МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование кафедры)

09.03.03 Прикладная информатика
(код и наименование направления подготовки, специальности)

Бизнес-информатика
(направленность (профиль)/специализация)

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка комплекса мероприятий по обеспечению информационной безопасности для ООО «ОРП-Ростов»

Студент(ка) И.А. Макалов _____
(И.О. Фамилия) (личная подпись)

Руководитель О.В. Аникина _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий
кафедрой к.т.н., доцент, А.В. Очеповский _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____2019 г.

Тольятти 2019

АННОТАЦИЯ

Тема: «Разработка комплекса мероприятий по обеспечению информационной безопасности для ООО «ОРП-Ростов»».

Ключевые слова: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ СИСТЕМА, ЗАЩИТА ИНФОРМАЦИИ.

Объектом исследования является общество с ограниченной ответственностью ООО «ОРП-Ростов». Предметом исследования информационная безопасность организации. Целью работы стала разработка комплекса мероприятий для повышения уровня информационной безопасности ООО «ОРП-Ростов».

Работа состоит из трех глав. В первой главе проводится анализ существующего положения с обеспечением информационной безопасности в компании, выявляются основные информационные активы, подлежащие защите, угрозы, уязвимости, формулируются методы, применяя которые можно достичь повышение информационной безопасности ИС компании.

Во второй главе обосновывается выбор методов и средств защиты информации, выбираются конкретные организационные и программные средства защиты информации.

В третьей главе выбирается методика оценки экономической эффективности предлагаемых к внедрению мер, проводится расчет конкретных показателей и срока окупаемости, а так же проводится проводится анализ уровня защищённости после внедрения комплексных мер.

Работа включает: страниц 68 с приложениями, рисунков 7, таблиц 9, источников 28.

ОГЛАВЛЕНИЕ

Введение

Проблема обеспечения информационной безопасности долгие годы является одним из важнейших вопросов для современных организаций.

Базовые идеи современных ИТ основаны на концепции, которая определяет организованность данных, а базах таким образом, чтобы они могли адекватно отображать изменяющийся мир и соответствовать информационным потребностям пользователей.

Любую систему можно представить в виде программного комплекса, который имеет функции поддержки надежного хранения данных в памяти ПК, выполнении специфических для каждого приложения преобразований и вычислений, предоставление пользователю удобного и понятного интерфейса.

Сейчас в странах с развитой финансовой структурой уже давно используются устойчивые традиции и направления в финансовой IT-сфере, которые направлены на оптимальное ведение бизнеса. Применение новейших технологий в области анализа данных становится в настоящее время общепринятой основой для реализации управленческих решений. Это дает возможность не только развивать ИС в сторону передовых стандартов, но и значительно изменять структуру и способы реализации бизнеса. Качественные изменения методов реализации бизнеса предъявляют обновлённые требования как к ПО, так и к создаваемым ИС.

В процессе подготовки концепции управления и подборе начальных средств предпочтительно применять и брать во внимание применяемые международные стандарты и рекомендации в анализируемой области. Эти стандарты суммируют уже полученный опыт управления глобальными, локальными сетями и интерсетями, на их базе выделяют главные функциональные области сетевого управления, выражают архитектуру, БД и протоколы сетевого управления. Применение стандартных методов и средств управления помогает гарантировать слаженность работы аппаратно-программных средств, созданных разными компаниями.

Целью данной работы является проведение комплекса мероприятий в целях повышения уровня информационной безопасности для ООО «ОРП-Ростов». В работе рассмотрена разработка привилегий с точки зрения внедрения организационных мероприятий и аппаратного-программного комплекса, так как только комплексное применение различных методов может дать удовлетворительный результат.

Данная работа рассматривает уязвимости информационных активов ООО «ОРП-Ростов» при реализации различных угроз.

Последствиями реализации угроз могут стать как крупные финансовые убытки так и подпорченная репутация компании.

Для осуществления поставленных целей необходимо решить следующие задачи:

- определить существующие риски и угрозы информационной безопасности, выделить информационные активы компании;
- оценить и выбрать наиболее важные и ценные информационные активы, а также наиболее серьёзные угрозы и уязвимости;
- оценить существующую систему защиты и сделать вывод о необходимости повышения уровня защищенности;
- определить конкретные меры, программные, аппаратные и организационные;
- оценить экономическую эффективность проведения мероприятий.
- провести оценку защищённости ИС после внедрения комплекса мер;

Объектом исследования является ООО «ОРП-Ростов», а предметом исследования является информационная безопасность компании.

Выпускная квалификационная работа состоит из трех глав.

В первой главе анализируется деятельность компании, выявляются информационные активы, подлежащие защите, риски и угрозы информационной безопасности. Рассматривается существующая система

информационной безопасности, производится выбор комплекса задач и определение организационных и инженерно-технических мер.

Во второй главе приведена правовая основа обеспечения ИБ, организационно-административные меры, описана структура программно-аппаратного комплекса.

В третьей главе оценена экономическая эффективность внедрения разработанной системы и срок ее окупаемости.

Глава 1 Анализ системы зашиты в компании

1.1 Краткая характеристика компании и ее локальной вычислительной сети

ООО «ОРП-Ростов» является коммерческой организацией.

Основным видом деятельности является «Аренда и управление собственным или арендованным нежилым недвижимым имуществом», зарегистрировано 6 дополнительных видов деятельности.

Арендаторами ООО «ОРП-Ростов» являются как продуктовые сети, так организации занимающиеся дистрибуцией, логистические компании, небольшие юридические бюро, и даже частные охранные предприятия.

Организационная форма структуры управления ООО «ОРП-Ростов» приведена на рисунке 1.1.

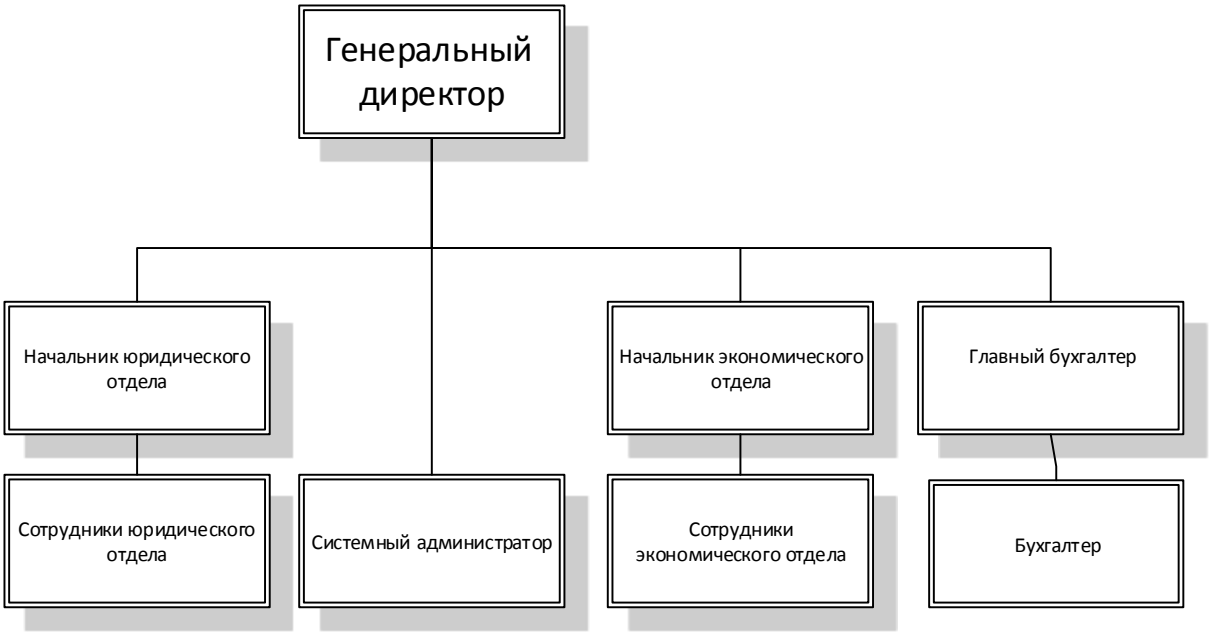

Рисунок 0.1 - Организационная структура ООО «ОРП-Ростов»

В соответствии с должностными инструкциями, генеральный директор организации:

- производит руководство организацией, в рамках законодательства действующего в Российской Федерации, неся полную ответственность за последствия принимаемых им решений, целостность и эффективное пользование имуществом ООО «ОРП-Ростов», следит за течением основных

бизнес-процессов , корректируя при необходимости деятельность сотрудников и других факторов влияющих на ключевые для организации процессы.

Определяет направления развития организации, оптимизирует бизнес-процессы, представляет компанию перед лицом клиентов и представителей власти.

Начальник юридического отдела имеет право:

- используя доверенность, представлять интересы ООО «ОРП-Ростов» в любых государственных или негосударственных предприятиях, учреждениях, коммерческих или нет организациях;
- вносить предложения в части Юридического обеспечения на рассмотрение генерального директора;
- запрашивать от подразделений фирмы и иных специалистов информацию или документы, необходимую для деятельности Юридического отдела.

А так же руководит деятельностью юридического отдела, обязательно присутствует на всех деловых встречах.

Главный бухгалтер – занимается учётом материальных и финансовых активов организации, хозяйственных, расчётных и кредитных операций, взаимодействует с обслуживающими организацию банками, расчётом и выплатой существующих налоговых сборов, расчётом и планированием доходов и расходов, анализирует качественные показатели деятельности организации, формирует и представляет по запросу генерального директора отчёты отражающую деятельность организации в финансовых и хозяйственных вопросах, участвует в сделках с клиентами как лицо ответственное за своевременное исполнение обязательств обоих сторон, рассчитывает и производит начисление заработной платы сотрудникам, руководит сотрудниками бухгалтерии и кассы, несет ответственность за сохранность материальных ценностей организации, регулярно организуя проверки соответствия описей действительности.

Работа экономиста заключаются в повышении эффективности, производительности и рентабельности деятельности организации. Заботиться о мероприятиях по снижению себестоимости услуг. Постоянно анализирует финансовые показатели организации, основываясь на этом, выносит предложения по увеличению прибыли. Изучает ситуацию на как мировом рынке так и на внутреннем рынке, прогнозируя повышение или снижение цен. Основываясь на показателях полученных в ходе анализа рынков принимает непосредственное участие в ценообразовании услуг представляемых организацией.

Системный администратор - занимается автоматизацией деятельности организации, контролем за работой компьютеров и оргтехники, контролирует работу вычислительной сети организации, следит за различными системами в том числе за системой резервного копирования данных, системой удаленного доступа, базами данных организации, добавляет, редактирует, удаляет учетные записи сотрудников, системой видеонаблюдения, взаимодействует со сторонними организациями поставляющими доступ в интернет, обслуживающими оргтехнику, вносит предложения по оптимизации работы с помощью информационных технологий, ведет учит выданных сотрудникам ноутбуков, а так же обеспечивает информационную безопасность предприятия, контроль доступа сотрудников к ресурсам сети интернет.

Информационная система в части программного обеспечения реализована на платформе Microsoft Windows , как в серверной так и в клиентской части.

Автоматизация работы подразделений организована с помощью с программных продуктов: «1С-Бухгалтерия», «1С-Предприятие», «СБИС ++ Электронная отчетность», «Недвижимость-Эксперт», пакета Microsoft Office 2010 (Acces,Word, Exel, Outlook), продуктами «Гарант» и «Консультант+», а так же множества других программных продуктов. На каждую программу обязательно имеется лицензия (за исключением открытого, свободно распространяемого).

Серверная часть расположена в отдельном помещении, в связи с сильной теплоотдачей оборудования подходящая температура в данном помещении поддерживается с помощью мощной сплит-системы, что обеспечивает стабильную работу серверного оборудования. На случай выхода из строя основной сплит-системы в серверной установлена резервная.

В серверной расположены пять системных блоков выполняющих следующие функции:

- контроллер домена+DHCP сервер (для обеспечения аутентификации пользователей, создание и применения единых политик безопасности, а также для автоматического присвоения необходимых параметров вновь подключенным в вычислительную сеть организации устройствам) (i7, 4 GB RAM, 512 GB HDD, Windows Server 2012);
- SQL-сервер (База данных организации, используется при работе таких программных продуктов как «1С-Предприятие», «1С-Бухгалтерия» а также как хранилище всей учетной информации связанной с деятельностью организации Xeon, 16 GB RAM, 512 GB HDD, Windows Server 2012);
- файловый сервер (каждый сотрудник имеет доступ к определенной части файлового хранилища, защищенной от несанкционированного доступа) (i3, 8 GB RAM, 2 TB HDD, Windows Server 2012);
- сервер безопасности (в организации используется антивирусные средства от «Лаборатории Касперского», межсетевой экран microsoft ISA сервер) (i3, 8 GB RAM, 1 TB GB HDD, Windows Server 2012);
- почтовый сервер «Microsoft Exchange 2012», для обмена электронной почтой как внутри организации так и со всем миром, Xeon, 16 GB RAM, 512 GB HDD);
- сетевое оборудование. Коммутаторы, маршрутизатор, WI-FI точка доступа (для обеспечения беспроводного доступа к сети организации);
- множество источников бесперебойного питания разной мощности, обеспечивающих бесперебойную работу серверов при кратковременном

отключении электроэнергии а так же возможность безопасного завершения их работы если решение проблем с электроэнергией потребует много времени.

Но несмотря на достаточное количество источников бесперебойного питания приостановка деятельности организации в связи с отключением электроэнергии достаточно убыточна, потому в обязанности системного администратора в ООО «ОРП- Ростов» входит аварийное восстановление электроэнергии с помощью генератора работающего на бензине мощностью достаточной для обеспечения работы серверной и ключевых сервисов организации.

В случае отсутствия интернет соединения множество бизнес процессов организации проходят затруднительно, и организация несет крупные убытки. По этой причине ООО «ОРП-Ростов» имеет подготовленный, заранее оплаченный резервный интернет канал, использующий другую магистраль, и предоставляемый иным интернет провайдером. В случае потери соединения основным каналом более чем на одну минуту, сетевое оборудование настроенное специальным образом автоматически перенаправляет весь трафик на резервный канал.

В качестве клиентских, используемых на рабочих местах сотрудников организации используются стационарные компьютеры, состоящие из:

- системного блока Intel Core i3, 4 GB RAM, 256 GB SSD);
- монитор ЖК Acer 17 дюймов;
- стандартная клавиатура;
- оптическая мышь.

Все рабочие места подключены к единой локальной вычислительной сети, а также имеют доступ к сети интернет.

Кроме того, для возможности работы сотрудников вне офиса в организации используются ноутбуки и планшетные компьютеры, организация не использует технологию виртуальных частных сетей, а значит мобильные рабочие станции не имеют доступа к вычислительной сети организации.

1.2 Анализ рисков информационной безопасности

1.2.1 Идентификация и оценка информационных активов

В ООО «ОРП- Ростов» можно выделить данные виды активов:

– информационные (финансовые показатели, базы данных, персональные данные сотрудников);

– физические (компьютеры, персонал, документы в печатном виде, периферийные устройства, серверное оборудование,);

– активы ПО (программное обеспечение).

Обязательной защите должны подлежать следующие активы:

– компьютеры сотрудников;

– базы данных;

– документация;

– персональные данные сотрудников;

– серверное оборудование;

– программное обеспечение.

Оценку по информационным активам организации представим в виде таблицы в Приложении 1.

К сведениям конфиденциального характера (на основании Указа Президента Российской Федерации от 6 марта 1997 года № 188 [1]) относятся:

1. сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2. сведения, составляющие тайну следствия и судопроизводства;

3. служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

4. сведения, связанные с профессиональной деятельностью, доступ к которой ограничен в соответствии с Конституцией Российской Федерации и федеральными законами;

5. сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

6. сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

Перечень сведений конфиденциального характера, ограничение доступа к которым определяется действующим законодательством РФ, сведен в таблицу Приложения 2.

Результаты анализа ценности информационных активов представлены в таблице (табл. 1.1)

Таблица 0.1 - Результаты анализа ценности информационных активов

Актив	**Ценность (от 1 до 5)**
Серверы	5
Клиенты (компьютеры сотрудников)	4
Реляционные БД	3
Персональные данные сотрудников	2
Документы	1

Информационные активы, имеющие наибольшую ценность:

- серверы;
- компьютеры сотрудников;
- реляционные БД;
- персональные данные сотрудников;
- документы.

Таким образом, наиболее важной информацией является информация, формируемая в результате коммерческой деятельности компании.

1.2.2 Оценка уязвимостей и угроз активов

Понятие «уязвимость» относится к атрибутам актива а так же к его свойствам, имеющим возможность быть использованными каким либо образом или для других целей, чем цели или свойства, для которых существовал данный актив.

Укажем степень оценки вероятности возможной реализации отмеченных уязвимостей (таблица Приложения 3).

Под угрозой информационной безопасности (ИБ) понимается совокупность условий и факторов, создающих потенциальную опасность, основанную на утечке информации, несанкционированным или непреднамеренным доступом к ней.

В общем случае угроза ИБ может характеризоваться следующими параметрами:

- источник угрозы;
- используемая уязвимость;
- способ реализации угрозы;
- деструктивные действия, выполняемые при реализации угрозы.

Основные виды угроз, существующие в компании, приведены в таблице Приложения 4.

Проведем анализ выполнения основных мероприятий по защите информационных ресурсов (табл. 1.2).

Таблица 0.2 - Анализ выполнения основных мероприятий по защите информационных ресурсов

Виды деятельности по организации системы защиты информации	**% выполнения**
Выполнение требования по должному уровню защиты информации пользователей ИС компании	50%
Формирование всех видов защиты информации в целях сохранения	

Виды деятельности по организации системы защиты информации	% выполнения
коммерческой тайны	30%
Улучшение системы защиты документооборота с целью исключения случаев НСД	90%
Запрет НСД к информации, включенной в реестр документов, содержащих коммерческую тайну	50%
Получение информации о возможных методах и способах выявления слабых мест в информационной системе компании с целью получения НСД к передаваемой информации	50%
Устройство контроля зоны помещений, в которых может находиться защищаемая информация	30%

Исходя из приведенной в таблице информации можно сделать вывод, что необходимо улучшать и оптимизировать систему защиты информации по всем направлениям, в том числе с помощью организационных, программно-аппаратных и технических методов.

Это означает необходимость в проведении комплекса мероприятий направленных на повышение уровня ИБ существующей системы, где будет затронуты всё перечисленные направления мер по обеспечению информационной безопасности ООО «ОРП-Ростов».

Сегодня существует множество методик и способов защиты конфиденциальной информации от несанкционированного или случайного доступа посторонних, рассмотрим самые популярные:

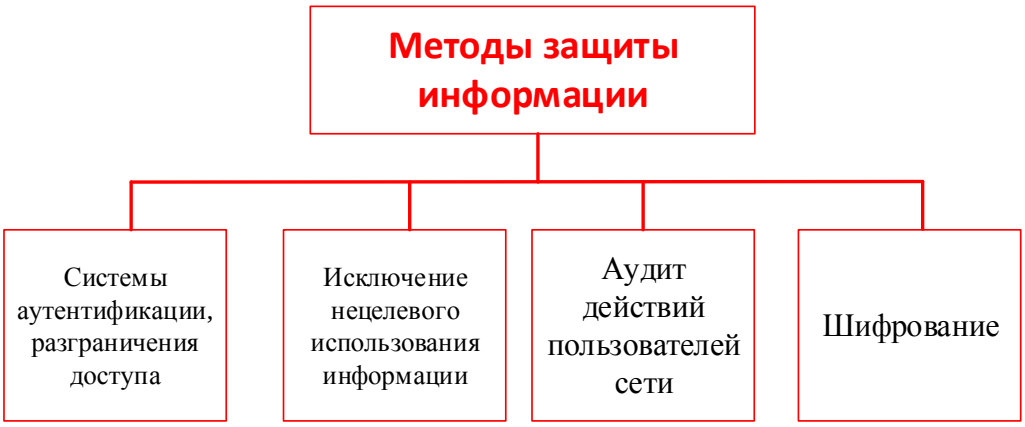

Рисунок 0.2 - Методы защиты конфиденциальной информации от несанкционированного или случайного доступа

- системы аутентификации, разграничения доступа;
- исключение нецелевого использования информации;
- постоянный аудит действий всех без исключения пользователей;
- шифрование информационных активов.

Система современных методов защиты данных вкратце выглядит следующим образом:

1. средства предохранения от противоправного подступа к информации, вот некоторые из них:

- авторизация как процесс проверки возможности пользователя выполнить действие, например, войти в систему;
- ограничение к управлению созданными ресурсами;
- предоставление доступа строго ограниченному кругу пользователей;
- аудит как фиксация всех действий пользователя с помощью специального протокольного Журнала. Это может помочь при восстановлении утраченных или атакуемых файлов.

2. системы наблюдения в сети:

- системы распознавания вторжений (специальное ПО отслеживает малейшие попытки несанкционированного доступа к закрытым данным);

- системы предотвращения передачи закрытых данных - когда происходит попытка утечки информации за пределы охраняемой системы, эти действия автоматически блокируются.

3. распознаватели протоколов, включая IP-мониторинг;

4. антивирусное программное обеспечение;

5. методы криптографии, включающие в себя шифрование для трансформации доступных данных в закрытые и наоборот и цифровую подпись. Последняя предназначена для проверки отсутствия изменений в электронном документе, причем американские и российские стандарты электронной подписи несколько разнятся;

6. возможности создания дополнительных копий информации;

7. использование источников бесперебойного питания и генераторов напряжения тока;

8. аутентификация («authorization – function of access to any resources» [9, 26 p.]) пользователя, то есть проверка на основе пароля, специального ключа доступа, сертификата или биометрии оснований доступа индивидуума к закрытой информации.

Некоторые из описанных выше методов и средств существуют уже более 10 лет, другие появились совсем недавно, но все они находятся в постоянном развитии, становясь все более чувствительными к тем или иным попыткам незаконного доступа. Конечно, только совокупность всех этих мер может обеспечить надежный барьер от утечки информации или технической поломки её носителя.

1.2.3 Оценка рисков

Результатный уровень информационной безопасности в итоге определяется как сумма всех рисков, актуальных для информационных активов и применяемых средств защиты информации.

Риски для рассматриваемых активов могут быть разными по своей природе, методам реализации и степени опасности, соответственно, для минимизации таких рисков могут применяться различные средства.

Риски можно классифицировать по следующим основаниям:

- повторяемые с какой-либо периодичностью риски, являющиеся связанными со средой работы информационной системы;
- разовые риски, возникающие в ходе ежедневной работы информационной системы и использования информационных активов.

Контроль рисков, как правило, осуществляется административными мерами и средствам и вынесен на уровень управления системой защиты информации, что требует применения специального программного обеспечения.

Контроль рисков, как и подготовка личной политики ИБ, актуальны для фирм, где анализ данных ведется нестандартными методами. Типичной фирме будет достаточно и классических мер ИБ, определенных в рамках изучения исследования классических рисков или без исследования вообще (актуально исходя из описанного выше законодательство РФ по этому вопросу).

Использование ИС заключено в группе рисков. Когда возможная угроза не так обширна, важно использовать точные и правильные методики защиты. Таким образом оценка рисков имеет ключевую роль в проектировании систем информационной безопасности.

Суть оценки возможных рисков основана на шкале, в которой отдельный риск соответствует имеющемуся уровню наличия каких либо угроз информационным активам.

Для получения ключевой оценки используется шкала критичности, включающую в себя три положения: низкий, высокий, средний. При использовании данного метода оценка каждого уровня формируется в рамках определённых уровней критичности для определённого актива, к примеру:

- активы данных можно оценить зная уровень нанесения возможного нанесения ущерба организации от умышленного или случайного несанкционированного к ним доступа, изменения или отсутствия к ним доступа в течение некоторого времени;

• ПО, материалы и сервисы оцениваются исходя из работоспособности и доступности. И тут важно выразить, какой уровень проблем получает фирма, если нарушается работа конкретного или нескольких этих активов. К примеру: остановка системы вентиляции после 3 суток приведет к поломке серверного оборудования компании, они потеряют доступ, и компания понесет убытки;

Пользователи ИС компании могут рассматриваться как имеющие различные уровни доступа к системе и информационным активам, следовательно, могущие в различной степени влиять на сохранность и доступность данных.

Сохранность данных в компании является частью ее репутации и является одним из влияющих факторов на ее деловую активность. При нарушении системы защиты информации уровень деловой репутации также может быть снижен.

Риски оцениваются в ходе комплексной оценки системы защиты информации и являются одним из важнейших составляющих такой оценки. Значение риска высчитывается как некоторый показатель, связанный со степенью важности имеющихся угроз и вероятностью их реализации.

Степень риска может зависеть от ценности информационного актива, вероятности реализации угроз, скорости внедрения средств защиты информации при обнаружении риска, актуальных и доступных методик защиты, которые в силах минимизировать уязвимость, угрозы и воздействия.

Ценность каждого актива отражается в рамках личной оценки владельца, а также ИТ-специалиста, который отвечает за ИБ. Возможные уязвимости всегда известны самому IT-специалисту.

Сейчас имеется ряд методик оценки рисков. И лучше всего, чтобы фирма сама применяла более доступных и удобный метод, который имел бы некий результат.

Процесс оценки риска идет экспертным методом, базируясь на изучении ценности актива, доступности внедрения самих угроз и уязвимостей, которые описаны в пунктах ниже.

В ситуации, когда уровень доступности актива для их нарушения выявлен в результате аудита информационной безопасности или оценки процессов, возникающих в ходе защиты информации, степень угрозы может быть подсчитана по каждому выявленному активу.

Далее, при вычислении уровня риска информационной безопасности для каждого из выявленных активов и каждой угрозы потребуется мнение эксперта, который может внести свои коррективы на основании имеющегося опыта.(Табл. 1.3).

Таблица 0.3 - Результаты оценки рисков информационным активам организации

Риск	Актив	Ранг риска
Кража	Серверное оборудование	5
Проникновение, в обход существующей системы разграничения доступа	База данных	6
Ненадлежащий надзор или его отсутствие за работой посторонних лиц (например уборщиц)	База данных	6
Неисправности аппаратного обеспечения	База данных	6
Проникновение, в обход существующей системы разграничения доступа	Серверы	4
Неисправности аппаратного обеспечения	Серверы	3
Ненадлежащий надзор или его отсутствие за работой посторонних лиц (например уборщиц)	База данных	4
Неисправности аппаратного обеспечения	Программное обеспечение	6

Риск	Актив	Ранг риска
Ненадлежащий надзор или его отсутствие за работой посторонних лиц (например уборщиц)	Документы	6
Кража	АРМ сотрудника	3
Проникновение, в обход существующей системы разграничения доступа	АРМ сотрудника	4
Неисправности аппаратного обеспечения	АРМ сотрудника	5
Проникновение, в обход существующей системы разграничения доступа	Программное обеспечение	6
Проникновение, в обход существующей системы разграничения доступа	Документы	5
Неисправности аппаратного обеспечения	Документы	3

Из таблице 1.3 становится ясно, какие задачи, необходимо решить в целях обеспечения информационной безопасности:

– обеспечение безопасности деятельности сотрудников;

– организация проведения мероприятий по организационной, и технической защите коммерческой тайны;

– контроль доступа, исключения нежелательного или умышленного доступа посторонних к конфиденциальной информации;

– поиск и нейтрализация уязвимостей информационной системы;

– организация охраны территории, зданий помещений, с защищаемой информацией.

Таким образом. для решения проблемы повышения информационной безопасности необходимо решить комплекс задач.

1.3 Обоснование необходимости проведения мероприятий по совершенствованию системы информационной безопасности

Исходя из ранее выполненного объема работ по выявлению информационных активов, рисков и угроз, а также степени соотношения между ними в данной компании, можно выявить следующие факторы негативно влияющие на защищённость информационных активов ООО «ОРП-Ростов», требующие проведения мероприятий по их устранению:

1. недостаток или неполная реализации организационных мер, включая регламенты действий сотрудников при использовании информационных активов, работы в информационной системе компании;
2. отсутствует контроль целостности;
3. не используются межсетевые экраны (система не защищена от «сетевых атак»);
4. данные между филиалами передаются по открытым каналам, без использования VPN (а значит без шифрования);
5. используется не защищённая электронная почта (возможен перехват или подмена данных в сообщениях);
6. отсутствует система разграничения полномочий (любой пользователь имеет доступ к файлам других сотрудников);
7. используемое антивирусное ПО не обладает функцией «защиты от несанкционированной активности приложений»;
8. внутренний сетевой трафик не шифруется;
9. имеется возможность подключения любых носителей информации.

Схематично недостатки приведены на рисунке 1.3.

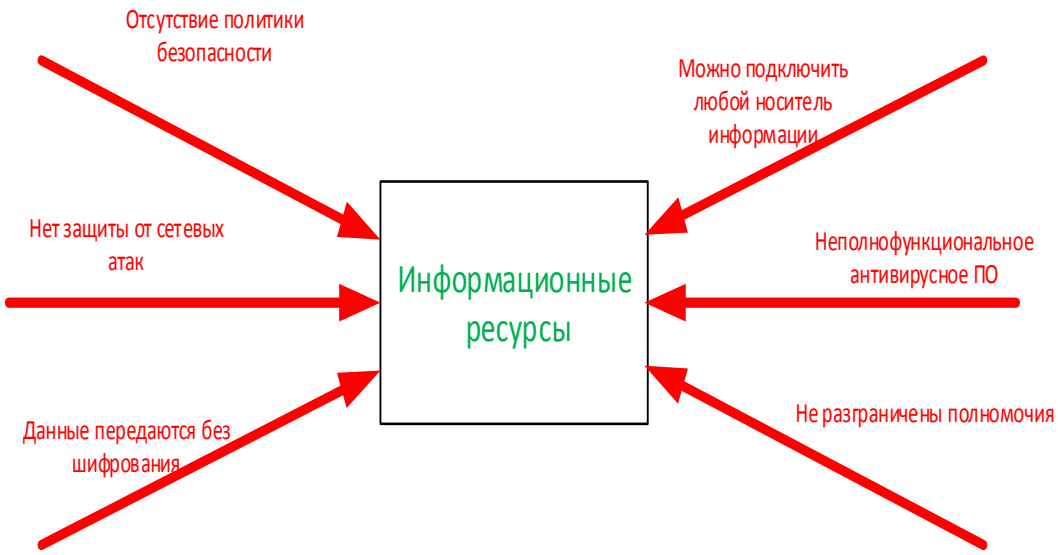

Рисунок 0.3 - Существующие недостатки системы ИБ

Исходя из перечня недостатков существующей системы информационной безопасности, в первую очередь необходимо устранить все возможности для получения несанкционированного доступа к информационным активам компании, подлежащим защите.

Вывод по первой главе

В первой главе выпускной квалификационной работы подробным образом рассмотрены все аспекты организации и обеспечения безопасности информационных систем компаний и вычислительных сетей как их составляющих. Проведён анализ основных целей, задач и принципов обеспечения безопасности информации, прежде всего к ним отнесены ограничение доступа к конфиденциальности информации и обеспечение целостности данных.

В результате разработки модели нарушителя безопасности локальной вычислительной сети определены его классы, дана классификация и описаны возможные используемые средства для получения несанкционированного

доступа. В результате анализа модели угроз локальной вычислительной сети показано, что основными методами реализации угроз являются такие, как сканирование сети, анализ сетевого трафика, выявление пароля, подмена доверенного объекта сети, внедрение ложного объекта сети, навязывание ложного маршрута сети, отказ в обслуживании, удалённый запуск приложений, вирусные атаки, другие вредоносные программы.

Также в первой главе описаны существующие модели качественного и количественного анализа угроз и рисков информационной безопасности локальной вычислительной сети.

Глава 2 Разработка комплекса мероприятий по обеспечению информационной безопасности

2.1 Выбор организационных мер для обеспечения информационной безопасности

Организационные меры обеспечения безопасности информационных систем предполагают исключительно безопасные методы и способы ведения документации, использование неких методик разработки и принятия программ, а также наличие процедур обработки инцидентов при возможных нарушениях систем безопасности.

Подобный способ обеспечения защиты данных предполагает, что для каждый системы будет разработан механизм ведения деловой деятельности компании, предусматривающий также возможность появления непредвиденных обстоятельств (ликвидацию последствий наращения системы безопасности) и включающий в себя определенную стратегию и некоторый план.

Можно выбрать три стратегии обеспечения ИБ, которые представлены в таблице 1.

Оборонительная стратегия означает, что при исключении вмешательства в процесс функционирования системы есть возможность нейтрализовать лишь наиболее опасные угрозы. Обычно это возможно благодаря построению защитной оболочки, которая подразумевает создание новых организационных мер, внедрение программных средств допуска к ресурсам в целом, применение технических средств контроля за доступом к помещениям, в которых находятся сервера и терминалы.

Наступательная стратегия характеризуется активным противодействием неизвестных угрозам, которые так или иначе влияют на безопасность ИС. Такая стратегия может состоять из установки дополнительных программно-аппаратных средств определения пользователей, использование более совершенных технологий разгрузки и восстановления данных, увеличение доступности системы при использовании горячего и холодного резервирования.

Возможно предложить три стратегии защиты информации, представленные в таблице 2.1.

Таблица 0.1 - Стратегии защиты информации

Учитываемые угрозы	Влияние на информационные системы		
	отсутствует	частичное	существенное
Наиболее опасные	Оборонительная стратегия ЗИ		
Все идентифицированные угрозы		Наступательная стратегия ЗИ	
Все возможные			Упреждающая стратегия ЗИ

Упреждающая стратегия предполагает полное исследование всех реальных угроз для системы обработки данных и создание адекватных мер по их нейтрализации еще в процессе проектирование и разработки системы. Главной частью упреждающей стратегии можно назвать оперативный анализ центров исследования проблем ИБ, рассмотрение российского и мирового опыта в отношении этих проблем, а также проведение независимого аудита степени безопасности всех данных компании.

Определение защитной стратегии показывает, что если не брать во внимание вмешательство в процесс работы ИС, то можно устранить лишь самые опасные угрозы. Как правило это можно сделать созданием «защитной оболочки», которая определяет создание дополнительных организационных мер, программных механизмов допуска, к ресурсам ИС, применение технических средств контроля за доступом к помещениям, в которых находятся серверное оборудование и терминалы.

Стратегия наступления предполагает весомое противодействие всем известным угрозам, которые затрагивают ИБ системы. Подобная стратегия обычно подразумевает установку дополнительных аппаратно-программных средств для аутентификации пользователей, реализацию более новых технологий восстановления и загрузки данных, увеличение доступности системы благодаря горячему и холодному резервированию.

Опираясь на уже существующие угрозы, компания занимает оборонительную стратегию.

Организационные методы инженерно-технической защиты данных часто являются некой организационной защитой, основа которой – управление доступом и регламентация. Подобные меры обычно позволяют определить порядок и режимы работы технических средств защиты данных.

Регламентация подразумевает установление территориальных, временных и других режимных ограничений в работе сотрудников компании с техническими средствами, направленными на реализацию системы защиты данных.

Обычно регламентация предусматривает:

- установку границ зон контроля;
- определение в каждой зоне своего уровня защиты;
- описание всей деятельности сотрудников и посетителей (составление распорядка дня, правил поведения в компании и т.п.);
- описание режимов работы технических средств, в т.ч. сбора, обработки, хранения и использования защищаемых данных на персональном компьютере, передачи документов и сбора продукции.

Для примера, в распорядке дня компании всем сотрудникам, которые работают с секретными документами, во избежание незаконного их копирования, определяются правила работы с такими документации после окончания рабочего дня. Пример следующий – установка времени работы с секретными документами в электронном виде на персональном компьютере, в течение которого во избежание утечек данных по каналам передачи данных включается генератор радиопомех.

Управление доступом к данным подразумевает мероприятия, которые могут обеспечить санкционированных доступ к ним людей, сигналов и средств. Оно может включать в себя:

- Определение лиц и обращений;
- Сверку полномочий доступа к защищенной информации;

- Запись всех обращений к защищенным данным;
- Реагирование на обращение к данным.

Определение пользователей, посетителей, сотрудников и обращений по каналам передачи данных используется для повышения надежности распознавания.

Проверка полномочий может включать в себя определение прав тех лиц, которые обратились к данным по каналам передачи информации. Для реализации доступа уровень полномочий не может быть ниже разрешённого. Для обеспечения контроля над прохождением носителей с конфиденциальными данными реализуется регистрация обращений к ним методом записи в карточке, журнале либо на магнитном носителе.

Реакция на любое обращение к данным заключается либо в разрешенном к ней доступе, либо в отказе от него. Отказ может дублироваться включением сигнализации, отправкой оповещение в службу безопасности и правоохранительные органы, задержанием нарушителей при их попытке несанкционированного доступа к защищаемым данным.

Основными организационными мерами обычно являются процесс создания политики ИБ методами разработки новых дополнительных документов, которые бы помогали конкретизировать выполнение некоторых мер обеспечения ИБ в отдельных вопросах и угрозах.

Политика ИБ («security policy – document containing rules and procedures of information security» [15, 17p]) – по сути важный документ, который применяется в системе контроля ИБ (СУИБ) фирмы, также являющийся одним из основных механизмов реализации уровня защищенности.

Базируясь на ISO 17799 («international standard of information and network securiry» [17, 17p]) описанная политика ИБ предполагает причастность руководства к реализации кодхода по отслеживанию ИБ, определению сути ИБ, основных целей и границ действий, включает базисные положения по нахождению механизмов и целей контроля, включающих структерные оценки и контроль всеми рисками.

Основываясь на ISO 27001 политика ИБ становится частью более законченного документа – политики СУИБ, включающей некоторые базисные принципы нахождения целей СУИБ, и описывает основную направленность и принцпиальность деятельности в рамках ИБ, учитывающей требования бизнеса, законы и нормы, а также некие обязательства и критерии подбора рисков.

Политики ИБ и СУИБ фирмы могут включаться в единый документ. При этом создание подобного документа проблематично и ответственно. Ведь политика ИБ должна строиться понятной для персонала и быть полноценной в рвамках всех проблем. Также, исходя из данного документа, будет создаваться и вся ИБ, и он в совю очередь обязан быть всеобъемлющим. Неоднозначные трактовки и упущения могут негативно сказаться в процессе работы СУИБ компании. Сама политика ИБ обязана полностью отвечать нормавм мировых стандартов ISO 17799/27001, и это становится важной частью при прохождении сертифицирования.

Базовой мерой организационной безопасности становится обновление имеющихся политик безопасности путем улучшения документов, которые включали бы полное описание всех мер по ИБ для каждого типа угрозы.

Политику безопасности часто называют основным инструментом в СУИБ фирмы, и часто она становится базовым механизмов системы ИБ в целом.

Основываясь на ISO 17799 описанная политика безопасности включает приверженность руководства и контролирует подход к контролю всей системой, выражает понятие ИБ, а также ее границы и цели, включает все правила для выявления потребности в механизмах контроля, а также оценки рисков и других принципов.

Основываясь на ISO 27001 политика ИБ становится частью более законченного документа – политики СУИБ, включающей некоторые базисные принципы нахождения целей СУИБ, и описывает основную направленность и принцпиальность деятельности в рамках ИБ, учитывающей требования бизнеса, законы и нормы, а также некие обязательства и критерии подбора рисков.

Политики ИБ и СУИБ фирмы могут включаться в единый документ. При этом создание подобного документа проблематично и ответственно. Ведь политика ИБ должна строиться понятной для персонала и быть полноценной в рвамках всех проблем. Также, исходя из данного документа, будет создаваться и вся ИБ, и он в совю очередь обязан быть всеобъемлющим. Неоднозначные трактовки и упущения могут негативно сказаться в процессе работы СУИБ компании. Сама политика ИБ обязана полностью отвечать нормавм мировых стандартов ISO 17799/27001, и это становится важной частью при прохождении сертифицирования.

Отразить политику СУИБ в терминах бизнеса и фирмы, ее нахождения, ресурсов и технологий, которая:

- состоит из базиса для выражения целей и показывает главные принципы и направленность работ в рамках ИБ;
- включает все требования бизнеса, нормативную и законодательную базы, а также имеющиеся обязательства в рамках ИБ;
- включает совокупный стратегический набор контроля рисками в фирме, в рамках которой и происходит внедрение и ведение СУИБ;
- описывает критерии для описания рисков;
- подтверждается администрацией.

Описанная в виде документа политика безопасности подтверждается директором, публикуется и доводится до рабочего состава фирмы всех внешних сторон, которые имеют к ней отношение.

Описанная политика ИБ заявляет о принадлежности руководства и реализует подход к контролю ИБ в фирме. Описанная политика должна включать в себя некоторые факторы:

- описание понятия ИБ, ее совокупных целей, границ действия и основ безопасности каждого механизма, что позволяет внедрять обобщенное применение данных;

- заявление о доступности руководства к поддержке достижений указанных целей и соблюдению правил ИБ, уровня развития и стратегии ИБ;
- основные принципы для выявления важности и механизма контроля, включающего структуру оценки и контроля рисками;
- описания по политике безопасности, принципам, которые важны для компании, включающие в себя:

1. полное соответствие нормам, праву, законам и договорам;
2. требования по оптимизации осведомлённости, курсам, обучению в рамках безопасности;
3. полностью непрерывный процесс бизнеса;
4. определение нарушений требований политики ИБ;
5. выделение личной и обобщенной ответственности за управление ИБ, куда включено и оповещение об произошедших ЧП;
6. ссылки на документы и источники, поддерживающие политику, включающие описание детального строения процедур для каждого класса ИС и правила безопасности, которым нужно следовать всем пользователям.

Такая политика ИБ доводится до рабочего состава фирмы в актуальной, логичной, полноценной форме.

Сама политика ИБ часто бывает лишь частью более обширной установленной политики.

Таким образом, основной организационной мерой должна стать политики информационной безопасности в ООО «ОРП-Ростов», ознакомление с ее положениями всех сотрудников и строгое им следование.

В ходе разработки политики безопасности был сформирован перечень норм для противодействия угрозам информационной системы организации. На основе этого свода правил положено начало процессу нейтрализации высокого уровня угроз информационной системы ООО «ОРП-Ростов».

Таблица 0.2 - Перечень правил политики безопасности

Правило политики информационной безопасности	**Ответственное лицо**	**Категория мер**
В организации следует вести аудит действий выполняемых персоналом в ИС	Администратор	Организационные и технические
В организации следует оговаривать и проводить внезапные проверки соблюдения сотрудниками мер безопасности	Администратор	Организационные
Обеспечение постоянной защиты БД и файловых серверов	Администратор	Организационные и технические
Обеспечить защиту бизнес-процессов всех подразделений и филиалов компании	Пользователи, администратор	Организационные и технические
Организация и контроль доступа	Администратор	Организационные и технические
Обеспечение защиты от вредоносного ПО	Администратор	Организационные и технические

Из таблицы 2.2 видно, что в компании необходимо соблюдать несколько правил информационной безопасности: аудит выполняемых персоналом действий, обязательно оговаривать и проводить внезапные проверки соблюдения сотрудниками мер безопасности, обеспечение защиты БД и файловых серверов, обеспечение защиты бизнес-процессов всех подразделений и филиалов компании, организация и контроль доступа, защита от вредоносного ПО. Каждое правило должно сопровождаться соответствующими видами защитных мер, а также должны быть назначены ответственные лица.

Все пользователи обязаны следовать установленным правилам поддержания безопасности при определении типа паролей. Важно четко следовать некоторым инструкциям:

- обязательно устанавливать свои пароли для обеспечения подотчётности;
- все сохранять в секрете;
- не оставлять пароли на бумаге, если носитель на бумаге может быть похищен и не находится в надежном месте;
- изменять пароли тогда, когда есть указания на возможный взлом системы или пароля;
- использовать пароли от 6 символов и более;
- изменять все пароли через регулярные промежутки времени (до 180 дней) и не использовать повторного или циклично использовать старые;
- как можно чаще менять пароли для доступа к системному ПО, администрирующим программам и ресурсам;
- всегда изменять разовые пароли в рамках входа в систему;
- не использовать пароли в сценариях самостоятельного входа – макросах или функциональных клавишах.

При выборе паролей не стоит пользоваться:

- данными рождения;
- ФИО и номерами авто;
- ID и названиями отделов;
- № телефона и другие группы символов, состоящее из одних цифр;
- ID пользователей, групп, системы;
- парами равных символов;
- одинаковыми буквами и цифрами.

Пользователи должны четко следовать всем параметрам поддержания антивирусной защиты при вводе данных в систему с внешних носителей, работе с e-mail и копировании данных из Интернета.

Нельзя самовольно отключать имеющиеся средства антивирусной защиты и применять внешние носители данных без проведения полной проверки антивирусными средствами.

Админы ИС обязаны всегда быть готовы к опасности попадания нелегального ПО в системы и в случае угрозы принимать ряд мер по минимизации и предотвращению последствий.

Важно соблюдать ряд рекомендаций:

- применять только лицензионное ПО и полный запрет на пиратский софт.

Антивирусные ПО обычно используются следующим образом:

- ПО для нахождения вирусных угроз используется для проверки ПК и носителей данных на нахождения явных угроз или в рамках меры предосторожности или ежедневной процедуры;
- ПО для нахождения изменений, внесенных в данные, которое имеется на ПК в случае необходимости для выявления корректив в рабочий софт.

Нужно постоянно выполнять проверки программ и данных в системах, которые имеют внутри себя критически важные ресурсы компании. Наличие непонятных файлов или незарегистрированных корректив должно быть расследовано формальным методом.

Дискеты и другие переносные носители лучше всего сканировать на вирусы до факта использования.

Нужно заранее выделить ряд процедур и обязанностей по оповещению в момент захвата системы вирусами и принятию срочных мер по минимизации итоговых потерь. Также важно реализовать план поддержания постоянной работы компании в случае вирусного заражения, в т. ч. планы для резервного переноса данных, восстановления всех доступных данных и программ.

2.2 Выбор программно-аппаратных мер

Аппаратные и программные средства дают возможность применять современные технологии аутентификации пользователей и ограничения доступа к информационным системам, а так же управление учётными записями пользователей в информационных системах. Современные средства

обеспечения безопасности в информационных системах имеют большое количество функций и инструментария для решения задач защиты информации от несанкционированного доступа и прочих угроз. Учитывая это, для выбора оптимального способа решения задач информационной безопасности, важно ясно понимать приоритетные направления и сценарии использования. Это поможет успешно и быстро решить задачу, обеспечив компании достойный уровень защиты от несанкционированного доступа.

Основываясь на пунктах 1.2 и 1.3, в том числе на оценке рисков информационных активов организации, следует вывод, для наиболее подходящими методами повышения степени защищённости персональных данных являются:

- ограничение доступа посторонних лиц к БД и СУБД;
- контроль над исполнением всех мероприятий по защите информационных активов;
- защита информации, передающейся как внутри локальной сети так и при передачи данных между филиалами;
- обеспечение защиты от утечки информации из внутренней сети в Интернет.

Рассмотрим программные комплексы со схожей стоимостью и функциональными возможностями:

- ИВК Кольчуга;
- ViPNet 4;
- Застава 5.2.

Firewall (межсетевой экран) с допольнительной функциональностью «ИВК Кольчуга» является программным комплексом, обеспечивающим защиту конфиденциальной информации, в том числе составляющей государственную тайну.

Основные возможности данного комплекса:

- ограничение пропускной способности;

- механизмы трансляции сетевых адресов (прямой и обратный);
- маскировка структуры локальной сети;
- защита от сетевых атак, как всей сети так и самого узла выполняющего функцию МЭ.
- фильтрация трафика по заданным правилам;
- статическая маршрутизация трафика TCP/IP;

Программный комплекс ViPNet - программный комплекс для обеспечения безопасности информации, состоящий из множества компонентов, предназначенный для небольших и средних компаний. Обеспечивает защиту локальной сети от любого рода атак из Интернета, кроме того дает возможность гибкого управления доступом к интернет-ресурсам, позволяет создавать защищённые виртуальные частные сети.

Основные возможности программы:

- объединение в виртуальную частную сеть всех устройств организации;
- шифрование внутреннего трафика;
- шифрование трафика при передаче между филиалами;
- встроенная система зачищенной электронной почты;
- веб-фильтрация;
- функция контроля приложений служащая для обнаружения и устранения активности программ-шпионов.

Программный комплекс ЗАСТАВА используется для обеспечения безопасности конфиденциальных данных, работает на сетевом уровне модели OSI.

Данный комплекс состоит из компонентов трёх типов (управление, клиент, сервер), устанавливаемых на компьютеры сотрудников, серверы и шлюзы локально сети, а также панели управления администратора под названием «Застава-Управление».

Комплекс Застава 5.2 обладает следующими особенностями:

- имеет широкий набор сценариев VPN-топологий и готовых правил для настройки МЭ, в том числе при использовании NAT (трансляции адресов);
- централизованным управлением политикой безопасности;
- защита ЛВС от сетевых атак;
- защитой самого устройства от различных сетевых атак;
- прямым и обратным механизмом трансляции сетевых адресов;
- фильтрацией трафика TCP/IP по заданным критериям;

Сравнение ключевых показателей программных продуктов представлено в таблице 2.2.

Таблица 0.3 - Перечень правил политики безопасности

Наименование ПО	**Шифрование внешнего трафика**	**Шифрование внутреннего трафика**	**Масштабируемость (1-5 баллов)**
ИВК Кольчуга	Да	Нет	3
VipNet 4	Да	Да	5
Застава 5.2	Да	Нет	2

Наибольший интерес вызывает линейка продуктов VipNet, имея пред другими рассматриваемыми продуктами такие преимущества:

- масштабируемость, существование множества компонентов позволяющих в любое время расширить функционал системы легко и без крупных затрат
- шифрование внутреннего трафика
- встроенная система зачищенной электронной почты
- функция контроля приложений служащая для обнаружения и устранения активности программ-шпионов.

Применение программного комплекса ViPNet позволит ликвидировать большую часть уязвимостей ИС ООО «ОРП-Ростов», что в совместно с

применением организационных мер защиты информации позволит нам решить поставленную задачу.

2.3 Организационные методы защиты

Основным механизмом достижения поставленной цели при достижении высокого уровня информационной безопасности для ООО «ОРП-Ростов» является издание приказов, регламентирующих действия сотрудников, при работе с информационными системами, в том числе должна быть определена зона ответственности каждого сотрудника, в особенности системного администратора. Для ООО «ОРП-Ростов» в политику безопасности будет включён ряд приказов и других руководящих документов:

1. Приказ № 523-а «О наделении сотрудников полномочиями, и назначении ответственных за соблюдение мер по обеспечению информационной безопасности»;
2. «Инструкция по установке и обновлению программного и аппаратного обеспечения»;
3. «Инструкция о порядке и нормах программно-технической защиты информации»
4. Приказ № 525-е «О закреплении за сотрудниками разрешённого к использованию программного обеспечения»;
5. Приказ № 560 «О ответственности, и дисциплинарных мерах при нарушениях требований связанных с информационной безопасностью».

Выполнение основной цели и поставленных задач станет возможно при:

- четкое разделение принципов анализа данных методами автоматизации работы персонала ООО «ОРП-Ростов», которые применяют ИС, а также работа сотрудников, обслуживающих технические и программные средства ИС, базируясь на указанных руководством фирмы документах, описывающих все важные нюансы поддержания ИБ;

- рассмотрения всех возможных проблем, применение требований из корпоративных норм и документов, описывающих все ключевые особенности поддержания безопасности информации;
- назначение, обучение, мотивация сотрудников, отвечающих за разработку и соблюдение мер обеспечивающих информационную безопасность;
- передача персоналу некоторых полномочий для полноценной реализации указанных функциональных задач, которые заключены в доступе к ИС;
- четкое понимание и следование сотрудников всем требованиям в рамках поддержания ИБ данных при обслуживании и работе в ПО;
- персональная ответственность сотрудника, который в рамках своих полномочий принимает участие в автоматизации и анализе данных и может иметь доступ к ИС, за все совершенные действия;
- описание и учет каждого защищаемого ресурса (данных, серверов, станций, каналов);
- выделение точных решений для поддержания полноценности технических ресурсов и постоянству защищенности ИС;
- использование физических и технических СЗИ с постоянной поддержкой использования;
- беседы с персоналом и реализация постоянного контроля за сотрудниками ООО «ОРП-Ростов» для следования всем требованиям ИБ;
- полноценная юридическая защита фирмы при обоюдной работе все отделов компании с внешними партнерами (а именно, с обменом данными) от НСД как этих компаний, так и от НСД персонала компании и третьих лиц;
- полноценный анализ, с помощью которого станет возможно ответить на вопросы достаточности реализуемых мер и используемых СЗИ, внедрением обновленных предложений по поддержанию лучшего уровня всей ИС.

Дозволение сотрудникам фирмы работать в АИС и иметь доступ к основным ресурсам важно четко регламентировать. Все корректировки полномочий пользователей системы могут быть реализованы в рамках регламента «Документ для корректировки перечня пользователей системы и их полномочий для доступа к системным ресурсам». Каждый сотрудник фирмы обязан иметь некий требуемый доступ для реализации своих функциональных требований с применением ресурсов АС. Но никто не должен иметь прав на полное удаление данных и ресурсов ИС. Сами директора отделов должны изначально подать заявки на предоставление доступа и ли его закрытие для своих сотрудников исходя из их полномочий для нормальной работы с самой ИС.

Структура АРМов, которые анализируют все защищенные данные (или которые имеют доступ к ним), обязана четко следить за правами пользователя, который работает сейчас за ПК. Нетребуемые в работе данные и их источники (приводы, диски, дисководы) нужно отключить (полностью или логически), а не нужные для работы программы просто удаляются.

Для упрощения обслуживании компании и ее сопровождения, все ПК имеют ряд ПО и собираются уже унифицировано в пределах требуемых норм.

Установка новых ПК, как и изменения конфигураций ПО или аппаратной части уже имеющихся ПК реализуются в четком порядке в рамках «Инструкции по обновлению, установке и ТО программ и аппаратных средств РС АС».

Физическая целостность всех аппаратных составляющих защищенных компьютеров может обеспечиваться организационными мерами с применением механических средств (замков), пломб (наклеек, стикеров и т.д.) и всех комплектующих частях вычислительной техники.

Постоянное отслеживание целостности и проверка штампов и пломб на ПК реализуется каждым пользователем персонально и админом по ИБ. Также контроль лежит на директорах отделов и службы ИБ.

Вся деятельность на защищенных ПК выполняется только в помещениях, которые имеют замки, сигнализацию, постоянное видеонаблюдение и охрану, что минимизирует проникновение внутрь третьих лиц и поддерживает некую физическую сохранность оборудование и сотрудников. Помещение и установка ПК и АРМов обязана исключать возможный осмотр на предмет вводимых данных для всех тех, кто не имеет прав на получение подобной информации.

Уборка в помещениях с такими ПК реализуется только в присутствии должностного лица, который отвечает за эти ТС и в рамках правил, исключающих любой доступ к защищенным ресурсам.

В помещениях в рамках анализа данных и отображения их на экране могут находится только те лица, которые допущены к данной работе официально. Все посетители не имеют права даже визуально знакомиться с данными, к которыми нет допуска.

По факту завершения работы все помещения с охраняемыми ПК передаются под охрану с включенной сигнализацией и отметками о сдаче/приеме помещений.

Во времена сетевой инфраструктуры также используют деление ЛВС (локальные вычислительные сети или «LAN-local area network» [20, 15 р.]) на сегменты, которые часто базируются на виртуальных ЛВС (VLAN) при следовании организационной структуры соединения и методикой работы отдела фирмы и данными.

Сервера ЛВС могут располагаться в выделенных сегментах. Важно обеспечить отсутствие рабочих мест обычных пользователей в этих указанных сегментах ЛВС.

2.4 Структура программно-аппаратного комплекса информационной безопасности и защиты информации предприятия

Программный комплекс ViPNet осуществляет комплексную защиту информации, может состоять из множества компонентов, например из межсетевого экрана, системы «Intrusion Detection System» служащей для

обнаружения вторжений, службы электронной почты (защищенной от спама, несанкционированного доступа, почтовых атак) клиента обмена мгновенными сообщениями, и основных административной, клиентской, и серверной частей.

Одним из преимуществ является простота внедрения, необходимо лишь установить на компьютеры пользователей и серверы основные компоненты. При этом не требуется закупать дополнительное оборудование или менять топологию сети. Данный комплекс при создании защищённого соединения использует схему шифрования с автоматически распределёнными симметричными ключами и автоматически их обновляет на стадиях установки программного обеспечения. Каждый пакет, отправленный в сеть, защищается шифрованием с применением уникального ключа, передаваясь без использования каких либо процедур установки соединения. Это дает возможность качественно организовать безопасную передачу информации по незащищённым каналам, и с использованием методов, для которых характерны большие потери трафика (спутниковые, модемные соединения), а также может использоваться в ЛВС, для которой критичны любые задержки во время установки соединения.

Программный комплекс лицензирован федеральной службой безопасности а так же ФСТЭК России, обеспечивает высокий уровень безопасности информации и отлично подходит к применению как в частных организациях, так в и государственных структурах в качестве средства обеспечения безопасности конфиденциальной информации или информации составляющей государственную тайну.

Программный комплекс ViPNet используя технологию «Virtual Private Network» может объединять как отдельные рабочие станции, так и целые компьютерные сети, а так же обеспечивать доступ к ним с мобильных устройств.

При этом каждый пакет данных при передачи как между отдельными сетями или при доступе к ЛВС с мобильных устройств, так и при обмене

данными внутри сети будет надёжно защищён комбинацией шифрования и туннелирования .

Кроме того комплекс имеет в своём составе программный межсетевой экран, что позволяет защитить информационную систему от различных сетевых атак, ограничив установление лишних соединений и попадание потенциально опасных пакетов данных в сеть.

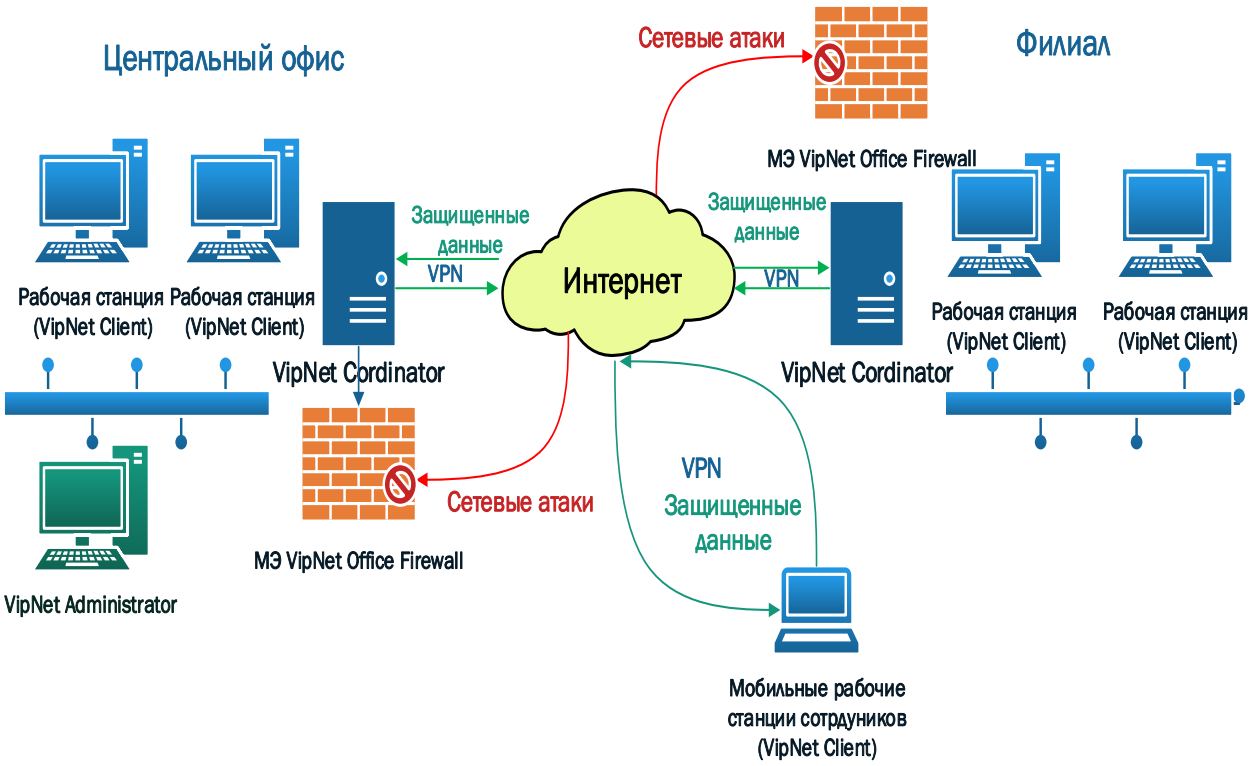

Рисунок 0.1 - Компоненты системы VipNet

Подобранное нами решение содержит следующие программные компоненты:

- VipNet Administrator (компонент управления) - отвечает за администрирование системы. Так же исполняет роль удостоверяющего центра;
- VipNet Cordinator (серверная часть) - используется для реализации функций сервера: туннелирование, маршутизацию почтовых и управляющих сообщений, регистрацию состояния всех компонентов сети;
- VipNet Client (клиентская часть) – используется для реализации клиентских функций: контролирует сетевую активность приложений,

шифрования трафика, обнаружения атак, аудит состояния системы и клиент защищённой электронной почты;

- ViPNet Office Firewall («firewall – network security system that monitors outgoing and incoming network traffic» [22, 99 p.]) - программный межсетевой экран, используется для фильтрации трафика поступающего в сеть а так же в обратном направлении. Имеет множество настроек, позволяя обеспечить защиту от сетевых атак, кроме того имеет функцию управления доступом в Интернет, для ограничения использования сотрудниками опасных или не относящихся к их деятельности интернет ресурсов.

Так же существуют и другие компоненты, дополнительно внедрить которые будет возможно без труда, не внося существенных изменений в и не приостанавливая работу действующей системы информационной безопасности, а так же комплекс имеет функции контроля приложений и защищенную службу электронной почты.

Структурная схема информационной системы ООО «ОРП-Ростов» представлена на рисунке 2.3.

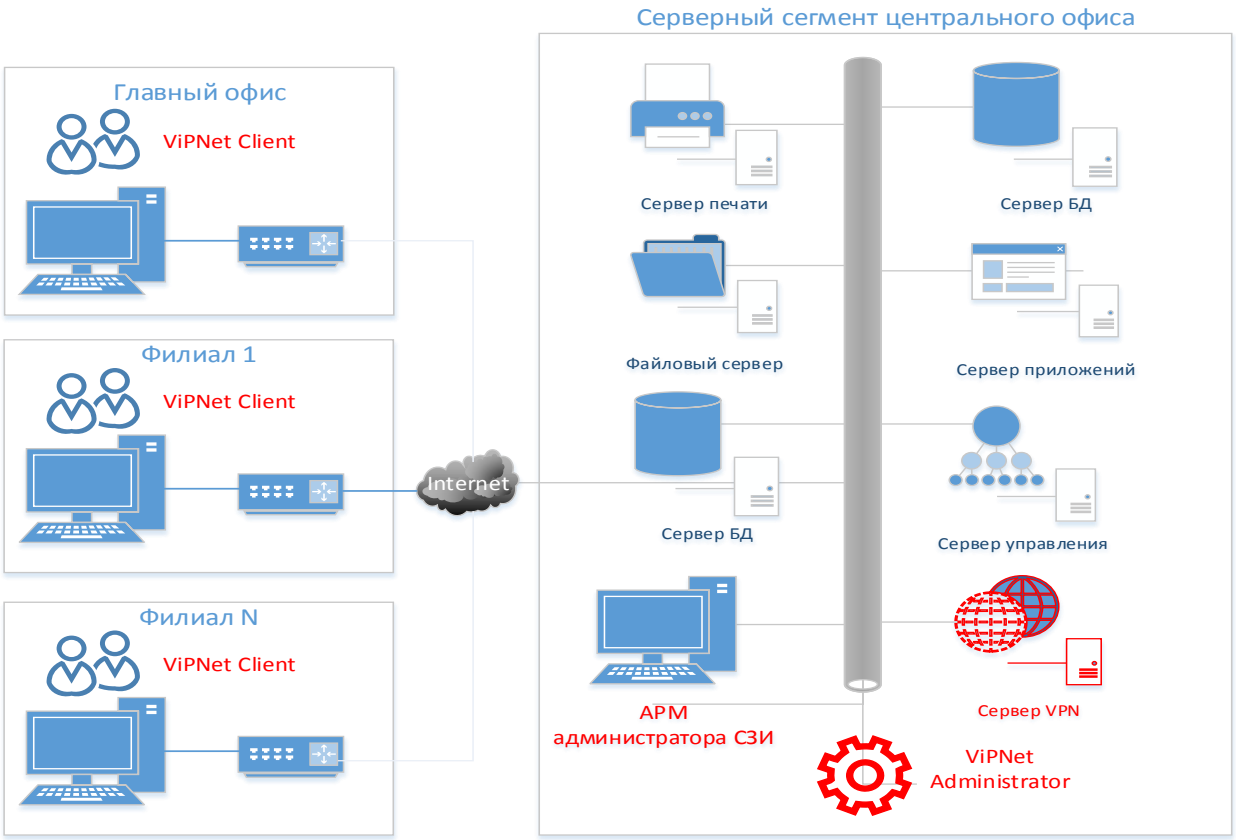

Рисунок 0.2 - Структурная схема программного обеспечения с учетом элементов системы VPN

Программный комплекс ViPNet позволяет организовать безопасный обмен данными по открытым каналам связи организованным с применением множества различных технологий.

VipNet позволяет организовывать VPN (виртуальные частные сети) любых топологий и конфигураций, обеспечивающих безопасное взаимодействие всех элементов сети вне зависимости от метода подключения, расположения и используемых сетевых протоколов при их подключении к сети. При использовании данного комплекса весь трафик, проходящий по этой сети, защищен самыми современными криптографическими методами. Все основные обменные процессы происходят с использованием сервисом отвечающих довольно высоким требованиям к обеспечению информационной безопасности. Возможность расширения системы путём установки или внедрения дополнительных компонентов позволяет легко увеличить область действия и уровень защищенности ИС в зависимости от необходимости .

2.5 Реализация мер по устранению факторов негативно влияющих на защищённость информационной системы ООО «ОРП-Ростов»

В ходе исследования были определены наиболее ценные информационные активы организации, выявлены угрозы и определена величина возможных потерь в случае их успешной реализации (более подробно величины возможных потерь представлены в приложении № 4), а так же выявлены факторы негативно влияющие на уровень защищенности.

Для устранения данных факторов была разработана политика информационной безопасности, изданы соответствующие приказы, проведено ознакомление сотрудников с правилами обеспечения надлежащего уровня информационной безопасности и дисциплинарных мерах применимых при их нарушении.

Поэтапно внедрение политики информационной безопасности выглядит следующим образом:

1. издание соответствующих приказов;
2. реализация ответственным за защиту информации сотрудником мер, для исполнения изданных приказов;
3. ознакомление сотрудников со вновь введёнными правилами и нормами в области информационной безопасности, а так же с дисциплинарными мерами, применяемыми при их нарушении;
4. повышенный уровень контроля исполнения сотрудниками мер по обеспечению информационной безопасности в течении шести месяцев с момента внедрения.

В целях устранения уязвимостей информационной системы имеющих программно-техническую основу был внедрён программный комплекс VipNet.

Внедрение проходило поэтапно:

1. определение целей;
2. подбор подходящего программного средства;

3. определение ответственных лиц и привлечение участников процесса внедрения;

4. составление проекта внедрения;

5. установка на серверы, рабочие станции и настройка программного обеспечения;

6. тестирование системы;

7. завершение процесса внедрения.

Для внедрения программного комплекса «VipNet» были привлечены системный администратор ООО «ОРП-Ростов» а так же эксперты компании «Infotecs» для консультаций при настройке программного комплекса. В ходе внедрения было установлено серверное и клиентское программное обеспечение.

Серверным программным обеспечением в данном случае является «VipNet Кординатор». Аппаратной платформой был выбран сервер используемый как контроллер домена, потому как его ресурсы используются не в полном объеме, а функции DHCP сервера которые он в том числе выполнял, теперь будут выполнятся программным обеспечением VipNet.

Панель управления администратора так же была установлена на аппаратную платформу используемую как контроллер домена и сервер динамической раздачи IP-адресов.

Клиентское программное обеспечение VipNet было установлено на все рабочие станции сотрудников, в том числе на ноутбуки используемые для доступа к информационной системе в случае работы вне офиса.

Для реализации функции межсетевого экрана нет необходимости в аппаратной платформе высокой мощности, по этой причине был использован системный блок находящийся в резерве, использование которого было прекращено ранее в связи с отсутствием потребности в дальнейшем использовании на момент принятия решения о его прекращении использования.

Тестирование проводилось с привлечением системного администратора, руководителей подразделений, сотрудников задействованных в выполнении ключевых бизнес-процессов ООО «ОРП-Ростов», и представителей компании «Infotecs». Системный администратор был назначен руководителем тестирования. Участникам тестирования была поставлена задача опробовать все возможности информационной системы используемые при выполнении их должностных обязанностей и составить отчёты о результатах заверив их подписью руководителей подразделений.

Тестирование программного комплекса завершилось успешно, влияния на выполнение функций связанных с бизнес-процессами ООО «ОРП-Ростов» выявлено не было.

В результате применения комплекса мер, организационных и программно-технических выявленные негативные факторы были устранены.

Схематично применение мер показано на рисунке 2.4.

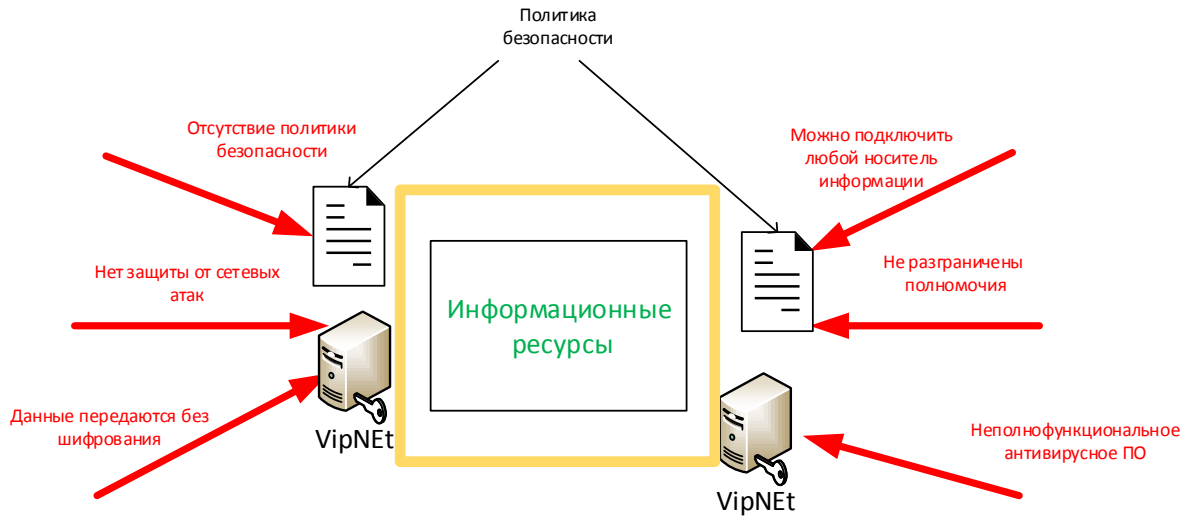

Рисунок 0.4 - Применение выбранных мер

Данные меры были необходимы и достаточны для того, чтобы вывести уровень защиту информации на нужный уровень и обеспечить необходимую защиту информации в виде информационных активов.

Выводы по второй главе

Таким образом, во второй главе выпускной квалификационной работы рассмотрено внедрение комплекса мер, необходимых для повышения уровня защиты информации и устранения выявленных в первой главе угроз.

В результате внедрения комплекса мер, в который входит:

- применение организационных мер в виде разработанных требований к сотрудникам компании по соблюдению режима информационной безопасности;
- внедрение специального программного комплекса для шифрования передаваемого трафика при его движении внутри компании, так же используемого для защиты от сетевых атак.

Факторы негативно влияющие на уровень защищённости информационных активов ООО «ОРП-Ростов» были устранены, следовательно уровень защищенности информационных активов организации значительно вырос.

Глава 3 Обоснование экономической эффективности проекта

3.1 Выбор и обоснование методики расчёта экономической эффективности

В документальном источнике ФСТЭК России «Суть защиты ЭВМ и АИС от НСД к данным», который включает систему взглядов ФСТЭК России на проблему ИБ и базовые принципы ЗИ, сказано, что «... Важная часть работ по защите заключена в оценивании результативности СЗИ, которое проходит по методике, включающей совокупность ТХ рассматриваемого объекта, включая все решения по практической и технической реализации СЗИ» [13].

Активная работа людей всегда и везде связана с проблематикой определения и принятия решений, направленных на реализацию конкретной цели. При этом по сути ряд решений в области ЗИ выполняется на понятийном уровне, без обоснования и учета. Но новейшие требования к ИБ говорят о явной важности применения обоснованных методик и средств, которые более качественно измерят показатель защищенности, а также оценят итоги СЗИ.

Полная защищенность данных требует многочисленных расходов на защиту. Поэтому, логично выбрать алгоритм рационального выбора СЗИ методом понимания его результативности, что поможет создать СЗИ при ряде ограничений по реализации.

Проблема оценки результативности СЗИ многих ИС очень сложна, и ее решение будет доступно только в случае использования методологии общей теории результативности, и к примеру, теории оценки результативности охранных систем.

Важно понимать, что задача подсчета результативности стоит на организационном уровне, считается важной в ряде задач поддержания ИБ и работы данных в ИС, таких как:

- проведение разработки СЗИ;
- создание плана мероприятий;
- подготовка документов;
- проведение работы с пользователями и посетителями;

- сертификация СЗИ анализа информации;
- получение лицензии для защиты процессов анализа информации;
- проверка объектов защиты;
- улучшение полученной системы.

Исходя из шкалы, которая участвует в измерении, получают количественные и качественные параметры результативности.

Параметры, значения которых расположены в порядковой и номинальной шкалах, именуются качественными.

К количественным относят такие параметры, которые можно измерить в метрической шкале.

В новейших исследованиях, которые описывают методы и СЗИ, в базе главного параметра результативности выступает применением потенциального ущерба в финансовом выражении.

Оценка результативности происходит с применением параметра результативности, который создается в рамках описанных ранее показателей. И в сравнении с параметром, который лишь отражает число или уровень достижения цели, критерий результативности выносит суждение о адекватности того или иного решения.

Критерий результативности можно понимать двояко:

- в более узком понимании: как правило оценки результативности;
- в более широком понимании: как совокупность параметров результативности, требований к системе и правил их сравнения для понимания обобщенной эффективности;

Чтобы подготовить показатели результативности, важно:

- выразить требуемую цель;
- привести несколько неуправляемых и управляемых параметров системы и среды;
- сформировать и выбрать критерии результативности.

Как критерий результативности, так и показатель результативности могут быть векторными и скалярными. Для выбора показателя результативности

важно основываться на таких требованиях, как четкое понимание цели, полнота, исчислимость, понятность физического смысла, малая размерность.

Результаты расчета величин потерь для ключевых информационных активов до применения мер защиты приведены в Приложении 5.

3.2 Расчёт показателей экономической эффективности проекта

Ранее было определено значение совокупной величины потерь в случае реализации всех угроз информационным активам.

Далее необходимо определить значение всех затрат на подготовку, реализацию и внедрение выбранных мер по защите информации, а также определить значение возможного снижения потерь при внедрении выбранных мер, то есть насколько в денежном отношении улучшится уровень защищенности информационных активов компании.

Для разработки, реализации и внедрения системы защиты информации могут быть применены следующие статьи затрат:

- заработная плата сотрудников компании при разработке системы защиты информации;
- заработная плата сотрудников компании при реализации системы защиты информации;
- заработная плата сотрудников компании при внедрении системы защиты информации;
- стоимость аппаратных и программных средств для реализации системы защиты информации.

Кроме того, при эксплуатации системы защиты информации необходимо учитывать такие затраты, как заработная плата обслуживающего персонала, стоимость электроэнергии, стоимость обслуживания и сопровождения оборудования.

Единовременные затраты приведены в таблице 3.1.

Таблица 0.1 - Единовременные затраты, выделяемые на разработку комплекса мероприятий направленных на повышение уровня защищённости ИС ООО «ОРП-Ростов»

Мероприятия (организационные)				
№ п\п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час)	Стоимость, всего (тыс.руб.)
1.	Разработка технического задания	147	48	6,223
2.	Согласование и утверждение ТЗ	146	24	3,342
3.	Разработка проекта СЗИ	140	12	2,01
4.	Расчет потребности в оборудовании	140	52	8,134
5.	Юридическая оценка инструкций и других руководящих документов	140	31	4,55
6.	Тестирование	147	12	2,01
7.	Обучение пользователей	147	47	6,325
8.	Ввод в эксплуатацию	145	12	2,01
Стоимость проведения организационных мероприятий, всего				35,67
Внедрение програмного комплекса VipNet				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
1.	ViPNet Coordinator	125	1	126
2.	ViPNet Client	21	34	920
Стоимость проведения мероприятий инженерно-технической защиты				1046
Объем разового ресурса, выделяемого на защиту информации				1082

Содержание и объем постоянного ресурса (за квартал), выделяемого на содержание системы защиты, приведено в таблице 3.2.

Таблица 0.2 - Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п\п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час)	Стоимость, всего (тыс.руб.)
1)	Увеличение заработной платы системного администратора в связи с возложением на него обязанностей по обеспечению защиты информации	130	720	93,6
Стоимость проведения организационных мероприятий, всего				**237,6**
Мероприятия инженерно-технической защиты				
№	Номенклатура ПиАСИБ,	Стоимость,	Кол-во	Стоимость,

п/п	расходных материалов	единицы (тыс.руб)	(ед.измерения)	всего (тыс.руб.)
1.	Сервер (350 вт)	0,004	480	0,0019
Стоимость проведения мероприятий инженерно-технической защиты				0,012
Объем постоянного ресурса, выделяемого на защиту информации				**237,6**

Динамика потерь за период 2 года представлена в таблице 3.3.

Таблица 0.3 - Оценка динамики величин потерь

	1 кв	2 кв	3 кв	4 кв	5 кв	6 кв	7 кв	8 кв
До внедрения системы защиты	358,33	716,67	1075,00	1433,33	1791,67	2150,00	2508,33	2866,67
После внедрения защиты	71,67	143,33	215,00	286,67	358,33	430,00	501,67	573,33
Снижение потерь	286,67	573,33	860,00	1146,67	1433,33	1720,00	2006,67	2293,33

В первой строке таблицы приведены значения потерь без системы защиты, во второй – после внедрения системы защиты. В третьей строке приведено значение снижения планируемых потерь. Как видно из таблицы, система защиты окупится в третьем квартале второго года

Независимо от результатов оценки окупаемости проекта необходимо учесть факт что при должном подходе, злоумышленник может влиять на деятельность организации, используя похищенную информацию, например привести организацию к значительным финансовым трудностям, в том числе и к банкротству.

График, характеризующий оценку срока окупаемости системы защиты, представлен на рисунке 3.1.

Рисунок 0.1 - Оценка срока окупаемости системы защиты

Таким образом, срок окупаемости системы составляет 21 месяц.

Выводы по третьей главе

В третьей главе работы выбрана и описана методика расчета экономической эффективности, проведен расчет его показателей, в том числе определен срок окупаемости внедрения выбранных мер защиты.

Заключение

Одной из ключевых проблем защиты информации при использовании информационных систем является защита информационных активов от несанкционированного доступа, и обеспечение целостности данных. Методы обеспечения безопасности информационных систем тесно связаны с глубоким анализом текущего состояния состояния, выявлением уязвимостей, выбором механизмов и средств защиты и эффективностью их внедрения в ООО «ОРП-Ростов», в том числе экономической.

В выпускной квалификационной работе решалась задача организации защиты информационной системы предприятия «ОРП-Ростов» на основе типовых решений. В ходе работы рассмотрено существующее положение с защитой информации в компании. В результате анализа был выявлен ряд уязвимостей системы, определяющий высокий риск реализации угроз. Основываясь на результатах исследования был разработан и в последствии внедрён комплекс мер, как организационных, так и программно-технических.

Разработка руководящей документации, создала основу, фундамент на котором будет действовать система обеспечения информационной безопасности, были созданы нормы и правила, инструкции, назначены ответственные.

Внедрение программного комплекса позволило сделать безопаснее как передачу любой служебной информации между филиалами организации, использование интернет ресурсов, электронной почты, так и использование информационных систем в деятельности организации в целом. Позволило сотрудникам, чья работа связана с разъездами, получить безопасный доступ к ресурсам организации со своих мобильных устройств, где бы они ни находились.

Дальнейшее совершенствование системы предполагается развивать в следующих направлениях:

- изучение стороннего опыта, слежение за мировыми тенденциями в области защиты информации;

- дополнение руководящей документации;
- строгом контроле соблюдения существующих норм, разработкой системы штрафов за нарушения правил описанных в руководящей документации;
- регулярным информированием сотрудников о инцидентах произошедших в других организациях по всему миру, причинах и последствиях;
- расширение функциональности программного комплекса VipNet, благодаря добавлению в его состав новых компонентов.
- введение должности администратора системы информационной безопасности.

Благодаря применению выбранных мер устойчивость к угрозам информационных систем используемых в ООО «ОРП-Ростов» значительно увеличилась, и при должном внимании, своевременном обновлении и совершенствовании сможет оставаться на высоком уровне ещё достаточно долгое время.

Список используемой литературы

Нормативно правовые акты

1. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения. Критерии оценки безопасности информационных технологий. Ч.1. Введение и общая модель. – М.: Госстандарт России, 2002.

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год Пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009 г.

3. Стандарт ЦБ РФ "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения", (принят и введен в действие распоряжением ЦБ РФ от 18 ноября 2004 г. N Р-609).

4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" С изменениями и дополнениями от: 27 июля 2010 г., 6 апреля, 21 июля 2011 г., 28 июля 2012 г., 5 апреля 2013 г.

5. Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» (ред. от 21.07.2014).

6. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. ГОСТ Р ИСО/МЭК 27001-2006.

Научная и методическая литература

7. Адаменко М. А., Основы классической криптологии. Секреты шифров и кодов, М., ДМК Пресс, 2016 г., 296 с.

8. Баранова, Бабаш: Криптографические методы защиты информации. Лабораторный практикум. Учебное пособие, М. Кнорус, 2017 г. 254 с.

9. Бирюков А.А., Информационная безопасность. Защита и нападение, М., ДМК-Пресс, 2017 г., 434 с.

10. Бондарев В.В., Введение в информационную безопасность автоматизированных систем, М. , Издательство МГТУ им. Н.Э.Баумана, 2016 г., 252 с.

11. Борисов М.С., Романов О. В., Основы организационно-правовой защиты информации. Учебное пособие, М. Ленанд, 2018 г, 312 с.

12. Царегородцев А. А., Тараскин Н.А.: Методы и средства защиты информации в государственном управлении. Учебное пособие, М., Проспект, 2017 г., 208 с.

13. Шаньгин В.Ф,: Информационная безопасность и защита информации, М., ДМК-Пресс, 2017 г., 702 с.

14. Брюс Шнайер, Прикладная криптография. Протоколы, алгоритмы и исходный код на С, М., Вильямс, 2016 г, 1024 с.

15. Душкин Р.А., Все о шифрах и кодах. В мире математики и криптографии, М., АСТ, 2018 г, 448 с.

16. Козлов С.А.: Защита информации. Устройства несанкционированного съема информации и борьба с ними, М., Академический проект, 2018 г., 286 с.

17. Краковский Ю.М.: Защита информации. Учебное пособие, М., Феникс, 2017 г., 348 с.

18. Марков А. С., Дорофеев А. В., Семь безопасных информационных технологий, М., ДМК-Пресс, 2017 г., 224 с.

19. Никифоров С.Н., Методы защиты информации. Защита от внешних вторжений. Учебное пособие, М., Лань, 2018 г, 96 с.

20. Нильс Фергюсон, Брюс Шнайер, Практическая криптография, М., Вильямс, 2017 г, 420 с

21. Райтман М. В., Искусство легального, анонимного и безопасного доступа к ресурсам Интернета, Спб., БХВ-Петербург, 2017 г., 724 с.

22. Скрабцов Н.А.: Аудит безопасности информационных систем, М. Питер, 2017 г., 277 с.

Электронные ресурсы

23. Обеспечение информационной безопасности организаций банковской системы РФ. Стандарт банка России СТО БР ИББС-1.0-2010.) [Электронный ресурс] http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd (дата обращения: 07.04.2019).

Литература на иностранном языке

24. Y. Diogenes, E. Ozkaya, Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics, Pacts, 2018, 399 p.

25. H. Jardyn, B. Rose, World of cryptography, World Scientific, 2018, 324 p.

26. W. Du, Computer & Internet Security: A Hands-on Approach, Dragon, 2019, 134 p.

27. M. Ciampa, CompTIA Security+ Guide to Network Security Fundamentals - Standalone Book, Cengage, 2018, 234 p.

28. Yang Xiao, Hui Chen , Frank Haizhon Li, Handbook of Security and Networks, World Scientific, 2017, 272 p.

Приложение 1 Оценка информационных активов компании

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка (руб/год)	Качественная
Информационные активы						
Ведение базы данных	Информация для БД	Текстовые файлы, печатные или рукописные	Начальник отдела IT	Расходы на создание	75000	высокая
	Финансовые показатели компании	Текстовые файлы, печатные или рукописные	Главный бухгалтер	Расходы на создание	40000	Средняя
	Персональные данные сотрудников	базы данных, личные дела	генеральный директор «ОРП-Ростов»	Расходы на создание	≈80 000	Высокая
Активы программного обеспечения						
Работа с ПО	Программы: бухгалтерские, офисные, прикладные	в электронном виде	Начальник отдела IT	Расходы на покупку и создание ПО	300000	Очень высокая
Физические активы						
Специалисты по созданию БД	Сотрудники фирмы	ООО «ОРП-Ростов»		≈42 000	Средняя	
Рабочие компьютеры	Компьютеры сотрудников	ООО «ОРП-Ростов»	Исходная стоимость товара Стоимость обновлений	≈300 000	Очень высокая	
Телефони	Телефоны	ООО	Исходная	≈50 000	Средняя	

я и периферия	сотрудников	«ОРП-Ростов»	стоимость товара			
Серверы рабочей информации	Компьютеры - серверы	ООО «ОРП-Ростов»	Исходная стоимость товара Стоимость обновлений	≈300 000	Очень высокая	
Съемные носители информации	CD и DVD диски, USB флеш-накопители и т.п.	Сотрудники, использующие съемные носители	Исходная стоимость товара	≈40 000	Средняя	
Компьютерная периферия	принтеры, факсы, ИПБ и т.п.	ООО «ОРП-Ростов»	Исходная стоимость товара	≈150 000	Высокая	
Сети интернет и внутренние сети фирмы	Ресурсы всемирной сети и ресурсы сети фирмы	ООО «ОРП-Ростов»	Расходы на оплату провайдеру	24 000	Средняя	

Приложение 2 Перечень сведений конфиденциального характера

№	Наименование сведений	Гриф[1]	Базы данных и носители сведений
1	Персональные данные сотрудников организации: ФИО, Паспортные данные, финансовые сведения, социальное, семейное положение и сведения об образовании сотрудников	СК ПД 2 К ПД 3,4	База данных «Сотрудник», трудовая документация, личные дела сотрудников и тп.
2	Персональные данные, полученные от клиентов: ФИО, паспортные данные, финансовые сведения	СК ПД 2 К ПД 3,4	база данных «Должник», «Клиент», контракты и тп.
3	Сведения о финансовом состоянии организации, перечень основных средств, статическая часть бухгалтерской и налоговой отчётности	К КТ	Бухгалтерская и налоговая отчётность
4	Расчетно-финансовые операции, сведения по ведению расчётного счёта и информация взаимодействия с кредитными организациями	К КТ	Банковские контракты, информация бухгалтерского отдела
5	Состояние денежных счетов организации, текущее финансовое состояние, финансовые потоки, информация о кредиторской и дебиторской задолженности организации	К КТ	Бухгалтерская отчётность, отчёты о деятельности организации
6	Сведения о концепции развития предприятия, стратегические планы развития, функциональные, маркетинговые, финансовые и логистические модели ведения бизнеса	СК КТ	Концепция ведения бизнеса, стратегические планы организации по функциональным направлениям
7	Сведения о планируемых и текущих совещаниях, перечень обсуждаемых вопросов, протоколы и отчёты по совещаниям	К КТ	Планы совещаний, протоколы и постановления
8	Сведения об условиях коммерческих контрактов, выплат клиентам и услуг организации	К КТ	Базы данных юридического отдела
9	Сведения, раскрывающие систему, средства защиты информации, порядок обработки и передачи конфиденциальной информации	СК КТ	Документы СОИБ

[1] ПД – персональные данные 1,2,3,4 – категории персональных данных;
К – конфиденциально;
СК – строго конфиденциально;
КТ – коммерческая тайна.

Приложение 3 Результаты оценки уязвимости активов ООО «ОРП- Ростов»

Группа уязвимостей Содержание уязвимости	**Базы данных**	**Серверы рабочей информации**	**Персональные данные сотрудников**	**Рабочие компьютеры**	**Документы и отчеты в печатном виде**
1. Среда и инфраструктура					
Неправильное или халатное использование физических средств управления доступом	средняя	высокая	высокая	высокая	высокая
2. Аппаратное обеспечение					
Недостаточное обслуживание СВТ	средняя	высокая	низкая	высокая	низкая
Изъяны в схемах амортизации и замены СВТ	низкая	высокая	низкая	высокая	высокая
Неконтролируемое копирование	высокая	низкая	низкая	высокая	низкая
Незащищенное хранение.					
3. Программное обеспечение					
Уязвимости ПО	высокая	средняя	высокая	высокая	низкая
Неправильное распределение прав доступа	высокая	низкая	низкая	низкая	низкая
4. Коммуникации					
Изъяны пользовательской аутентификации	высокая	высокая	высокая	низкая	низкая
Запуск ненужных служб	высокая	средняя	средняя	средняя	средняя
Незащищённые линии связи	высокая	высокая	высокая	низкая	низкая
Опасная сетевая архитектура	высокая	высокая	высокая	средняя	низкая
5.Персонал					
Неадекватные процедуры вербовки		высокая		высокая	
Неправильное использование ПО и оборудования	высокая	высокая	высокая	высокая	

Приложение 4 Величины потерь (рисков) для критичных информационных ресурсов до внедрения системы защиты

Актив	Угроза	Величина потерь (тыс.руб.)
Серверное программное обеспечение	Доступ к информации в обход имеющихся правил или прав пользователей к ресурсам информационной системы с рабочих станций легальных пользователей	75
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	60
	Заражение вирусами	110
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	220
Базы данных	Выход из строя оборудования информационных систем и оборудования	90
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	60
	Заражение вирусами	75
	Разглашение, передача или утрата атрибутов разграничения доступа	20
Документы и отчеты в печатном виде	Применение технических средств для несанкционированного съема информации	75
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	155
	Выход из строя оборудования информационных систем и оборудования	120
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	115
	Заражение вирусами	40
Литература и электронные издания для служебного пользования	Разглашение, передача или утрата атрибутов разграничения доступа	75
	Применение технических средств для несанкционированного съема информации	70
Персональные компьютеры пользователей	Заражение вирусами	65
	Разглашение, передача или утрата атрибутов разграничения доступа	95

Актив	Угроза	Величина потерь (тыс.руб.)
	Применение технических средств для несанкционированного съема информации	75
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	55
	Выход из строя оборудования информационных систем и оборудования	75
	Заражение вирусами	195
	Разглашение, передача или утрата атрибутов разграничения доступа	155
Результаты маркетинговых исследований	Применение технических средств для несанкционированного съема информации	220
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	90
	Заражение вирусами	20
	Разглашение, передача или утрата атрибутов разграничения доступа	75
Персональные данные сотрудников	Применение технических средств для несанкционированного съема информации	155
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	120
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	40
	Заражение вирусами	75
	Разглашение, передача или утрата атрибутов разграничения доступа	70
Суммарная величина потерь, тысяч рублей		2940

Приложение 5 Величины потерь (рисков) для критичных информационных ресурсов после внедрения системы защиты информации

Актив	Угроза	Величина потерь (тыс.руб.)
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	12
	Заражение вирусами	22
	Разглашение, передача или утрата атрибутов разграничения доступа	39
	Применение технических средств для несанкционированного съема информации	31
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	44
Базы данных	Выход из строя оборудования информационных систем и оборудования	18
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	12
	Заражение вирусами	15
	Разглашение, передача или утрата атрибутов разграничения доступа	4
Документы и отчеты в печатном виде	Применение технических средств для несанкционированного съема информации	15
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	31
	Выход из строя оборудования информационных систем и оборудования	24
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	23
	Заражение вирусами	8
Литература и электронные издания для служебного пользования	Разглашение, передача или утрата атрибутов разграничения доступа	15
	Применение технических средств для несанкционированного съема информации	14
	Некомпетентное использование,	12

Актив	Угроза	Величина потерь (тыс.руб.)
	настройка или неправомерное отключение средств защиты	
	Выход из строя оборудования информационных систем и оборудования	15
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	8
Персональные компьютеры пользователей	Заражение вирусами	13
	Разглашение, передача или утрата атрибутов разграничения доступа	19
	Применение технических средств для несанкционированного съема информации	15
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	11
	Выход из строя оборудования информационных систем и оборудования	15
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	22
	Заражение вирусами	39
	Разглашение, передача или утрата атрибутов разграничения доступа	31
Результаты маркетинговых исследований	Применение технических средств для несанкционированного съема информации	44
	Некомпетентное использование, настройка или неправомерное отключение средств защиты	18
	Выход из строя оборудования информационных систем и оборудования	14
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	15
	Заражение вирусами	4
	Разглашение, передача или утрата атрибутов разграничения доступа	15
Персональные данные сотрудников	Применение технических средств для несанкционированного съема информации	31
	Некомпетентное использование, настройка или неправомерное	24

Актив	Угроза	Величина потерь (тыс.руб.)
	отключение средств защиты	
	Выход из строя оборудования информационных систем и оборудования	20
	Отключение или вывод из строя подсистем обеспечения функционирования информационных систем	8
	Заражение вирусами	15
	Разглашение, передача или утрата атрибутов разграничения доступа	14
Суммарная величина потерь, тысяч рублей		749