаторов Cisco Catalyst 4500-X.

Резервное копирование баз данных осуществляется на систему хранения данных стоечного исполнения Synology SA3600.

## 1.3 Информация, подлежащая защите, определение источников информации

Приём вызовов службы скорой медицинской помощи осуществляется операторами, которые по результатам опроса позвонившего лица вводят в базу данных характеристики происшествия.

Все действия операторов (в том числе и переговоры) регистрируются в электронных базах данных системы обработки вызовов.

Вызов (сообщение о происшествии) от позвонившего лица через технические площадки местного оператора связи поступает в соответствующий программно-технический комплекс приема и обработки вызовов для автоматической регистрации и заполнения параметров:

– автоматически определяется номер абонентского устройства, с которого поступил вызов;

– автоматически от оператора связи принимаются данные о местоположении абонентского устройства, с которого осуществляется вызов;

– позвонившее лицо автоматически оповещается о записи разговора (если оператор немедленно подключился к данному вызову, то такое оповещение делает именно оператор);

– осуществляется автоматическая запись разговора вплоть до его окончания.

При этом на экране АРМ оператора ЦОВ отображается следующая информация:

– префикс района вызова (код зоны вызова) конкретного муниципального образования;

– номер абонентского устройства (телефона) с которого поступил вызов.

– местоположение абонентского устройства;

– фамилия, имя, отчество владельца абонентского устройства.

Перечисленные выше данные, а также данные о моменте (дате и времени) поступления вызова (сообщения о происшествии) фиксируются автоматически в унифицированной электронной форме события (вызова) (карточке вызова) и сохраняются в базе данных вызовов.

Оперативный срок хранения таких данных в системе обработки вызовов составляет 1 месяц, долговременный срок хранения – 36 месяцев.

Для обеспечения унификации процессов информационного обмена применяется унифицированная электронная форма учета события (информационная карточка). Под унифицированной электронной формой учета события (информационной карточкой) понимается документ единой базы данных системы обработки вызовов, доступ к которому имеет персонал системы в соответствии со своей компетенцией.

Координаты места происшествия, передаваемые внешними информационными системами (терминалами системы ЭРА-ГЛОНАСС, другими сигнальными системами и комплексами), также вводятся в базы данных системы обработки вызовов автоматически.

Рассматривая источники информации в центре обработки вызовов, можно выделить следующие:

– документация;

– персонал;

– оказываемые услуги;

– технические средства обеспечения деятельности;

– косвенные источники;

– информация на технических носителях [3, 4].

Всю информацию, циркулирующую в центре обработки вызовов службы скорой медицинской помощи в с. Майма Республики Алтай, можно разделить на три вида:

1) конфиденциальная информация, с ограничением допуска посторонних лиц (вопросы, касающиеся сил и средств);

2) персональные данные (база данных абонентов и сотрудников);

3) открытая информация, не подлежащая защите, утечка которой не нанесет вреда организации [8, 12].

По мнению Астахова А.М.: «Анализ рисков является наиболее значимой частью процесса управления рисками информационной безопасности». Этот процесс состоит из выявления и оценивания рисков, снижения их до требуемого уровня, а также применения оправданных мер для поддержки рисков в пределах установленного уровня.

Идеальной защиты не существует. При анализе каждой системы можно выявить уязвимости, угрозы, вероятности реализации угроз и ущерб. Опираясь на результат анализа рисков можно разработать и применить адекватные меры для снижения значений рисков до уровня, который приемлем для организации.

Риски могут иметь различные формы, не обязательно связанные с информационными технологиями. «С точки зрения информационной безопасности, существует несколько видов рисков, на которые организация должна обратить внимание. Семью основными категориями являются: действия человека, физический ущерб, неисправность оборудования, утрата данных, внутренние и внешние атаки, неправильное использование данных, ошибки в программном обеспечении» Гришина Н.В. [2, 7].

Выводы, которые отражены в отчете проведенного анализа рисков, не только влияют на управленческие решения и поведение руководителей отделов информационной безопасности, но также могут повлиять на решения руководства организации в целом. Правильная оценка рисков позволяет эффективно использовать имеющиеся ресурсы. Риски должны быть выявлены и оценены с позиции величины потенциальных потерь. Тем не менее, на практике реальные риски трудно оценить, но вполне возможно выделить приоритетные риски, которым следует уделить внимание в первую очередь. Также расставленные приоритеты среди рисков позволяют выстроить оперативный, тактический и стратегический план действий администраторов информационной безопасности.

Информационные ресурсы – это данные, используемые для получения информации; документы и массивы документов, самостоятельные и в системах.

Информационные ресурсы организации находятся в файлах массивов информации на компьютерах, архивах, фондах, библиотеках [8].

Более подробный анализ информационных ресурсов в центре обработки вызовов службы скорой медицинской помощи в с. Майма Республики Алтай представлен в таблице 1.

Таблица 1 – Информационные ресурсы службы скорой медицинской помощи в с. Майма Республики Алтай

| Наименование ресурса | Вид ресурса | Место хранения | Срок хранения | Вид хранения |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| Личное дело сотудника | ПДн | Старший смены | 75 лет | Бумажный |
| Данные абонентов | ПДн | Операторы ЦОВ, Старший смены, психолог | 75 лет | Электронный (АИС «ЦОВ») |
| Ведомость учета документов | Для служебного пользования | Старший смены | 5 лет | Бумажный, электронный (АИС «ЦОВ») |

Продолжение таблицы 1

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Статистическая отчетность | Для служебного пользования | Операторы ЦОВ, Старший смены | 5 лет | Бумажный, электронный (АИС «ЦОВ») |
| Другие документы (справки, докладные и др.) | Для служебного пользования | Старший смены | До прекращения срока действия | Бумажный |
| Устав организации | Информация свободного доступа | Старший смены | До ликвидации организации | Бумажный |
| Приказы, распоряжения | Для служебного пользования | Старший смены ЦОВ | 5 лет | Бумажный, электронный |
| Проекты приказов, распоряжений | Для служебного пользования | Старший смены | 1 год | Бумажный, электронный |
| Годовые планы структурных подразделений организации | Для служебного пользования | Старший смены | 5 лет | Бумажный, электронный |

## 2 Проектирование системы информационной безопасности

Во втором разделе работы осуществлено проектирование системы информационной безопасности объекта, рассмотрены типовые требования к автоматизированным информационным системам, построены модели угроз и возможных нарушителей, а также проведена оценка проектируемой системы информационной безопасности используя модель оценки эффективности Домарева.

### 2.1 Анализ требований к автоматизированным системам

Для создания защищенных автоматизированных информационных систем требуется наличие соответствующих знаний и опыта.

Потребитель может не разбираться в таком проекте и подробностях его развития, однако он должен следить за каждой ступенью на предмет соответствия техническому заданию и требованиям необходимых нормативных документов. В свою очередь, собственный опыт проектирования требует использования необходимых документов в этой сфере для получения максимально эффективного результата.

Таким образом, процесс проектирования защищенных автоматизированных информационных систем должен базироваться на знании и чётком выполнении требований существующих нормативных документов, как со стороны ее создателей, так и со стороны пользователей [8].

Защита информации – это набор комплексных мероприятий, совершающихся с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации, несанкционированного копирования, блокирования информации и т.п.

Из-за того, что потеря информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подходят также и мероприятия, связанные с повышением надежности сервера из-за отказов или нарушений в работе жестких дисков, недостатков в текущих программных средствах и т.д. [3, 6].

Существует четыре уровня защиты информации:

1) предотвращение (лишь авторизованный персонал имеет доступ к информации и технологии);

2) обнаружение (предусматривается раннее обнаружение нарушений и злоупотреблений, даже если системы защиты были обойдены);

3) ограничение (минимизируются потери, если преступление все-таки случилось, невзирая на защитные меры);

4) восстановление (обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по этой операции).

Существует 2 источника информации, на которых основывается оценка компании: внутренний и внешний. Под внутренними источниками понимаются официальные каналы распространения информации в организации, предоставление информации руководителю организации, ее структурных подразделений, филиалов и представительств. Под внешними – любая другая информация, полученная из любых других источников: партнеров, конкурентов, клиентов, властей и т.п.

Источники конфиденциальной информации предоставляют полные сведения о составе, описании и роде деятельности организации. Поэтому хорошая система защиты информации, созданная с учетом всех нюансов, позволит избежать различных проблем.

Анализ рисков является одним из способов управления ими, позволяя выбирать адекватные меры для защиты информации с помощью определения уязвимостей, угроз, а также оценки возможного воздействия, позволяя своевременно реагировать на угрозы [2].

Основными целями анализа рисков являются:

а) выявление угроз и уязвимостей;

б) идентификация активов и их ценности для организации;

в) количественная оценка вероятности угроз и влияния на бизнес потенциальных угроз;

г) обеспечение экономического баланса между ущербом от воздействия угроз и стоимостью контрмер.

По мнению Астахова А.М.: «Благодаря анализу рисков можно сравнить потенциальный годовой ущерб с годовой затратой контрмер».

Сам процесс анализа рисков согласно ГОСТ Р ИСО/МЭК 27005-2010 делится на несколько этапов:

1) выявление активов и их ценности для организации;

2) выявление угроз и их характеристик;

3) идентификация существующих средств управления рисками информационной безопасности [2,3].

При помощи данного этапа можно избежать лишних затрат и повысить эффективность уже существующих средств управления рисками информационной безопасности.

4) выявление уязвимостей, которые могут быть использованы злоумышленниками;

5) определение последствий, при происшествии негативного события;

6) установление количественной или качественной оценки рисков [2].

В зависимости от данных и их полноты, полученных при проведении анализа рисков, оценка рисков может иметь различную степень детализации. От степени детализации и обстоятельств зависит методология оценки рисков.

По мнению Астахова А.М.: «Она может быть качественной, количественной или комбинированной. В обычных случаях для получения общих представлений об уровне риска используется качественная оценка. Такая оценка удобна поначалу, так как в сравнении с количественной является менее сложной. Такая методика используется там, где невозможно получить удобные

числовые значения. Недостатком же является то, что выбор шкал является субъективным» [2, 5].

При качественной оценке применяется шкала значения атрибутов, при помощи которой описываются значения возможных последствий и вероятности их возникновения. Значения шкал и сами шкалы могут быть подстроены для конкретных обстоятельств, так как не всегда одно и то же описание подходит для разных рисков.

Для более точных оценок рисков используется количественная методология оценки рисков. В такой методологии применяются шкалы не с описательным, а числовым значением. Числовые значения последствий и их вероятности берутся из различных источников. От полученных числовых значений и выбранных моделей будет зависеть конечное значение риска. Именно поэтому все входящие данные и значения должны быть аргументированы. С одной стороны, такая методика позволяет количественно оценить риск, но в случаях, когда невозможно проверить числовые данные создается ложное чувство точности и ценности установленных величин риска [1, 2, 5].

От видов риска и цели их оценивания зависит то, каким способом будет выражаться последствие риска и его вероятность. Несмотря на то, что при качественной оценке конкретные числа не называются, а лишь их диапазон.

Выбранный диапазон показывает некий числовой промежуток, что косвенным образом позволяет оценить риск в числовом значении. Часто, при оценивании рисков применяются и качественная и количественная методики.

Оба подхода в зависимости от обстоятельств используются в разной степени, что позволяет компенсировать недостатки каждого подхода, взятого отдельно.

При проведении анализа рекомендуется указывать уровень неуверенности в оценке, так как это способствует лучшему пониманию результатов анализа.

После того, как организация определила величину риска, у нее есть 4 варианта действий: перенести, избежать, уменьшить или принять риск. Перенос

риска обозначает, что организация передает ответственность за него кому-либо другому, кто может более эффективно управлять риском.

Чтобы избежать, риска, необходимо прекратить деятельность, которая его вызывает. Для снижения риска до уровня, который удовлетворяет организацию, реализуются определенные меры. Принятие риска выгодно тогда, когда расходы на контрмеры превышают размер потенциального ущерба [1,2].

Для проведения анализа требований информационной безопасности была использована нормативная база, состоящая из некоторых документов:

– ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России.

– ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России.

– ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.

– ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

– ГОСТ Р 52069-2003. Защита информации. Система стандартов. Основные положения.

– ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью.

– ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности.

– ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

– ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

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

– Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

– Постановление Правительства Российской Федерации от 15.09. 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Постановление Правительства РФ от 8 февраля 2018 г. N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

В соответствии с проведенным анализом требований информационной безопасности к автоматизированным информационным системам, а также проведенным определением источников информации был осуществлен переход к построению моделей угроз и возможных нарушителей.

## 2.2 Модели угроз и возможных нарушителей

Для составления модели угроз и модели нарушителя необходимо определить наиболее важную информацию, проходящую в сети организации, а также хранимую на бумажных носителях.

В организации циркулируют:

– персональные данные сотрудников организации;

– персональные данные абонентов;

– служебная тайна организации;

– открытая информация [8].

Под угрозой имеется в виду высокая существующая вероятность специального или непреднамеренного действия, в результате которого могут быть нарушены основные свойства информации и систем ее обработки: доступность, целостность и конфиденциальность [15].

Модель угроз информационной безопасности представлена в Приложении А.

Следует иметь в виду, что финальная цель нарушения может быть разной, она варьируется от категории объекта и облика возможного нарушителя.

Возможные типы нарушителей делятся на две категории, а именно:

Внешние нарушители:

– разведывательные службы государств;

– криминальные структуры;

– недобросовестные партнеры;

– другие физические лица, не относящиеся к указанным выше.

2) Внутренние нарушители:

– лица, имеющие санкционированный доступ к информационной системе, но не имеющие доступа к защищаемой информации. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование информационной системы;

– зарегистрированные пользователи информационной системы, осуществляющие ограниченный доступ к ресурсам АИС с рабочего места;

– зарегистрированные пользователи информационной системы, осуществляющие удаленный доступ к защищаемой информации по локальным и (или) распределенным информационным системам;

– зарегистрированные пользователи информационной системы с полномочиями администратора безопасности сегмента информационной системы;

– зарегистрированные пользователи с полномочиями системного администратора информационной системы;

– зарегистрированные пользователи с полномочиями администратора безопасности информационной системы;

– программисты-разработчики прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте;

– разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств в информационной системе.

В таблице 2 рассмотрена модель нарушителя для центра обработки вызовов службы скорой медицинской помощи в с. Майма Республики Алтай.

Таблица 2 – Модель нарушителя ЦОВ службы скорой медицинской службы в с. Майма Республики Алтай.

| Наличие угрозы | Нарушитель | Вероятность реальной угрозы | Обоснование |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Съем информации с магнитного носителя | Посетитель | Средняя | В помещении, где производится обработка вызовов |
| | Обслуживающий персонал | Высокая | Постоянный доступ |
| | Злоумышленник | Высокая | Взлом |
| | Пользователь | Высокая | Постоянный доступ |
| Утечка акустической (речевой) информации | Посетитель | Средняя | Услышал во время посещения |
| | Обслуживающий персонал | Средняя | Подслушивание без применения технических средств |
| | Злоумышленник | Высокая | Применение технических средств перехвата информации |
| | Пользователь | Средняя | Подслушивание без применения технических средств |
| Утечка видовой информации | Посетитель | Низкая | В помещении, где производится обработка вызовов |
| | Обслуживающий персонал | Высокая | Имеется доступ к закрытым помещениям |
| | Злоумышленник | Высокая | Взлом |
| | Пользователь | Высокая | Постоянный доступ к носителям информации |
| Утечка | Посетитель | Низкая | Не актуально |
| | Обслуживающий | Низкая | Не актуально |

| | | | |
|---|---|---|---|
| информации по каналу ПЭМИН | персонал | | |
| | Злоумышленник | Высокая | Перехват электромагнитных излучений |
| | Пользователь | Низкая | Не актуально |
| «Анализа сетевого трафика» с перехватом передаваемой и принимаемой из внешних сетей информации | Посетитель | Низкая | Не актуально |
| | Обслуживающий персонал | Низкая | Не актуально |
| | Злоумышленник | Высокая | Взлом |
| | Пользователь | Средняя | Доступ к средствам обработки информации |

| | | | |
|---|---|---|---|
| Сканирование, направленное на выявление типа используемых операционных систем, топологии сети, открытых портов и служб и др. | Посетитель | Низкая | Не актуально |
| | Обслуживающий персонал | Низкая | Не актуально |
| | Злоумышленник | Высокая | Взлом |
| | Пользователь | Высокая | Постоянный доступ к средствам обработки информации |
| Внедрение ложного объекта | Посетитель | Средняя | Во время посещения |
| | Обслуживающий персонал | Высокая | В рабочее время |
| | Злоумышленник | Низкая | Не актуально |
| | Пользователь | Высокая | В рабочее время |
| Выявления паролей | Посетитель | Низкая | Не актуально |
| | Обслуживающий персонал | Низкая | Не актуально |
| | Злоумышленник | Высокая | Взлом |
| | Пользователь | Высокая | Доступ к паролям |
| Удаленный запуск приложений | Посетитель | Низкая | Не актуально |
| | Обслуживающий персонал | Низкая | Не актуально |
| | Злоумышленник | Высокая | Взлом |
| | Пользователь | Средняя | Внедрение вредоносной программы во время рабочего дня |
| Внедрение по сети вредоносных | Посетитель | Низкая | Не актуально |

| | | | |
|---|---|---|---|
| программ | | | |
| | Обслуживающий персонал | Низкая | Не актуально |
| | Злоумышленник | Высокая | Взлом |
| | Пользователь | Средняя | Внедрение вредоносной программы в локальную сеть во время рабочего дня |

## 2.3 Состав и оценка эффективности проектируемой системы информационной безопасности

На всех этапах жизненного цикла системе защиты информации присущи неопределенность ее свойств в условиях реального воздействия случайных факторов из внешней и внутренней среды. Оценка эффективности деятельности является составной частью процедуры управления эффективностью деятельности организации. Оценка эффективности системы защиты информации выполняется с учетом определенных потенциальных угроз и моделей нарушителей.

Проектируемая система информационной безопасности службы скорой медицинской помощи Республики Алтай представлена на рисунке 5.

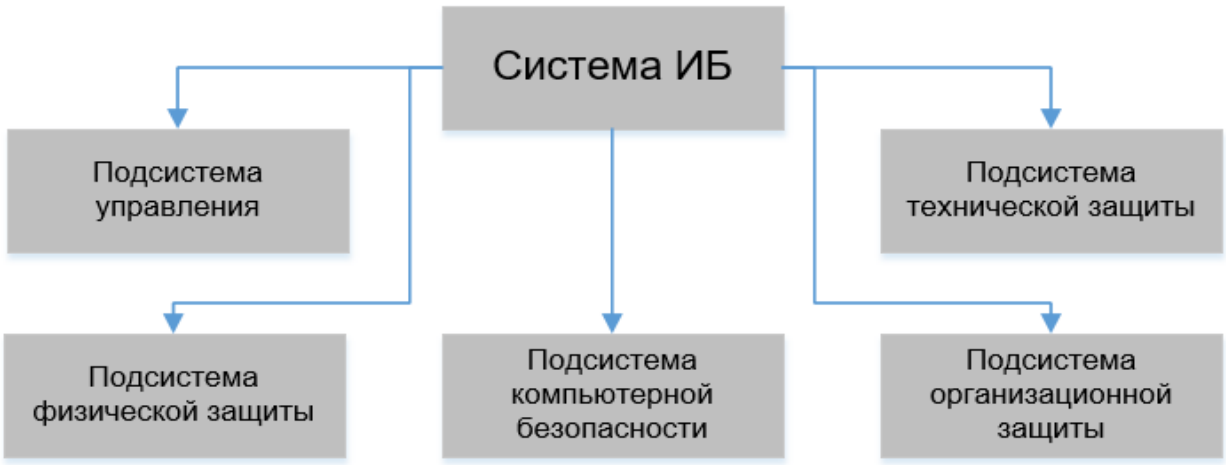


Рисунок 5 – Проектируемая система информационной безопасности службы скорой медицинской помощи Республики Алтай

Из рисунка 5 видно, что проектируемая система информационной безопасности состоит из 5 ключевых подсистем.

Для оценки эффективности защиты системы информационной безопасности службы скорой медицинской помощи Республики Алтай будет использована модель оценки эффективности Домарева, которая путём экспертных оценок показывает наиболее уязвимые места в системе информационной безопасности организации, тем самым определяя область дальнейшего совершенствования системы.

Так как руководством организации была принята наступательная стратегия обеспечения информационной безопасности, вероятность защиты информации должна быть не ниже 0,87.

В таблице 3 представлены показатели эффективности системы информационной безопасности для каждой из подсистем информационной безопасности организации.

Таблица 3 – Обобщенные показатели эффективности системы информационной безопасности организации

| Показатели | Подсистемы ИБ организации | | | | | $Q_{сзи}$ |
|---|---|---|---|---|---|---|
| | Управления | Компьютерной безопасности | Физической защиты | Организационной защиты | Технической защиты | |
| | Коэффициенты важности по направлениям | | | | | |
| | 0,2 | 0,2 | 0,2 | 0,2 | 0,2 | |
| Количественный | 0,89 | 0,84 | 0,88 | 0,87 | 0,88 | 0,86 |

Исходя из таблицы 3, можно сделать вывод, что наиболее уязвимое место в системе информационной безопасности организации – подсистема компьютерной безопасности, вероятность защиты информации для данной

подсистемы – 0,84, а вероятность защиты информации в организации в целом – 0,86, что не соответствует утвержденной наступательной стратегии (вероятность защиты информации 0,87 – 0,93).

Для получения более детального результата, была проведена подробная оценка эффективности всей подсистемы компьютерной безопасности, представленной в таблице 4.

Таблица 4 – Оценка эффективности подсистемы компьютерной безопасности

| № этапа | Перечень показателей | № элемента матрицы | Требуемый профиль безопасности | Достигнутый профиль безопасности | Степень выполнения групп требований | Количественная оценка |
|---|---|---|---|---|---|---|
| | *m* | № | $Q_{тр}$ | $Q_{д}$ | $Q_{груп}$ | *Q* |
| Определение объектов ИС, подлежащих защите | 1 | 121 | 0,87 | 0,91 | 0,9 | 0,84 |
| | 2 | 122 | | 0,89 | | |
| | 3 | 123 | | 0,88 | | |
| | 4 | 124 | | 0,9 | | |
| Выявление потенциальных угроз | 5 | 221 | | 0,91 | 0,89 | |
| | 6 | 222 | | 0,89 | | |
| | 7 | 223 | | 0,87 | | |
| | 8 | 224 | | 0,88 | | |
| Проведение оценки угроз и рисков | 9 | 321 | | 0,9 | 0,88 | |
| | 10 | 322 | | 0,88 | | |
| | 11 | 323 | | 0,87 | | |
| | 12 | 324 | | 0,87 | | |
| Определение требований к СЗИ | 13 | 421 | | 0,9 | 0,88 | |
| | 14 | 422 | | 0,88 | | |
| | 15 | 423 | | 0,87 | | |
| | 16 | 424 | | 0,88 | | |
| Осуществление выбора средств защиты информации | 17 | 521 | | 0,54 | **0,53** | |
| | 18 | 522 | | 0,55 | | |
| | 19 | 523 | | 0,47 | | |
| | 20 | 524 | | 0,56 | | |
| Внедрение средств ЗИ | 21 | 621 | | 0,87 | 0,87 | |
| | 22 | 622 | | 0,87 | | |
| | 23 | 623 | | 0,87 | | |
| | 24 | 624 | | 0,87 | | |
| Осуществление управления | 25 | 721 | | 0,91 | 0,91 | |
| | 26 | 722 | | 0,9 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 27 | 723 | | 0,9 | | |
| | 28 | 724 | | 0,91 | | |

Исходя из таблицы 4, были выявлены несоответствия требованиям безопасности на этапе №5 «Осуществление выбора средств защиты информации».

Степень выполнения требований по каждому этапу из подсистемы компьютерной безопасности графически представлена на рисунке 6.

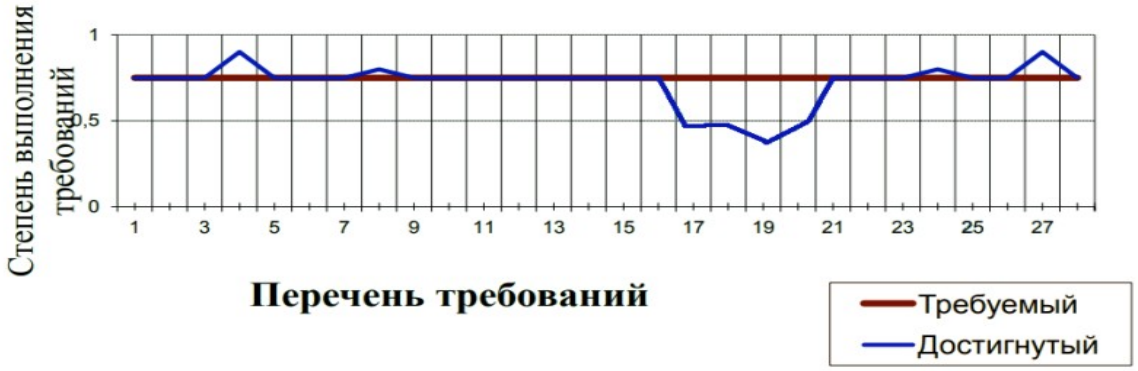



Рисунок 6 – Графическое сравнение оценки эффективности подсистемы компьютерной безопасности

Из рисунка 6 видно, что наиболее уязвимыми показателем являются позиции с 17 по 20 – осуществление выбора средств защиты информации.

По результатам анализа состава и оценки эффективности существующей системы информационной безопасности выявлено (на основе методики Домарева), что в целом вероятность защиты информации системы информационной безопасности – 0,86, что не соответствует утвержденной в организации наступательной стратегии (0,87 – 0,93).

В ходе анализа всех подсистем информационной безопасности методикой Домарева было выявлено, что подсистема технической защиты – наиболее проблемная отрасль. Вероятность защиты информации данной подсистемы равна 0,84, что не соответствует наступательной стратегии.

Рекомендуется совершенствовать данную подсистему для достижения требуемого уровня защищенности всей системы информационной безопасности службы скорой медицинской помощи Республики Алтай.

# 3 Разработка защищенного комплекса

## 3.1 Структурно-функциональная схема проекта

Одной из важных тенденций в развитии современных автоматизированных систем является широкое использование технологий виртуализации, предполагающих активное применение наряду с физической инфраструктурой виртуальной инфраструктуры компьютерных сетей.

Виртуальная инфраструктура эмулируется за счет физической инфраструктуры специализированными операционными системами, называемыми гипервизорами, функционирующими на специально выделенных серверах виртуализации.

В состав виртуальной инфраструктуры входят:

- виртуальные серверы и сетевые хранилища данных (СХД), предоставляющие соответствующие информационные ресурсы за счет реальной инфраструктуры;
- виртуальная вычислительная сеть, состоящая из виртуального коммуникационного оборудования (виртуальных коммутаторов, маршрутизаторов) и виртуальных каналов связи;
- виртуальные рабочие станции, т. е. виртуальные автоматизированные рабочие места (АРМ), к которым пользователи подключаются с реальных рабочих станций для использования информационных ресурсов, предоставляемых виртуальными серверами и СХД за счет ресурсов реальной инфраструктуры.

Таким образом, технологии виртуализации позволяют создавать на одном сервере виртуализации несколько логических систем – изолированных виртуальных машин – с полным набором функций физических устройств, эмулируемых за счет реальных ресурсов и связанных между собой эмулируемым виртуальным коммуникационным оборудованием.

Вместе с тем применение технологий виртуализации способствует возникновению дополнительных угроз информационной безопасности, для которых не применимы традиционные для физической инфраструктуры средства и методы защиты.

Появление дополнительных угроз ИБ, неспецифичных для физической инфраструктуры, повышает уровень информационных рисков автоматизированных систем, использующих технологии виртуализации. Для повышения безопасности автоматизированных систем, использующих технологии виртуализации, и предотвращения реализации угроз путем эксплуатации уязвимостей, применяются контрмеры, но и после их введения могут сохраняться остаточные уязвимости.

Поэтому актуальной задачей является снижение информационных рисков автоматизированных систем, использующих технологии виртуализации до приемлемого уровня путем устранения уязвимостей (слабых мест), на основе управления доступом к информации в виртуальной среде и применения средств защиты в виртуальной инфраструктуре.

В качестве объектов защиты, специфичных для виртуальной инфраструктуры, выступают следующие объекты:

- виртуальные вычислительные системы (виртуальные машины – ВМ);
- средства управления виртуальной инфраструктурой (ВМ управления средой виртуализации);
- виртуальная вычислительная сеть;
- отдельные виртуальные устройства обработки, хранения и передачи данных (виртуальные процессоры, диски, память, виртуальное сетевое оборудование и др.);
- гипервизоры, формирующие среду виртуализации;
- серверы виртуализации, на которых функционируют гипервизоры.

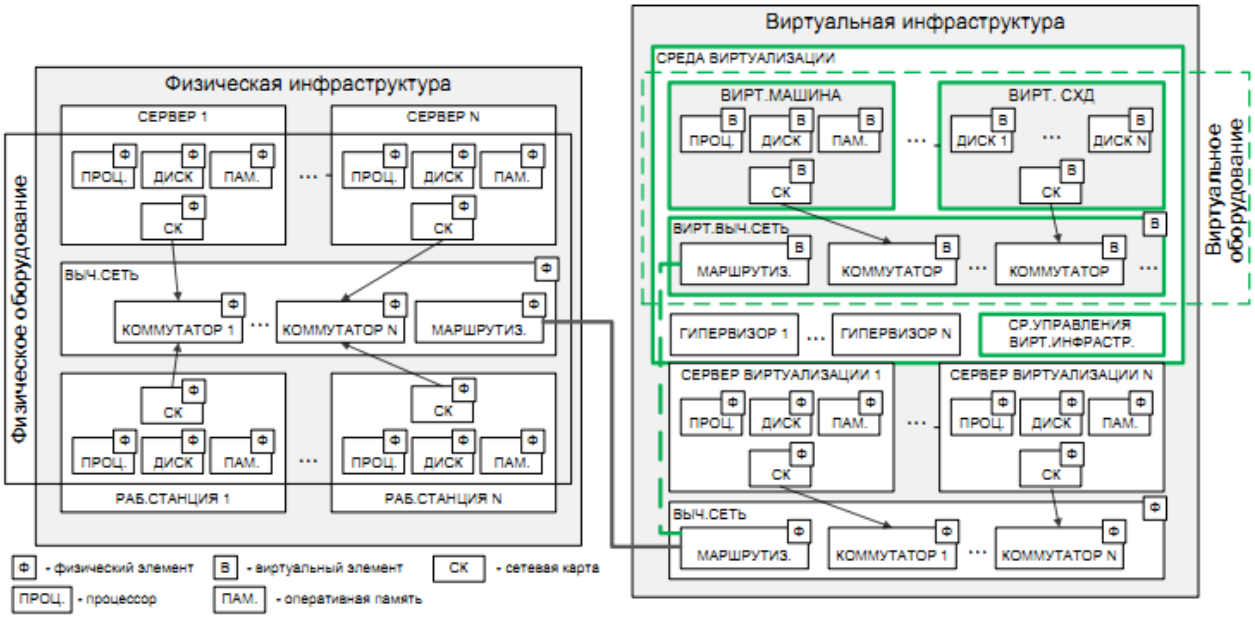



Рисунок 7 – Физическая и виртуальная инфраструктура компьютерной сети

На рисунке 7 наглядно представлены элементы физической и виртуальной инфраструктур. При этом элементы виртуальной инфраструктуры эмулируются с помощью программных гипервизоров, формирующих среду виртуализации и функционирующих на реальных серверах виртуализации.

Целесообразно выделить перечень угроз, характерных для виртуальной инфраструктуры:

- угрозы загрузки нештатной ОС на серверах виртуализации и виртуальных машинах;
- угрозы маскировки под зарегистрированного пользователя при доступе к среде виртуализации (гипервизору) и виртуальным машинам;
- угрозы хищения, подлога и модификации данных внутри виртуальных машин;
- угрозы возникновения ошибок в управлении доступом к среде виртуализации (гипервизору) и ресурсам виртуальных машин, например, неправильное назначение полномочий пользователям;
- угрозы несанкционированного сетевого взаимодействия внутри виртуальной сетевой инфраструктуры;

- угрозы несанкционированной маршрутизации сетевого трафика внутри виртуальной инфраструктуры;
- угрозы несанкционированного изменения, копирования, перемещения (миграции) виртуальных машин и обрабатываемых на них данных;
- угрозы внедрения программных вирусов и закладок в среду виртуализации (гипервизор) и внутрь виртуальных машин;
- угрозы компрометации подсистемы защиты инфраструктуры виртуальных машин (отсутствия информации о событиях НСД, перехвата управления средой виртуализации, нарушения целостности программного обеспечения (ПО), изменения параметров функционирования средств защиты и др.);
- угрозы потери данных внутри виртуальной инфраструктуры и нарушения работоспособности виртуальных машин.

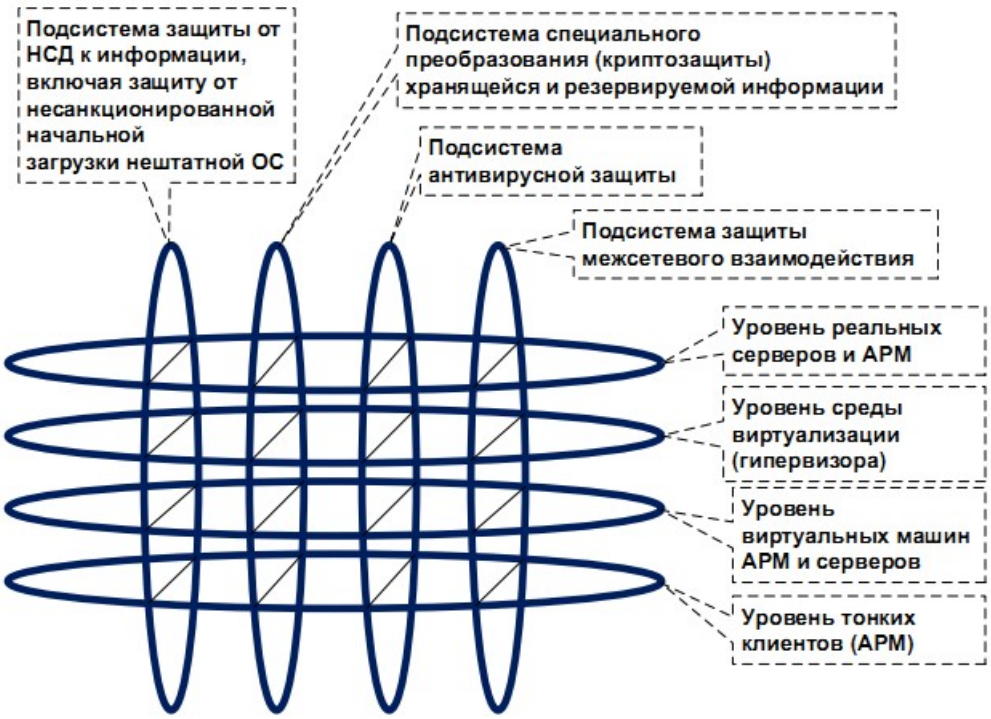



Рисунок 8 – Уровни и подсистемы защиты

С целью нейтрализации угроз для виртуальной инфраструктуры в автоматизированной должны быть предусмотрены разные уровни защиты с реализацией соответствующих подсистем (рисунок 8):

- уровень тонких клиентов (АРМ), с которых пользователи осуществляют доступ к виртуальным машинам АРМ и серверов;
- уровень виртуальных машин АРМ и серверов, функционирующих в среде виртуализации;
- уровень среды виртуализации (гипервизора), обеспечивающей работоспособность виртуальных машин;
- уровень реальных серверов и АРМ.

Нормативные требования по защите виртуальной инфраструктуры раскрыты в ряде отечественных нормативных документов.

При формировании требований по защите виртуальной инфраструктуры важно учитывать также звенья технологических цепочек обработки информации в АС, что позволит адаптировать меры защиты применительно к структурно-функциональным характеристикам информационной системы, используемым технологиям, а также к конкретным условиям обработки информации.

В соответствии с приказами ФСТЭК России № 17 от 2013 г. и № 27 от 2017 г., механизмы защиты среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также исключать воздействие на информацию и компоненты, в том числе на средства управления виртуальной инфраструктурой, виртуальные машины (гипервизоры), системы хранения данных (включая систему хранения образов виртуальной инфраструктуры), сеть передачи данных через элементы виртуальной или физической инфраструктуры.

Защита от несанкционированного доступа к информации на уровне среды виртуализации в настоящий момент может быть реализована на основе следующих сертифицированных средств:

- средства защиты платформ виртуализации vGate-S R2 для виртуальной инфраструктуры на базе VMware vSphere, а также vGate R2 для гипервизора Hyper-V из состава Windows Server;
- программного комплекса виртуализации и управления (ПК «ВИУ»), а также программного комплекса «Средства виртуализации «Брест» (ПК СВ «Брест») для ОС Astra Linux Special Edition (Astra Linux SE).

Защита от несанкционированного доступа при реализации технологических цепочек обработки информации в ЛВС должна обеспечиваться сертифицированными средствами защиты информации (СрЗИ), например:

- аппаратным модулем доверенной загрузки «Соболь» версии 4.2 с электронными ключами iButton;
- средством защиты информации от НСД Secret Net;
- генератором паролей «Генератор»;
- средством защиты инфраструктуры виртуальных машин vGate-S R2;
- средством специального преобразования хранящейся информации Zecurion Zserver;
- САВ3 Kaspersky Endpoint Security.

В цепочках по выполнению прикладных функций в соответствии с используемой схемой обработки информации выделяются следующие типовые звенья:

- обработка информации в рамках сеанса работы пользователей на закрепленных за ними АРМ;
- обмен информацией между физическим и виртуальным АРМ (ВМ АРМ) по протоколу доступа к удаленному рабочему столу этой ВМ (RDP, PCoIP или VMware Blast);
- обработка информации на ВМ АРМ, функционирующей в среде виртуализации;

- обмен информацией между ВМ АРМ и ВМ серверов обработки/приложений/баз данных, функционирующих в среде виртуализации, по протоколам предоставления информационных сервисов;
- обработка информации на ВМ серверов обработки/приложений/баз данных, функционирующих в среде виртуализации;
- обмен информацией между ВМ серверов обработки/ приложений/баз данных по протоколам предоставления информационных сервисов;
- доступ к сетевым хранилищам информации (СХД) и накопление информации в СХД.

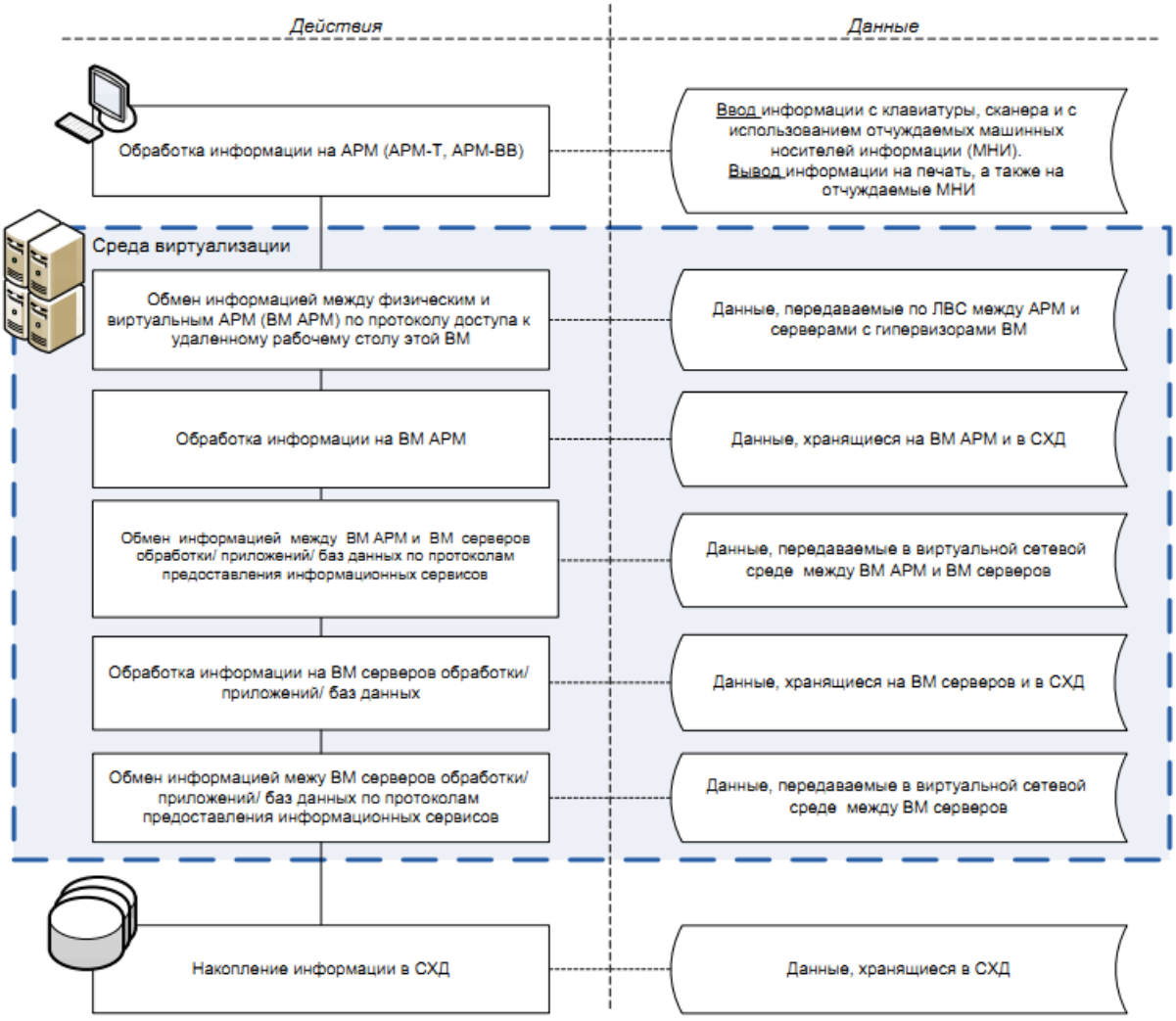



Рисунок 9 – Типовые звенья технологических цепочек обработки информации

Для защиты самих средств защиты информации в виртуальной инфраструктуре целесообразно использовать следующие механизмы:

- механизмы обеспечения доверенной загрузки средств вычислительной техники, реализуемые на физических АРМ и серверах аппаратным модулем доверенной загрузки (АПМДЗ) «Соболь», а на виртуальных АРМ и серверах – средством защиты инфраструктуры виртуальных машин vGate-S R2;
- механизмы контроля целостности программного обеспечения, включая ПО средств защиты информации, реализуемые АПМДЗ «Соболь», средством защиты информации от НСД Secret Net, а также средством защиты инфраструктуры виртуальных машин vGate-S R2;
- механизмы обеспечения замкнутой программной среды, реализуемые средством защиты информации от НСД Secret Net;
- механизмы регистрации и контроля действий пользователей, реализуемые средством защиты информации от НСД Secret Net.

## 3.2 Выбор целесообразных программно-технических средств и организационных мероприятий

В качестве средств защиты информации проектируемой информационной системы службы скорой медицинской помощи Республики Алтай предлагается осуществить выбор следующих средств защиты информации:

- общего программного обеспечения клиентской и серверной части;
- программных средств виртуализации;
- средств доверенной загрузки для защиты средств вычислительной техники от несанкционированного доступа;
- средств антивирусной защиты информации;
- средств криптографической защиты информации;
- средств обнаружения вторжений.

### 3.2.1 Выбор общего программного обеспечения

О необходимости форсированного развития отечественного рынка программного обеспечения, обеспечения максимальной независимости от иностранных разработок в сфере высоких технологий и сохранения информационного суверенитета впервые на высшем уровне заговорили в 2014 году, когда санкции США и Евросоюза резко повысили риски, связанные с применением зарубежного софта в бизнесе и государственных организациях.

Именно тогда в Министерстве связи и массовых коммуникаций РФ всерьез озадачились решением этого стратегически значимого, по мнению чиновников, вопроса вместе со стимулированием спроса на национальные продукты и проработкой соответствующих мер поддержки отечественных разработчиков.

Как результат – в кратчайшие сроки на законодательном уровне были утверждены ограничения на допуск иностранного ПО при осуществлении государственных и муниципальных закупок, а также правила формирования и ведения единого реестра российских программ.

Так как проектирование информационной системы службы скорой медицинской помощи Республики Алтай осуществляется за счет средств министерства здравоохранения Российской Федерации выбор программного обеспечения осуществляется из реестра российских программ.

Выбор общего программного обеспечения осуществлен из следующих вариантов:

1) Операционная система «Альт Линукс СПТ». Разработчики: ООО «Свободные программы и технологии», «Базальт СПО». Сайт продукта: sptlinux.ru

Альт Линукс СПТ представляет собой унифицированный дистрибутив для серверов и рабочих станций с встроенными программными средствами защиты информации, сертифицированными ФСТЭК России:

- класс защиты средств вычислительной техники от несанкционированного доступа;

- 3 уровень контроля отсутствия недекларированных возможностей.

Альт Линукс СПТ включает в себя:

- Альт Линукс СПТ Сервер;
- Альт Линукс СПТ Рабочая станция;
- Альт Линукс СПТ Тонкий клиент.

Альт Линукс СПТ Сервер сочетает в себе все возможности классического сервера и современные технологии управления ими.

Преимущества:

- легкое управление через веб-интерфейс;
- обеспечение мандатного принципа контроля доступа встроенными средствами;
- совместимость с ведущими Российскими производителями крипто-средств;
- централизованная аутентификация и обновление рабочих станций;
- не требуется отключение SecureBoot при загрузке ОС;
- стабильная работа сетевой и дисковой подсистем в течение длительного времени под высокой нагрузкой;
- возможность разворачивания в закрытом сегменте сети локального репозитория для установки и обновления программ;
- использование Samba 4 в роли контроллера домена Active Directory;
- возможность размещать системные службы (сервисы) в изолированных окружениях (виртуальных машинах);
- защита ввода и вывода на отчуждаемый физический носитель;
- управления фильтрацией сетевых пакетов;
- маскирование структуры внутренних подсетей;
- организация Интранет с механизмом аутентификации пользователей и назначения сетевых адресов - DNS-сервер (Bind);
- система регистрации событий.

Альт Линукс СПТ Рабочая станция предназначена для повседневной работы на персональных компьютерах, обеспечивает комфортную защищенную

работу с информацией ограниченного доступа с возможностью просмотра и копирования данных меньшей степени конфиденциальности или из открытых источников.

Преимущества:

- удобный, интуитивно понятный графический интерфейс;
- обеспечение мандатного принципа контроля доступа с помощью SELinux;
- веб-интерфейс настройки подсистемы печати Cups.

2) Astra Linux «Орел». Разработчик: НПО «Русские базовые информационные технологии» (РусБИТех). Сайт продукта: astra-linux.ru

Разработка научно-производственного объединения «РусБИТех», представленная в двух вариантах: Astra Linux Common Edition (общего назначения) и Astra Linux Special Edition (специального назначения).

Особенности последней версии ОС: развитые средства обеспечения информационной безопасности обрабатываемых данных, механизм мандатного разграничения доступа и контроля замкнутости программной среды, встроенные инструменты маркировки документов, регистрации событий, контроля целостности данных, а также прочие обеспечивающие защиту информации компоненты.

По заверениям разработчиков, Astra Linux Special Edition – единственная программная платформа, сертифицированная одновременно в системах сертификации средств защиты информации ФСТЭК России, ФСБ, Минобороны РФ и позволяющая обрабатывать в автоматизированных средствах всех министерств, ведомств и других учреждений России информацию ограниченного доступа, содержащую составляющие государственную тайну сведения с грифом не выше «совершенно секретно».

3) ROSA Linux. Разработчик: ООО «НТЦ ИТ РОСА». Сайт продукта: rosalinux.ru

Семейство операционных систем ROSA Linux включает внушительный набор решений, предназначенных для домашнего использования (версия ROSA

Fresh) и применения в корпоративной среде (ROSA Enterprise Desktop), развѐртывания инфраструктурных IT-служб организации (ROSA Enterprise Linux Server), обработки конфиденциальной информации и персональных данных (РОСА «Кобальт»), а также составляющих государственную тайну сведений (РОСА «Хром» и «Никель»). В основу перечисленных продуктов положены наработки Red Hat Enterprise Linux, Mandriva и CentOS с включением большого количества дополнительных компонентов – в том числе оригинальных, созданных программистами научно-технического центра информационных технологий «РОСА».

В частности, в составе дистрибутивов ОС для корпоративного сегмента рынка представлены средства виртуализации, ПО для организации резервного копирования, инструменты для построения частных облаков, а также централизованного управления сетевыми ресурсами и системами хранения данных.

Характеристики платформ представлены в таблице 5.

Таблица 5 – Сравнительные характеристики платформ ОС.

| Название | Достоинства | Недостатки |
|---|---|---|
| «Альт Линукс СПТ» | Не требуется отключение SecureBoot при загрузке ОС.<br>Средства управления операционной системой через веб-интерфейс (Alterator) | После настройки не печатает принтер.<br>Текст выглядит недостаточно четким. |
| Astra Linux «Орел» | Бесплатное обновление. | Не обновляются важные библиотеки (glibc).<br>Много ненужных приложений. |
| ROSA Linux | Стабильность.<br>Полностью русифицированный дистртибутив. | Старые версии пакетов.<br>Описание пакетов на английском языке.<br>Некоторых программ нет в репозиториях. |

Рассмотрев описание функциональных особенностей, реализованных защитных механизмов и сравнительных характеристик выбор остановлен на платформе Astra Linux «Орел» для клиентской и серверной части.

### 3.2.2 Выбор программных средств виртуализации

В качестве гипервизора платформы операционной системы Astra Linux «Орел» возможно использование следующих программных сред:

1) Гипервизор KVM.

Основные характеристики гипервизора KVM:

- поддержка аппаратной виртуализации и паравиртуальных устройств для гостевых систем;
- поддержка технологий виртуализации MMU (AMD NTP и Intel EPT);
- возможность работы с оборудованием из гостевой ОС (AMD IOMMU, Intel VT-D, SR-IOV);
- мандатный доступ к процессам гостевых ОС;
- поддержка устройств USB 2.0;
- защищенный доступ к гостевым ОС по протоколам VNC и SPICE;
- поддержка технологий повышенной аппаратной защиты NX и SMEP.

Ограничения гипервизора KVM для гостевых ОС:

- до 64 виртуальных процессоров;
- в режиме полной виртуализации до 4 IDE устройств;
- эмуляция до 28 паравиртуальных устройств.

2) ПК СВ «Брест».

Простота и скорость развертывания ПК СВ «Брест» не противоречат высокому уровню защищенности изделия, функционирующего в условиях мандатного, дискреционного и ролевого разграничения доступа с контролем целостности. Беспрецедентность данного решения делает его наиболее конкурентным в ЦОД корпоративного сегмента, в ЦОД государственных органов, вооруженных сил и других силовых структур Российской Федерации.

Программные возможности:

- централизованное управление;

Одним или несколькими ЦОД, управление кластером (или несколькими кластерами), входящими в ЦОД, управление хостом (сервером) в каждом кластере. Поддерживаются серверы архитектуры Intel x86_64 с конфигурацией до 160 логических процессоров, имеющих до 2 ТБ ОЗУ каждый. Для процессоров должны быть доступны технологии виртуализации.

Централизованное управлением пулом виртуальных машин (ВМ). Поддерживаются виртуальные машины Intel x86_64 или Intel x86 с конфигурацией до 64 виртуальных процессоров и до 2 ТБ ОЗУ каждая.

- централизованное управление пользователями;

Интеграция с доменами ALD. Идентификация, аутентификация и авторизация пользователей, операторов и обслуживающего персонала для получения сеанса работы с рабочим столом ВМ через домен безопасности.

Мандатная, дискреционная и ролевая модели разграничения доступа субъектов (пользователей) к объектам (виртуальные машины, хосты, кластеры, ЦОДы и др.).

- контроль целостности;
- централизованный аудит;
- формирование отчетов;
- миграция виртуальных машин в режиме работы;
- создание кластеров высокой доступности (High Availability);
- построение политик по распределению нагрузки;
- мониторинг аппаратного состояния серверов, входящих в ЦОД;
- проброс USB-устройств в обе стороны (как на клиента, так и от него) разграничение доступа к этим устройствам;
- поддержка протоколов управления VNC или SPICE;
- поддержка агрегации (логического объединения портов) сетевых соединений при построении высокопроизводительной отказоустойчивой сетевой инфраструктуры;

- создание нескольких сетей и разделение служебного и пользовательского трафика на разные информационные потоки, поддержка VLAN.

В качестве гипервизора выбрана сертифицированная отечественная платформа ПК СВ «Брест» имеющая наиболее развитый функционал и защитные механизмы.

### 3.2.3 Выбор средств доверенной загрузки для защиты средств вычислительной техники от несанкционированного доступа

Доверенная загрузка – это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации/аутентификации пользователя.

Аппаратные модули доверенной загрузки имеют значительные преимущества перед программными средствами. Но обеспечение доверенной загрузки не может быть выполнено только аппаратно.

Главные преимущества аппаратных средств:

- высокая степень защищённости информации о паролях, ключах и контрольных суммах системных файлов;
- возможная засекреченность алгоритмов шифрования, выполняемых аппаратно;
- невозможность запуска компьютера, не вскрывая его содержимого;
- невозможность запуска операционной системы пользователя, даже после извлечения аппаратного модуля в случае шифрования загрузочного сектора;
- невозможность получить любые данные после извлечения аппаратного модуля в случае полного шифрования данных.

Наиболее популярными модулями доверенной загрузки на современном рынке считаются:

1) Программно-аппаратный комплекс «Соболь» производства компании «Код Безопасности».

2) Средство доверенной загрузки «Dallas Lock» производства компании «Конфидент».

3) Аппаратно-программный модуль доверенной загрузки «Криптон-замок» производства компании Анкад.

Основываясь на выделенных достоинствах и недостатках перечисленных средств, была составлена сравнительная таблица основных характеристик (таблица 6).

Таблица 6 – Сравнительный анализ модулей доверенной загрузки

| Требования | Модуль доверенной загрузки | | |
|---|---|---|---|
| | ПАК «Соболь» | СДЗ «Dallas Lock» | АПМДЗ «Криптон-замок» |
| Контроль целостности программной среды | + | + | + |
| Контроль целостности реестра операционной системы | + | + | - |
| Идентификация и аутентификация с помощью аппаратных идентификаторов | + | + | + |
| Запрет загрузки со съемных носителей | + | - | - |
| Ведение журналов | + | + | + |
| Блокировка доступа | + | + | + |
| Аппаратный датчик случайных чисел | + | - | - |
| Контроль работоспособности | + | - | - |
| Разграничение ресурсов для каждого пользователя | - | - | + |

В результате сравнительного анализа выбран программно-аппаратный комплекс «Соболь» производства компании «Код Безопасности».

ПАК «Соболь» обеспечивает запрет загрузки операционной системы с недоверенных внешних носителей, позволяет проводить идентификацию и аутентификацию пользователей до загрузки операционной системы и блокирует доступ в систему при попытке отключения электронного замка с помощью модуля сторожевого таймера.

ПАК «Соболь» сертифицирован ФСТЭК России, ФСБ России и Минобороны России. Соответствует требованиям руководящих документов к средствам доверенной загрузки уровня платы расширения второго класса и может использоваться в автоматизированных системах до класса защищенности 1Б включительно, в ИСПДн до УЗ 1 включительно и в ГИС до 1-го класса защищенности включительно.

### 3.2.4 Выбор сетевых экранов

Целевые критерии при выборе межсетевого экрана – класс защищенности по требованиям ФСТЭК, наличие сертификата и период его действия, цена, пропускная способность, количество портов, возможность работы как сервера доступа с шифрованием трафика.

Основным средством обеспечения информационной безопасности, блокирующей несанкционированный доступ в локально вычислительную сеть, является межсетевой экран.

Проведем сравнительный анализ представленных на рынке и наиболее популярных решений по защите периметра организации.

Сопоставление параметров представлено в таблице 7.

Таблица 7 – Параметры сетевых экранов

| Наименование | ССПТ-2-81 | Juniper SRX3400 | ПАК ViPNet Coordinator HW100 |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Класс защиты и сертификаты соответствия | 3 класс, сертификаты ФСТЭК № 2141 и ФСБ № СФ/СЗИ-0139 | 3 класс, сертификат ФСТЭК № 3197 | 4 класс, сертификат ФСБ России № СФ/115-1285 и № |

| | | | |
|---|---|---|---|
| | | | СФ/115-1286 |
| Кол-во интерфейсов | 2 | 2 | 4 |
| Скорость | 10000 Мбит/сек | 16 Гбит/с | 950 Мбит/сек |
| Тип интерфейса | Ethernet 10BASE T/100BASE-TX/1000BASE TX/10000BASE TX | Ethernet 10/100/1000 BASE - T; Gigabit Ethernet (SFP); 10 Gigabit Ethernet | Ethernet 10/100/1000 |
| Цена | 370 000 руб. | 795 430 руб. | 233 800 руб. |

Выбор остановлен на наиболее экономически выгодном варианте – ПАК ViPNet Coordinator HW100.

### 3.2.5 Выбор средств обнаружения вторжений

Система обнаружения вторжений (Intrusion Detection System (IDS)) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Наиболее популярными программными средствами обнаружения вторжений на современном рынке считаются:

1) «Континент» – семейство продуктов для обеспечения сетевой безопасности при подключении к сетям общего пользования посредством межсетевого экранирования, построения частных виртуальных сетей (VPN) и системы обнаружения вторжений (СОВ).

2) ViPNet IDS – это программно - аппаратный комплекс, выполненный в виде отдельно стоящего сетевого устройства, предназначенный для обнаружения вторжений в информационные системы на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным.

3) Аппаратно-программный комплекс «Рубикон» выполняет функции межсетевого экранирования и системы обнаружения вторжений, является

программно-аппаратным комплексом, это упрощает установку этого программного средства и его сопровождение.

В состав комплекса входит маршрутизатор с поддержкой мандатных меток. Имеет сертификаты соответствия ФСТЭК России и Минобороны России.

Основываясь на выделенных достоинствах и недостатках перечисленных средств, была составлена сравнительная таблица основных методов защиты информации (таблица 8).

Таблица 8 – Сравнительный анализ средств обнаружения вторжений

| Требования | Средство обнаружения вторжений | | |
|---|---|---|---|
| | VipNet IDS | Континент | Рубикон |
| Фильтрация трафика | + | - | - |
| Регулярное обновление сигнатур | + | + | - |
| Централизованное управление | + | + | - |
| Техническая поддержка | + | - | + |
| Графические отчеты | + | + | - |
| Журнал обнаружения вторжений | + | - | - |
| Сертификаты ФСТЭК России | + | + | + |
| Сертификат ФСБ России | + | - | - |
| Цена | 171 300 руб | 186 581 руб | 490 000 руб |

В результате сравнительного анализа выбрано средство обнаружения вторжений VipNet IDS.

Выбранные программно-аппаратные средства для использования в ЦОВ и ЦОД службы скорой медицинской помощи в с. Майма Республики Алтай представлены в таблице 9.

Таблица 9 – Программно-аппаратные средства ЦОВ и ЦОД

| Наименование программно-технического | Место установки | Основные функции |
|---|---|---|

| | | |
|---|---|---|
| средства | | |
| 1. Общесистемное программное обеспечение: | | |
| Astra Linux «Смоленск» (в комплекте с ПК СВ «Брест») | ЦОД | Серверная операционная система |
| Astra Linux «Орёл» | ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ | Операционная система рабочих станций |
| 2. Прикладное программное обеспечение: | | |
| LibreOffice 6.4.2 | ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ | Набор офисных программ для создания, редактирования документов, таблиц, баз данных, презентаций |

Продолжение таблицы 9

| 1 | 2 | 3 |
|---|---|---|
| Браузер Yandex Browser | ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ | Просмотр интернет-сайтов |
| 3. Применяемые средства защиты информации: | | |
| Kaspersky Endpoint Security Linux 10.1.1.6421 | ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ, ЦОД | Комплексная антивирусная защита на всех каналах поступления и передачи информации |
| VipNet Client 4 for Linux | ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ | Программный комплекс, предназначенный для построения и обеспечения безопасной передачи данных между защищенными сегментами виртуальной сети VipNet, а также фильтрации IP-трафика, с использованием транспортной среды произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего доступа. |
| VipNet CSP | ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ | Крипто-провайдер установки и использования электронно-цифровой подписи |
| ПАК «Соболь 4.2» АМДЗ | ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены | Аппаратный модуль доверенной загрузки, предотвращение НСД к АРМ |

| | | |
|---|---|---|
| | ЦОВ | |
| ViPNet IDS 1000 | ЦОД | Программно-аппаратный комплекс для обнаружения вторжений в информационные системы, |

### 3.3 Функциональная оценка эффективности подсистемы компьютерной безопасности

Для оценки эффективности функционирования системы ИБ и защищённости подсистемы компьютерной безопасности после ее совершенствования и внедрения новых средств защиты вновь используется модель оценки эффективности Домарева.

В. В. Домарев разработал свою модель оценки систем ЗИ, основанную на системном подходе. Понятие системности по Домареву заключается не просто в создании соответствующих механизмов защиты, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла ИС. При этом все средства, методы и мероприятия, используемые для защиты информации, объединяются в единый целостный механизм - систему защиты.

Создавая данную модель, Домарев исходил из того, что многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. В то же время большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том, как же приступить к созданию системы защиты информации для конкретной информационной системы, с учетом присущих ей особенностей и условий функционирования. Возникает вопрос: можно ли сформировать такой подход к созданию систем защиты информации, который объединил бы в нечто единое целое усилия, знания и опыт различных специалистов? При этом желательно, чтобы указанный подход был универсальным, простым, понятным и позволял бы в одинаковой степени удовлетворить любые требования специалистов по

обеспечению информационной безопасности.

Практическая задача обеспечения информационной безопасности состоит в разработке модели представления системы (процессов) ИБ, которая на основе научно-методического аппарата позволяла бы решать задачи создания, использования и оценки эффективности СЗИ для проектируемых и существующих уникальных ИС.

Ниже представлен результат оценки защищённости подсистемы компьютерной безопасности (таблица 10).

Таблица 10 – Итоговая оценка эффективности подсистемы компьютерной безопасности.

| № этапа | Перечень показателей | № элемента матрицы | Требуемый профиль безопасности | Достигнутый профиль безопасности | Степень выполнения групп требований | Количественная оценка |
|---|---|---|---|---|---|---|
| | *m* | *№* | $Q_{тр}$ | $Q_{д}$ | $Q_{груп}$ | *Q* |
| 1.Определение объектов ИС, подлежащих защите | 1 | 121 | 0,87 | 0,91 | 0,9 | 0,88 |
| | 2 | 122 | | 0,89 | | |
| | 3 | 123 | | 0,88 | | |
| | 4 | 124 | | 0,9 | | |
| 2.Выявление потенциальных угроз | 5 | 221 | | 0,91 | 0,89 | |
| | 6 | 222 | | 0,89 | | |
| | 7 | 223 | | 0,87 | | |
| | 8 | 224 | | 0,88 | | |
| 3.Проведение оценки угроз и рисков | 9 | 321 | | 0,9 | 0,88 | |
| | 10 | 322 | | 0,88 | | |
| | 11 | 323 | | 0,87 | | |
| | 12 | 324 | | 0,87 | | |
| 4.Определение требований к СЗИ | 13 | 421 | | 0,9 | 0,88 | |
| | 14 | 422 | | 0,88 | | |
| | 15 | 423 | 0,87 | 0,87 | | |
| | 16 | 424 | | 0,88 | | |
| 5.Осуществление выбора средств защиты информации | 17 | 521 | | 0,87 | 0,88 | |
| | 18 | 522 | | 0,88 | | |
| | 19 | 523 | | 0,87 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 20 | 524 | | 0,87 | | |
| 6.Внедрение средств ЗИ | 21 | 621 | | 0,88 | 0,87 | |
| | 22 | 622 | | 0,88 | | |
| | 23 | 623 | | 0,87 | | |
| | 24 | 624 | | 0,88 | | |
| 7.Осуществление управления | 25 | 721 | | 0,91 | 0,91 | |
| | 26 | 722 | | 0,9 | | |
| | 27 | 723 | | 0,9 | | |
| | 28 | 724 | | 0,91 | | |

Из таблицы 10 следует, что оценка защищенности подсистемы компьютерной безопасности показывает, что эффективность этапа № 3 составляет 0,88 при требуемом показателе вероятности защиты информации от 0,87 до 0, 95.

Также представлена таблица с обобщенными показателями защищенности системы информационной безопасности, в которой отражены количественные и качественные показатели защиты и коэффициенты важности по направлениям, что позволяет наглядно оценить, как мероприятия по совершенствованию отразились на всей системе информационной безопасности в целом (таблица 11).

Таблица 11 – Итоговые обобщенные показатели эффективности системы информационной безопасности предприятия.

| Показатели | Подсистемы ИБ организации | | | | | $Q_{сзи}$ |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| | Коэффициенты важности по направлениям | | | | | |
| | 0,2 | 0,2 | 0,2 | 0,2 | 0,2 | |
| Количественный | 0,89 | 0,88 | 0,88 | 0,87 | 0,88 | 0,88 |

Таким образом, таблица 11 позволяет наглядно оценить, как внедрение в подсистему компьютерной безопасности предложенных мер отразилось на эффективности всей системы ИБ в целом.

Основной задачей моделирования является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки

эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

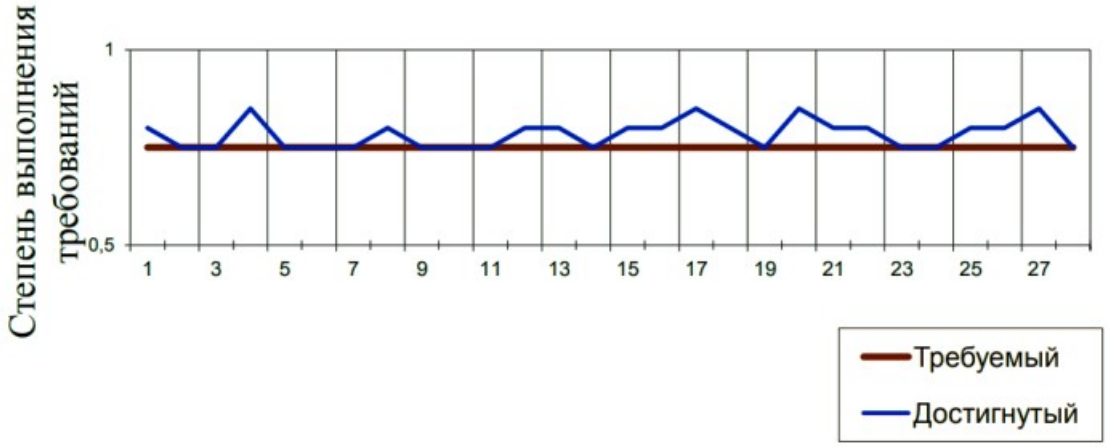



Рисунок 11 – Итоговое графическое сравнение оценки эффективности подсистемы компьютерной безопасности

Из рисунка 11 видно, что подсистема компьютерной безопасности удовлетворяет принятой наступательной стратегии, и вероятность защиты информации достигает требуемого уровня.

Таким образом, осуществление предложенных мероприятий повысит вероятность защиты информации с 0,53 до 0,88, что удовлетворяет принятой руководством наступательной стратегии обеспечения информационной безопасности.

### 3.4 Расчет технико-экономических показателей

Определим исходные данные для расчета затрат на проектирование защищенного комплекса средств автоматизации приема вызовов скорой медицинской помощи.

Сметная стоимость проекта включает в себя затраты, определяемые по формуле (1):

$$C_{модерн} = C_{пр} + C_{о}, \qquad (1)$$

где $C_{пр}$ – стоимость программных средств;

$C_o$ – затраты на оборудование;

В качестве средств защиты информации проектируемой информационной системы службы скорой медицинской помощи Республики Алтай предлагается установить следующие средства:

- операционную систему Astra Linux «Орел» в количестве 6 лицензий для клиентской части;
- платформа виртуализации ПК СВ «Брест» в комплекте Astra Linux «Смоленск»;
- средство антивирусной защиты Kaspersky Endpoint Security Linux 10.1.1.6421 в количестве 7 лицензий;
- ПАК «Соболь» в количестве 7 шт;
- ПАК ViPNet Coordinator HW100 2шт;
- средство обнаружения вторжений VipNet IDS 1 шт.

### 3.4.1 Расчёт расходов на оборудование

К расходам на оборудование относят затраты на его приобретение. Затраты по ним определяются по экспертным оценкам. Расчёт расходов на оборудование приведён в таблице 12.

Таблица 12 – Расчет затрат на оборудование проекта

| Наименование | Характеристики | Кол-во | Сумма, руб. |
|---|---|---|---|
| ПАК «Соболь» | Контроль целостности программной среды<br>Контроль целостности реестра операционной системы<br>Идентификация и аутентификация с помощью аппаратных идентификаторов<br>Запрет загрузки со съемных носителей<br>Ведение журналов<br>Блокировка доступа<br>Аппаратный датчик случайных чисел<br>Контроль работоспособности<br>Разграничение ресурсов для каждого пользователя | 7 | (11 950 руб. × 7) = 83 650 руб. |

| | | | |
|---|---|---|---|
| ПАК ViPNet Coordinator HW100 | 4 класс, сертификат ФСБ России № СФ/115-1285 и № СФ/115-1286<br>950 Мбит/сек<br>Ethernet 10/100/1000 | 2 | (89 400 руб. × 2) = 178 800 руб. |
| ПАК VipNet IDS | Фильтрация трафика<br>Регулярное обновление сигнатур<br>Централизованное управление<br>Техническая поддержка<br>Графические отчеты<br>Журнал обнаружения вторжений<br>Сертификаты ФСТЭК России<br>Сертификат ФСБ России | 1 | 171 300 руб. |
| Итог | | | 433 750 руб. |

Итоговая стоимость оборудования составляет 433 750 руб.

### 3.4.2 Расчёт расходов на программное обеспечение

Расчёт расходов на покупку программного обеспечения приведён в таблице 13.

Таблица 13 – Расчет затрат на программное обеспечение для модернизации

| Наименование | Характеристики | Кол-во | Сумма, руб. |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Astra Linux «Орёл» Common Edition версия 2.12 | Операционная система для персонального использования.<br>Разрядность ОС 32/64.<br>Минимальная частота процессора 1 ГГц, оперативная память 1 Гб, требуемое место на диске 20 Гб | 6 | (6 500 руб. × 6 ) = 39 000 руб. |
| ПК СВ «Брест»+ Astra Linux «Смоленск» Special Edition версия 1.6 | Централизованное управлением пулом виртуальных машин (ВМ).<br>Поддерживаются виртуальные машины Intel x86_64 или Intel x86 с конфигурацией до 64 виртуальных процессоров и до 2 ТБ ОЗУ каждая. | 1 | 380 000 руб. |
| Kaspersky Endpoint Security Linux 10.1.1.6421 | Комплексное антивирусное средство, включающее в себя:<br>Анализ поведения;<br>Защиту от эксплойтов;<br>Откат вредоносных действий;<br>Предотвращение вторжений;<br>Защиту от файловых угроз;<br>Защиту от почтовых угроз;<br>Защиту от веб-угроз;<br>Защиту от сетевых угроз;<br>Сетевой экран; | 7 | (1 729 руб. × 7) = 12 103 руб. |

| | | | |
|---|---|---|---|
| | Защиту от атак BadUSB;<br>Веб-контроль;<br>Контроль программ;<br>Контроль устройств;<br>Шифрование файлов;<br>Полнодисковое шифрование. | | |
| Итог | | | 431 103 руб. |

Итоговая стоимость программного обеспечения составляет 431 103 руб.

Результаты расчета затрат на реализацию проекта представлены в таблице 14.

Таблица 14 – Результаты расчета затрат на реализацию проекта

| № | Наименование статей | Обозначение | Сумма, руб. |
|---|---|---|---|
| 1 | Оборудование | $С_{мат}$ | 433 750 |
| 2 | Программное обеспечение | $С_{пр}$ | 431 103 |
| Итого | | $С_{модерн}$ | 864 853 |

Таким образом, полная стоимость проекта составляет 864 853 руб.

## Заключение

Развитие информационных технологий и рост их значения для обеспечения потребностей социальных сфер объективно приводят к увеличению расходов государства на информационные технологии.

В настоящее время уровень затрат на информационные технологии организации приближается, а иногда и превышает уровень инвестиций в другие производственные процессы, вместе взятые.

Одним из наиболее широко распространенных методов является метод оценки совокупных затрат на информационные технологии позволяющий оценить совокупные затраты на информационные технологии (оборудование, инструментальные средства (ПО), процессы сопровождения информационных систем, а также действия конечных пользователей), анализировать их и соответственно управлять ИТ-затратами (бюджетом) для достижения наилучшей отдачи от ИТ в организации.

В выполненной работе был проведен анализ объекта информационной защиты, в результате которого определено, что руководством организации была принята наступательная стратегия обеспечения информационной безопасности, с вероятностью защиты информации равной в пределах от 0,87 до 0,95. В результате оценки эффективности проектируемой системы информационной безопасности определено, что вся система в целом не удовлетворяет принятой стратегии (0,86), а подсистеме компьютерной безопасности соответствует наименьшая вероятность защиты информации (0,53).

Для повышения эффективности подсистемы компьютерной безопасности был предложен ряд программных и программно-аппаратных средств защиты для оборудования защищаемого помещения.

В результате оценки эффективности предложенных мер определено, что мероприятия по совершенствованию вывели на требуемый уровень как подсистему компьютерной безопасности, так и всю систему информационной безопасности центра обработки вызовов службы скорой медицинской помощи в целом.

Таким образом, был предложен комплекс организационных мер и средств программной и программно-аппаратной защиты для подсистемы компьютерной безопасности в системе информационной безопасности организации. Цели работы достигнуты, проект экономически выгоден.

**Список использованных источников**

1) Альтерман, А.Д. Современное программное и аппаратное обеспечение / А.Д. Альтерман // Международный научный журнал «Инновационное развитие». - Пермь, 2017. - № 12. - 19 с.

2) Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2015 - 312 с.

3) Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

4) Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2016. - 474 с.

5) Воронов А.А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А.А. Воронов, И.Я. Львович, Ю.П. Преображенский, В.А. Воронов // Информация и безопасность. 2016. – 234 с.

6) Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2017. - 336 с.

7) ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». М.: Стандартинформ, 2008

8) ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России;

9) ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования;

10) ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью;

11) ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности;

12) ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем;

13) Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 5 декабря 2016 г. №646).

14) Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. №149 - ФЗ // «Российская газета» от 29 июля 2006 г.

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

16) Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

17) Постановление Правительства Российской Федерации от 15.09. 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

18) Постановление Правительства РФ от 8 февраля 2018 г. N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

19) Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.

20) Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. - К.: ТИД Диа Софт, 2017;

21) Лушников, Н.Д. Комплексная установка элементов системы безопасности предприятий / Н.Д. Лушников, А.Д. Альтерман // Международный научный журнал «Инновационное развитие». - Пермь, 2017. - № 12. - 74 с.

22) Лушников, Н.Д. Современные технические средства борьбы с хакерскими атаками / Н.Д. Лушников, А.Д. Альтерман // Международный научный журнал «Инновационное развитие». - Пермь, 2017. - № 12. - 80 с.

23) Львович И.Я. Применение методологического анализа в исследовании безопасности / И.Я. Львович, А.А. Воронов // Информация и безопасность. 2017. – 470с.

24) Мищенко, Е.С. Организационные структуры управления (современное состояние и эволюция): учебное пособие / Е.С. Мищенко. – Тамбов: Изд-во ГОУ ВПО ТГТУ, 2018. – 104 с. – 450 экз.

25) Нойкин, С.А. Анализ и оценка внешней среды организации /С.А. Нойкин // Вестник Пензенского государственного университета. - 2017. - №3(11). - С. 44-49.

26) Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2016. - 304 с.

27) Солдатов М.А., Анализ угроз информационной безопасности. Теория и практика экономики и предпринимательства / Солдатов М. А., Бойко Е. В. – М., 2016 – 272с.

28) Торокин А.А. Инженерно-техническая защита информации // М.: Гелиос АРВ, 2016 г. - 958 с.

29) Трофимова, Н.О. Анализ угроз информационной безопасности. Экономика и социум / Трофимова, Н. О., Фахрутдинова, И. Р // М., 2016 – 556с.

30) Хорев А. А. Способы и средства защиты информации: учеб. пособие // М.: МО РФ, 2017г.

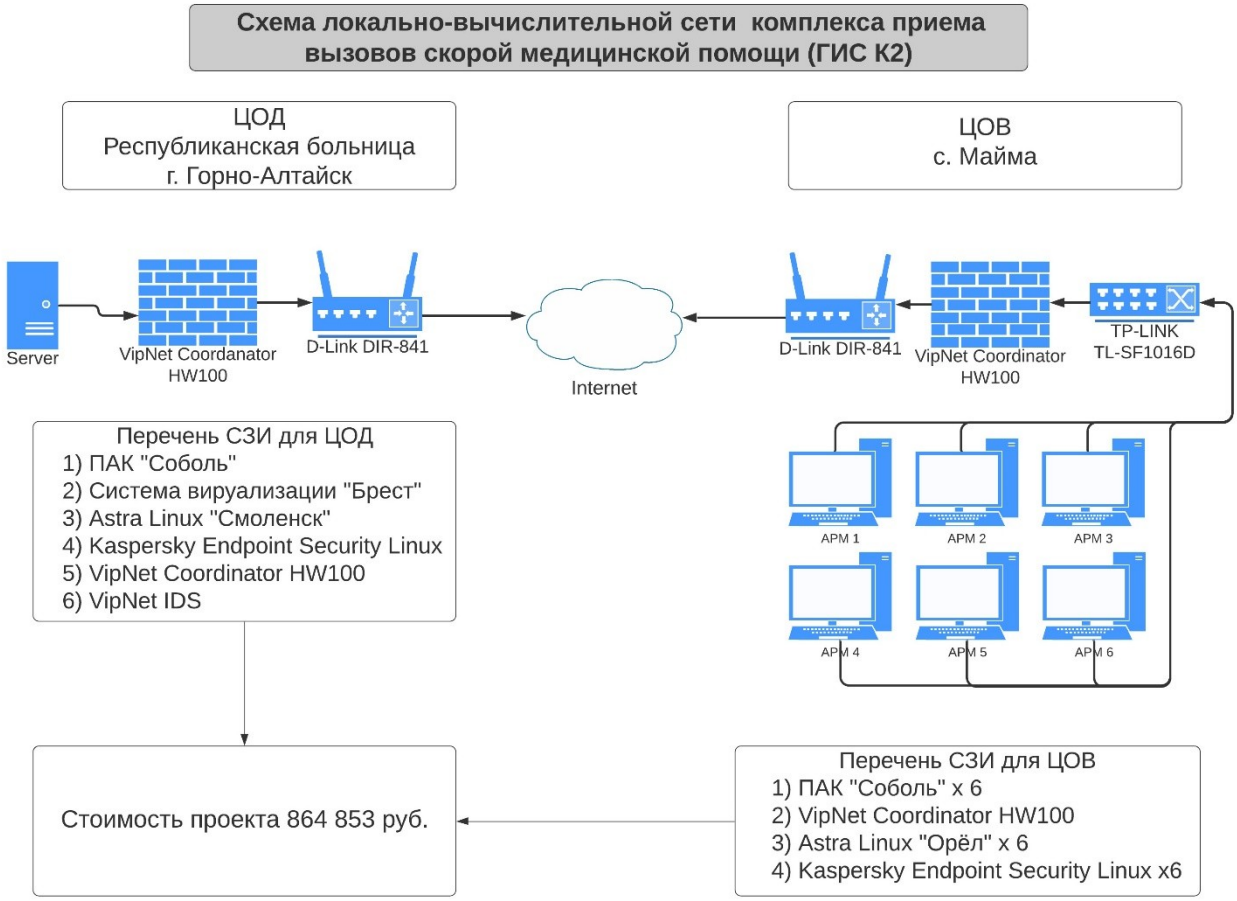
31) Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. - М.: Форум, Инфра-М, 2018. - 416 с.

32) Эпельфельд И.И., Сухотерин А.И. Рекомендации по внедрению защищенного документооборота на предприятии // Ресурсам области - эффективное использование / Сборник материалов XV Ежегодной научной конференции студентов Финансово-технологической академии. Часть 1. - Королёв: Финансово, 2017. - С. 175-183.

33) Электронный ресурс. Научная электронная библиотека. http://www.elibrary.ru

34) Электронный ресурс. Национальный открытый Универсистет НОУ «ИНТУИТ». http://www.intuit.ru/.

## Приложение А. Общая схема локально-вычислительной сети ЦОВ



## Приложение Б. Модель угроз ЦОВ в с. Майма Республики Алтай

| Наименование угрозы | Вероятность реализации угрозы | Возможность реализации угрозы | Опасность угрозы | Актуальность угрозы | Меры по противодействию угрозе | |
|---|---|---|---|---|---|---|
| | | | | | Технические | Организационные |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1. Угрозы от утечки по техническим каналам | | | | | | |
| 1.1. Угрозы утечки акустической информации | Маловероятна | Средняя | Низкая | Неактуальная | | Изучение инструкции пользователя Изучение технологического процесса |
| 1.2. Угрозы утечки видовой информации | Маловероятна | Низкая | Низкая | Неактуальная | Жалюзи на окна. Расположение монитора | Изучение инструкции пользователя Изучение технологического процесса |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Маловероятна | Низкая | Низкая | Неактуальная | | |
| 2. Угрозы несанкционированного доступа к информации | | | | | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств АИС «ЦОВ» носителей информации путем физического доступа к защищаемой информации. | | | | | | |
| 2.1.1. Кража ПЭВМ | Маловероятна | Низкая | Низкая | Неактуальная | | |
| 2.1.2. Кража носителей информации | Маловероятна | Низкая | Низкая | Неактуальная | Хранение в сейфе Шифрование | Пропускной режим. Охрана. Акт установки |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | данных | средств защиты. Учет носителей информации. Изучение инструкции пользователя |
| 2.1.3. Кража ключей доступа | Маловероятна | Низкая | Низкая | Неактуальная | Хранение в сейфе | Изучение инструкций |

Продолжение Приложения Б

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 2.1.4. Кражи, модификации, уничтожения информации. | Маловероятна | Низкая | Низкая | Неактуальная | Шифрование данных Система защиты от НСД | Пропускной режим Охрана Акт установки средств защиты |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Маловероятна | Низкая | Низкая | Неактуальная | | Пропускной режим Охрана |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Маловероятна | Низкая | Низкая | Неактуальная | Шифрование данных | Ремонт допущенными сотрудниками |
| 2.1.7. Несанкционированное отключение средств защиты | Низкая вероятность | Средняя | Низкая | Неактуальная | Настройка средств защиты | |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий); | | | | | | |
| 2.2.1. Действия вредоносных программ (вирусов) | Низкая вероятность | Средняя | Низкая | Неактуальная | Антивирусное ПО Kaspersky Endpoint Security 11 | Изучение инструкции пользователя Изучение инструкции ответственного |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | Изучение инструкции администратора безопасности Изучение технологичес кого процесса обработки |

Продолжение Приложения Б

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 2.2.2. Недекларированн ые возможности системного ПО и ПО для обработки персональных данных | Маловероятна | Низкая | Низкая | Неактуал ьная | Настройка средств защиты | Приобретение у доверенной организации |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | Средняя вероятность | Средняя | Низкая | Неактуал ьная | Настройка средств защиты | Изучение инструкции пользователя Изучение инструкции ответственног о Изучение инструкции администратор а безопасности Изучение инструкции технологическ ого процесса обработки |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования АИС «ЦОВ» и СЗ в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | | | | | |
| 2.3.1. Утрата ключей и атрибутов доступа | Средняя вероятность | Средняя | Низкая | Неактуал ьная | Хранение в сейфе | Изучение инструкции пользователя Изучение инструкции администратор а безопасности |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | Просмотр журнала учета паролей |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | Высокая вероятность | Высокая | Низкая | Актуальная | Настройка средств защиты | Инструкция пользователя |

Продолжение Приложения Б

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 2.3.3. Непреднамеренное отключение средств защиты | Маловероятна | Низкая | Низкая | Неактуальная | Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности Настройка средств защиты | Изучение инструкции пользователя Изучение инструкции администратора безопасности Изучение инструкции по антивирусной защите |
| 2.3.4. Выход из строя аппаратно-программных средств | Средняя вероятность | Средняя | Низкая | Неактуальная | | Следить за состоянием программно-аппаратных средств |
| 2.3.5. Сбой системы электро-снабжения | Маловероятна | Низкая | Низкая | Неактуальная | Использование источника бесперебойного электропитания | |
| 2.3.6. Стихийное бедствие | Маловероятна | Низкая | Низкая | Неактуальная | Пожарная сигнализация | Изучение инструкции по действиям в случае возникновения нештатной |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | ситуации |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | | | | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке | Маловероятна | Низкая | Низкая | Неактуальная | Шифрование данных. Система защиты от НСД | Акт установки средств защиты Разрешительная система допуска Изучение технологического процесса обработки |

Продолжение Приложения Б

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | Маловероятна | Средняя | Средняя | Актуальная | | Обязательство о не разглашении Изучение инструкции пользователя |
| 2.5. Угрозы несанкционированного доступа по каналам связи | | | | | | |
| 2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из АИС «ЦОВ» и принимаемой из внешних сетей информации: | | | | | | |
| 2.5.1.1. Перехват за переделами с контролируемой зоны; | Маловероятна | Низкая | Низкая | Неактуальная | VPN соединение | |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями; | Маловероятна | Низкая | Низкая | Неактуальная | | Пропускной режим Охрана |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | Маловероятна | Низкая | Низкая | Неактуальная | | Пропускной режим Охрана. |
| 2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций АИС, | Высокая вероятность | Высокая | Низкая | Актуальная | Корректная настройка FireWall | |

| | | | | | | |
|---|---|---|---|---|---|---|
| топологии сети, открытых портов и служб, открытых соединений и др. | | | | | | |
| 2.5.3. Угрозы выявления паролей по сети. | Маловероятна | Низкая | Низкая | Неактуальная | VPN соединение | |
| 2.5.4. Угрозы навязывание ложного маршрута сети. | Маловероятна | Низкая | Низкая | Неактуальная | VPN соединение, FireWall | |

Продолжение Приложения Б

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 2.5.5. Угрозы подмены доверенного объекта в сети. | Маловероятна | Низкая | Низкая | Неактуальная | VPN соединение | |
| 2.5.6. Угрозы внедрения ложного объекта как в АИС, так и во внешних сетях. | Маловероятно | Низкая | Низкая | Неактуальная | VPN соединение | |
| 2.5.7. Угрозы типа «Отказ в обслуживании». | Маловероятно | Низкая | Низкая | Неактуальная | FireWall | |
| 2.5.8. Угрозы удаленного запуска приложений. | Маловероятно | Низкая | Низкая | Неактуальная | VPN соединение, FireWall | |
| 2.5.9. Угрозы внедрения по сети вредоносных программ. | Маловероятно | Низкая | Низкая | Неактуальная | Антивирусное ПО Kaspersky Endpoint Security 11 | |