**Оглавление**

[Введение 4](#_Toc503431442)

[1 Теоретические основы обеспечения информационной безопасности на малых предприятиях 7](#_Toc503431443)

[1.1 Различные подходов к определению понятия информационной безопасности 7](#_Toc503431444)

[1.2 Система обеспечения информационной безопасности на малых предприятиях 13](#_Toc503431445)

[1.3 Математическая модель определения вероятности кражи данных с компьютеров малого предприятия 16](#_Toc503431446)

[2 Анализ системы информационной безопасности на предприятии ООО «Лазурит» 29](#_Toc503431447)

[2.1 Краткая характеристика предприятия ООО «Лазурит» 29](#_Toc503431448)

[2.2 Анализ и характеристика информационных ресурсов предприятия ООО «Лазурит» 32](#_Toc503431449)

[2.3 Оценка угроз и определения вероятности кражи информационных данных предприятия ООО «Лазурит» 37](#_Toc503431450)

[3 Разработка рекомендаций по совершенствованию системы информационной безопасности 42](#_Toc503431451)

[3.1 Методы и средства защиты информации на предприятии 42](#_Toc503431452)

[3.2 Разработка мероприятий по совершенствованию системы информационной безопасности 50](#_Toc503431453)

[Заключение 58](#_Toc503431454)

[Список использованных источников 60](#_Toc503431455)

# Введение

Развитие общества в последние десятилетия характеризуется стремительным проникновением во все сферы человеческой жизни новых информационно-коммуникационных технологий. Эти изменения привели к формированию качественно нового типа общества, получившего название «информационного». Компьютеризация существенно влияет на процессы обучения, на постановку и решение научных задач, на исследования в области мышления и процессов познания.

В настоящее время деятельность любой организации тесно связана с информационными технологиями. Электронная почта, поиск потенциальных клиентов в интернете, продвижение в социальных сетях, использование IM-мессенджеров для корпоративного общения, а также онлайн-банкинг – вот без чего невозможно представить работу малого предприятия. Бизнес зависим от интернета – это факт, однако интернет таит в себе множество угроз. В соответствии с анализом «лаборатории Касперского» 96% малых предприятий в России за 2014 год столкнулись с киберугрозами.

Актуальность выбранной темы обусловлена тем, что в современных условиях процесс успешного функционирования и экономического развития российских предприятий во многом зависит от совершенствования их деятельности в области обеспечения экономической и информационной безопасности.

Целью данной работы является исследование основ обеспечения информационной безопасности и оценка вероятности кражи данных с компьютеров малого предприятия.

Исходя из поставленной цели в рамках данной работы предлагается решение следующих задач:

- изучение различных подходов к определению понятия информационной безопасности;

- рассмотрение системы обеспечения информационной безопасности на малых предприятиях;

- построение математической модели определения вероятности кражи данных с компьютеров малого предприятия;

- анализ и характеристика информационных ресурсов предприятия ООО «Лазурит»;

- оценка угроз и определения вероятности кражи информационных данных предприятия ООО «Лазурит»;

- выявление методов и средств защиты информации на предприятии;

- разработка мероприятий по совершенствованию системы информационной безопасности.

Объектом исследования в работе является малое предприятие ООО «Лазурит», а именно салон «Леонардо».

Предметом исследования в работе выступает система обеспечения информационной безопасности.

В данной работе были использованы следующие работы в области исследования особенностей безопасности информационных ресурсов: Баранова А.П., Гончарова О.И., Донской, Е. Н., Есаулова В.Т., Козуновой С.С., Конотопова М.В., Ляпиной И.Р., Ломазова А.В., Мельникова Д.А., Мухина И.Н., Петрова С.В., Полунина А., Поляковой Т.А., Родиной Ю.В., Росенко А. П., Окулова Н.С., Савченко И.А.,Прокофьева Д.Н. , Суглобова А.Е., Тимофеева А.М., Шаньгина В.Ф., Шамсуева М.Х. и др.

Методологической основой данной работы послужили методы: анализ литературы, нормативно–правовой документации по теме работы, изучение и обобщение отечественной и зарубежной практики, графоаналитический метод, математическое моделирование.

Теоретическое значение исследования заключается в изучении теоретических основ обеспечения информационной безопасности в малых предприятиях.

Практическое значение исследования состоит в разработке мероприятий по совершенствованию системы информационной безопасности.

Структура работы представлена введением, тремя главами и заключением. Первая глава посвящена изучению теоретических основ обеспечения информационной безопасности на малых предприятиях. Во второй главе проанализирована система информационной безопасности на примере предприятия ООО «Лазурит». Третья глава представлена разработкой рекомендаций по совершенствованию системы информационной безопасности.

# 1 Теоретические основы обеспечения информационной безопасности на малых предприятиях

* 1. **Различные подходов к определению понятия информационной безопасности**

Издавна считалось, кто владеет информацией, тот владеет ситуацией. Поэтому еще на заре человеческого общества возникает разведывательная деятельность, поэтому появляются государственные и коммерческие секреты, а в период войн военные.

Стремление сохранить в тайне от других то, что дает преимущество и власть, видимо является главной мотивацией людей в исторической перспективе. Многие собственники в целях защиты своих интересов засекречивают информацию и тщательно ее охраняют или патентуют.

Засекречивание информации приводит к постоянному совершенствованию средств и методов добывания охраняемой информации и к совершенствованию средств и методов защиты информации.

В мировой практике сначала применялись термины «промышленная тайна», «торговая тайна», «тайна кредитных отношений», т.е. название тайны увязывалось с конкретной сферой деятельности.

Российский юрист В. Розенберг сделал попытку объединить эти названия в одном «промысловая тайна» и даже выпустил в 1910 году одноименную книгу. Однако термин не прижился. И в Российской империи и за рубежом окончательно утвердился термин «коммерческая тайна», объединивший тайну любой деятельности, имеющей целью извлечение прибыли.

В России в ноябре 1917 года коммерческая тайна была отменена. Во время НЭПа она неофициально «возродилась», но в дальнейшем использовалась лишь внешнеторговыми предприятиями СССР при контактах с другими странами, однако отечественной законодательной основы под этим не было.

Коммерческая тайна в современной трактовке – информация, данные, сведения, объекты, разглашение, передача или утечка которых третьим лицам могут нанести ущерб интересам или безопасности обладателя.

Стандарт ISO/IEC 17799 определяет информационную безопасность как обеспечение конфиденциальности, целостности и наличия информации.

Безопасность это не только защит от преступных посягательств, но и обеспечение сохранности (особенно электронных) документов и информации, а также меры по защите важнейших документов и обеспечению непрерывности и/или восстановлению деятельности в случае катастроф.

Под информационной безопасностью следует понимать защиту субъектов информационных отношений. Основные ее составляющие конфиденциальность, целостность, доступность.

Таким образом, информация признается активом, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Одним из первых российских законов, посвященных вопросам информационной безопасности, следует считать Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года. В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области, регулируются отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Также в законе представлены определения основных понятий в сфере информационной безопасности.

Так, информационные технологии определяются как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов; информационная система – как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств; обладатель информации – как лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам и т.д.

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации представлены в Стратегии национальной безопасности РФ (2015) и Доктрине информационной безопасности РФ (2016). В Стратегии национальной безопасности РФ информационная безопасность рассматривается как неотъемлемая составляющая национальной безопасности России, поскольку «все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории…. Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий»[[1]](#footnote-1).

В Доктрине информационной безопасности РФ информационная безопасность определяется как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[[2]](#footnote-2).

Информационная безопасность – механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;

- целостность: достоверность и полноту информации методов ее обработки;

- доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Другими важными компонентами, которым большое внимание уделяется профессионалами в области компьютерной безопасности, являются контроль над доступом и строгое выполнение обязательств.

Контроль над доступом подразумевает не только факт, что пользователь имеет доступ только к имеющимся ресурсам и услугам, но и тот факт, что у него есть право доступа к ресурсам, которые он законно ожидает. Что касается строгого выполнения обязательств, то это подразумевает невозможность отказа пользователям того, что он отправил сообщение и наоборот. Существенными проблемами, связанными с обеспечением компьютерной безопасности, также являются борьба с компьютерной преступностью (попытки предотвращения, обнаружения атак) и конфиденциальность (анонимность) в киберпространстве.

В развитых зарубежных государствах (США, государства Европейского Союза, Канада и др.) защита национальных интересов от злоупотреблений в использовании информационно–коммуникационных технологий трактуется в контексте «кибербезопасности» и «сетевой безопасности».

«Кибербезопасность» рассматривается как защищенность от внешних и внутренних угроз безопасности киберпространства. Это пространство образуется взаимосвязанной сетью инфраструктур, обеспечивающих реализацию информационных технологий различного назначения.[[3]](#footnote-3)

В Стратегии обеспечения национальной безопасности киберпространства США (2011 г.) отмечается, что политика государства направлена на «защиту от нанесения ущерба работе информационных систем критических инфраструктур и, таким образом, на содействие защите людей, экономики и национальной безопасности США». При этом государство стремится, с одной стороны, уменьшить уязвимость объектов киберпространства к угрозам «прежде, чем они могут нанести ущерб кибернетическим системам, поддерживающим критические инфраструктуры страны, а с другой – гарантировать, что такие нарушения киберпространства будут нечастыми, будут иметь минимальную длительность, с нарушениями можно будет справиться и такие нарушения будут причинять наименьший возможный ущерб».

Общая схема явлений, охватываемых понятиями «информационная безопасность», «кибербезопасность» и «сетевая безопасность» представле-на на рисунке 1.1.



Рисунок 1.1. – Соотношение понятий «информационная безопасность», «кибербезопасность» и «сетевая безопасность»

Понятие «сетевая безопасность» – защищенность глобальных и национальных телекоммуникационных сетей от нежелательного доступа в сеть со стороны третьих лиц, от нарушения сохранности данных и эффективного функционирования сети в целом.

В структуре регулируемых правом общественных отношений в области обеспечения информационной безопасности выделяются следующие основные составляющие:

– объекты информационной безопасности;

– угрозы информационной безопасности;

– субъекты информационной сферы[[4]](#footnote-4).

Информационная сфера образуется совокупностью информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений

Распространение информации может быть либо движущим, либо сдерживающим фактором развития всех сторон жизни. Соответственно, как справедливо писал В.Т. Есаулов, плодами общественного прогресса пользуются различные силы, в том числе и деструктивные, что ведет к возникновению принципиально новых угроз жизнедеятельности отдельного человека, социальной группы, функционированию государств и мирового сообщества в целом.[[5]](#footnote-5)

Это требует более подробного рассмотрения самого понятия «угроза информационной безопасности РФ».

Исследователи предлагали разнообразные варианты трактовки термина:

– угрозы информационной безопасности – это использование различных видов информации против того или иного социального (экономического, военного, научно-технического и т. д.) объекта с целью изменения его функциональных возможностей или полного поражения;

– угрозой информационной безопасности называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или компоненты автоматизированной информационной системы может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений;

– угрозы информационной безопасности – это различные обстоятельства (условия, факторы состояния), т.е. опасные воздействия на информацию, информационную инфраструктуру, реализацию правового статуса человека и гражданина в области информационной деятельности, а также опасные действия, связанные с причинением вреда реализации национальных интересов, связанных с этими объектами.

## 1.2 Система обеспечения информационной безопасности на малых предприятиях

Для каждого предприятия внешние и внутренние угрозы могут быть как сугубо индивидуальными, так и распространенными во всей экономической среде. Учитывая их количество и разнообразие можно сделать вывод, что надежная защита любой организации возможна только при комплексном и системном подходе к ее организации.

Малый и средний бизнес (МСБ) в России, в последнее время, имеет жизненно важное значение для роста экономики и играет значительную роль в обеспечении занятости населения субъектов РФ. Понятие МСБ можно охарактеризовать как преимущественно устойчивые и рентабельные предприятия, хорошо структурированные, с квалифицированным менеджментом и хорошо отлаженным механизмом финансирования, где семья и друзья выступают не второстепенным фактором.

Одной из главных проблем в развитии предприятий МСБ является обеспечение информационной безопасности. Как правило, предприятия выделяют не более 10% своего дохода на защиту коммерческих интересов, а чаще не считают это необходимым. В настоящее время, сохранность и конфиденциальность информации – один из жизненно важных аспектов для функционирования предприятия. Таким образом, информационная безопасность занимает одно из ключевых мест при организации деятельности любого бизнеса[[6]](#footnote-6).

На современном этапе развития предпринимательской деятельности большое значение уделяется не банковским картам физических лиц, а счетам и конфиденциальной информации организаций, потеря или искажение которой приносит финансовые и организационные проблемы, К такой информации можно отнести:

- финансовые отчеты;

- базы данных клиентов;

- деловая переписка;

- детали конкретных сделок;

- интеллектуальная собственность;

- бизнес планы.

Система экономической безопасности предприятия (СЭБ) – это комплекс организационно - управленческих, режимных, технических, профилактических и пропагандистских мер, направленных на качественную реализацию защиты интересов предприятия от внешних и внутренних угроз.

Особенностью и, одновременно, сложностью при построении системы экономической безопасности для малого предприятия является тот факт, что ее действенность во многом зависит от человеческого фактора. Как показывает практика, даже при наличии на предприятии профессионального специалиста по обеспечению экономической безопасности и современных технических средств, добиться желаемых результатов сложно, пока в коллективе каждый сотрудник не осознает важность и необходимость внедряемых мер экономической безопасности.

В настоящее время взаимосвязь экономической и информационной безопасности является очевидной. Подавляющее большинство расчетов, денежных переводов, передачи стратегически важных данных производится в электронном виде. Следовательно появляются уязвимости, связанные с несовершенством защиты информационных технологий, которыми активно пользуются злоумышленники.

В последнее время отмечается рост кибератак именно на небольшие компании. Это связано с тем, что малый и средний бизнес не обладает средствами высокоуровневой защиты, которые используют крупные предприятия. Ограниченный объем затрат на обеспечение информационной безопасности делает малые предприятия особенно уязвимыми.

Малый и средний бизнес, в отличие от больших компаний, не считает приоритетной задачу разработки четкой стратегии развития IT - инфраструктуры своего предприятия, на первое место ставится продуктовая, операционная или маркетинговая деятельность.

Отсюда и возникают проблемы, связанные с информационной безопасностью. Немаловажной причиной является отсутствие квалифицированного персонала, в редких случаях небольшие компании могут похвастаться наличием в штате IT - специалиста.

Обычно его функции выполняет опытный пользователь из числа штатных сотрудников или, в лучшем случае, приходящий системный администратор.

Малым и средним предприятиям доступна большая гибкость при решении вопросов информационной безопасности. Они могут выбрать различные аппаратные комплексы, специализированное программное обеспечение для установки на стандартные серверы или обратиться к внешним поставщикам, предоставляющим услуги информационной безопасности[[7]](#footnote-7).

Таким образом можно сделать вывод, что даже для малого предприятия вопросы информационной безопасности являются важными и актуальными. Существующие тенденции говорят о том, что малые предприятия, в силу отсутствия эффективной системы обеспечения экономической и информационной безопасности, являются наиболее привлекательными целями для атак со стороны злоумышленников. Современные методы обеспечения информационной безопасности позволяют прогнозировать, предотвращать и ликвидировать угрозы информации при сравнительно не больших затратах, однако на данный момент руководство большинства малых организаций не считает необходимым наличие системы обеспечения информационной безопасности.

## 1.3 Математическая модель определения вероятности кражи данных с компьютеров малого предприятия

Известно, что безопасность информации ограниченного распространения (ИОР) обеспечивается на всех стадиях её жизненного цикла. Однако, с точки зрения соблюдения конфиденциальности информации, важнейшим этапом является этап использования ИОР по назначению. Исследования показывают, что именно на этом этапе имеет место наибольшее количество несанкционированных воздействий. В то же время анализ статистических данных показывает, что большинство случаев несанкционированного доступа к ИОР связаны с так называемыми антропогенными факторами. В свою очередь антропогенные факторы обусловлены деятельностью или бездеятельностью человека, приводящей к преднамеренным или непреднамеренным ошибкам, как собственника, так и пользователей конфиденциальной информации. Это связано с нарушением правил обращения с конфиденциальной информацией, недостаточным уровнем знаний, умений и практических навыков по применению существующих средств и методов защиты информации. Указанные обстоятельства свидетельствуют о необходимости рассмотрения АИС как сложной человеко-машинной системы, для которой характерны признаки, присущие сложным системам.

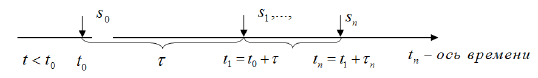
Практика показывает, что оптимизация процесса обеспечения безопасности ИОР возможна на основе разработки новых, более современных защитных механизмов с учетом воздействия на человеко-машинную информационную систему различных угроз.

Это связанно с тем, что существующие методы и методики, применяемые для оценки безопасности ИОР, не ориентированы на получение количественных результатов. В связи этим актуальной научной проблемой, обусловленной острой потребностью обеспечения безопасности ИОР, является разработка методов, адаптированных к процессам и явлениям, возникающим в человеко-машинных информационных системах направленных на количественную оценку таких проявлений .

Как показано в основу методов исследования безопасности ИОР может быть положено математическое описание процесса воздействия на АИС и ее структуры элементы различных угроз, вследствие чего, система может переходить в различные состояния, обусловленные проявлением или не проявлением угроз, возникновение или не возникновением особой ситуации, нарушением безопасности ИОР, последствиям от реализации различных угроз и величиной ущерба, наносимого собственнику ИОР[[8]](#footnote-8).

Понятие Марковского случайного процесса применительно к АИС.

Пусть на АИС в произвольный момент времени ti воздействует i-я угроза. В результате такого действия АИС переходит из состояния S0 в состояние Si. Представим процесс перехода АИС из S0 –го состояния Si  - е состояние как это показано на рис .1.2



­Рисунок 1.2. - Процесс перехода АИС из S0 ­– го состояния в S1  -е состояние в результате воздействия i-й угрозы можно представить следующим образом

Пусть в момент времени t<t0 АИС находилась в стационарном состояние предшествующем воздействию воздействию i-й угрозы. Такое состояние характеризует предысторию процесса – прошлое состояние АИС до момента времени t0 . В момент времени t0 на АИС воздействует i- я угроза, в результате которой АИС за время t1=t0+τ переходит в состояние S0-о в состояние S1 –e. Если такой процесс соответствует Марковскому случайному процессу, то можно предсказать такой переход , учитывая только настоящее состояние АИС –S0 и, забыв о ее предыстории. Само состояние S0 зависит от прошлого, но, как только оно достигнуто, о прошлом состояние можно забыть.

Таким образом, Марковском случайно процессе будущие состояние АИС зависит от прошлого только через настоящие.

Итак, случайный процесс применительно к АИС называется Марковским , если для любого момента времени t0 вероятно характеристики АИС в будущем зависят только от ее состояния в данный момент t0 и не зависят от того , когда и как АИС пришла в это состояние.

Из выше сказанного следует, что для такого случайного процесса характерны: случайная смена состояний АИС и вероятностная связь между предшествующими и последующими состояниями; зависимость между случайной сменой состояний АИС и временем воздействия на АИС различных угроз.

Процесс называется процессом с непрерывным временем, если моменты возможных переходов из состояния *в состояние не фиксированы заранее, а не определены, случайны, т.е. переход может осуществляться в* любой момент времени[[9]](#footnote-9).

Для Марковского случайного процесса с непрерывным временем существует закономерность, что время между наступлениями того или иного события является случайным, но подчиненным определенному закону. Этот закон называется показательным, а именно:

*P(t)=1-*  (1.1)

где t – время воздействия угроз на АИС ;

λ – интенсивность воздействия;

P(t) - вероятность воздействия угрозы за промежуток времени ∆t.Частные случаи, вытекающие из выражения (1.1):

если ∆t → 0, тогда P(t)=0; если ∆t → ∞, тогда P(t)=1.

Для описания поведения такого случайного Марковского процесса используется интенсивность переходов λij(t), показывающее вероятность перехода системы, находящейся в состоянии j в состоянии i в момент времени t можно составить систему дифференциальных уравнений,

*Pj(t)=ij(t)Pi(t),*

решение которой определяет вероятность Pj(t) нахождение системы *j –* м состоянии в момент времени t.

При однородном во времени непрерывном Марковском случайном процессе условные интенсивности переходов, записываются в виде матрицы,

*А=||||,* (1.2)

постоянны. Тогда система дифференциальных уравнений переходит в систему алгебраических уравнений, которую легко решить, используя преобразования Лапласа.

Поток событий – это последовательность однородных событий, следующих одно за другим в случайные моменты времени, например поток угроз (внутренних, внешних и др.).

Важной характеристикой потока событий является его интенсивность λ- среднее число событий в единицу времени. Интенсивность потока λ может быть постоянна (λ=const) или переменна (λ=var).

Поток событий называется регулярным, если события следуют одно за другим через равные промежутки времени.

Поток событий называется стационарным, если его вероятностные характеристики не зависят от времени.

Поток событий называется потоком без последствий, если для любых двух непересекающихся интервалов времени и , число событий, попадающихся на один из них, не зависит от того, сколько событий попало на другой.

Наглядной формой представления таких воздействий являются графы, с помощью которых представляются все возможные варианты событий, которые могут иметь место при воздействии на систему внешних факторов. Вершины графа обозначают события, а ребра – связи между ними. На каждом ребре графа можно указать соответствующую данному событию вероятность. Такой граф называется взвешенным. В теории вероятностей он носит название дерева событий или дерева возможных исходов. Граф состояний позволяет легко посчитать вероятности возможных исходов после нескольких этапов процесса.

Другой вид графа – ориентированный взвешенный граф, вершины которого обозначают не события, а состояния системы. Вершины графа соединяются стрелками, указывающими направление возможных переходов из состояния в состояние.

Если вероятности переходов связаны только с предшествующими состояниями, то реализуется процесс без последствий, или простая цепь Маркова.

Если вероятность переходов связана с учетом более ранних состояний (предыстории), то цепь Маркова называют сложной.

Если полагают, что на рассматриваемом отрезке времени переходные вероятности не зависят от номера испытания, то такая цепь Маркова называется однородной.

Цепи Маркова, в которых переходные вероятности зависят от номера испытания (различных факторов, способствующих переходу системы в различные состояния) называются неоднородными.

Переходная матрица, как правило, дополняется матрицей начального состояния. Существует два способа задания начального состояния: детерминированный (неслучайный); случайный.

Такой упорядоченный набор величин (чисел) называется вектором, а сами величины или числа – компонентами вектора. Различают вектор-строку и вектор- столбец. В данном случае понятие вектора в абстрактном пространстве является пространством вероятностей.

Постановка задачи. Допущения. Граф состояния системы**.** Пусть на АИС за конечное время *τ* воздействует n простейших потоков угроз с интенсивностями. λi, i=1,n.

Пусть μi – интенсивность парирования последствий *i*-й угрозы. Соответственно,Ri – вероятность парирования, Ri – вероятность не парирования *i*-й угрозы.

Тогда, μi, Ri – интенсивность парирования, а μi, Ri – интенсивность не парирования последствий воздействия на АИС потока угроз.

Допущения:

- поток парирования и не парирования угрозы простейший;

- возможности по парированию последствий воздействия на АИС *i-*й угрозы не ограничены, т.е. μi,≥λi

- так как рассматриваются простейшие потоки, то появление одновременно двух и более угроз является невозможным событием.

Для определения вероятности благополучного исхода при воздействии на АИС потока угроз представим систему АИС в виде графа (см. рисунок 1.3). n

В соответствии с рисунком 1.3. можно составить матрицу интенсивностей перехода вида (1.3).

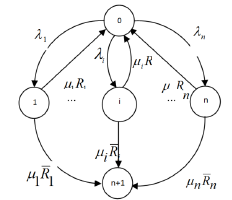


Рисунок 1.3. – Граф состояний АИС[[10]](#footnote-10)

- λ0 … λi … λn  0

µi·Ri … - µi … 0 µiRi

ǁ λik = (1.3)

µnRn … 0 … -µn  µnRn

0 …0 …0 …0

где λ0=λ1+λ2+…+λn, *j=k=*1,2,…,*n+*2

В соответствии с рисунком 1.2. АИС в момент времени может находиться в одном из следующих состояний:

- состояние «0» – поток угроз за время τ не проявился;

- состояние «1», …,*i* , …,n – одна из угроз проявилась;

- состояние «n+1 » – неблагополучное поглощающее состояние, при котором угроза реализовалась.

Матрица (1.3) обладает следующими свойствами: диагональные члены матрицы равны сумме остальных элементов данной строки, взятых с обратным знаком; сумма всех элементов каждой строки равна нулю; число нулевых строк в матрице интенсивностей переходов соответствует количеству поглощающих со- стояний; интенсивность перехода равна нулю при отсутствии стрелки.

Определение вероятностей перехода АИС в каждое возможное состояние**.** Для определения вероятностей перехода АИС в каждое возможное состояние воcпользуемся системой дифференциальных уравнений Колмогорова, в соответствии с которыми можно написать.

=-*P0(τ)Σni=2λi*+Σµ*iRiPi(τ)*,

=λiP0(τ) −µiPi(τ), (1.4)

=Σn*i=1*µi*RiPi(*τ).

Применяя к системе дифференциальных уравнений (1.4) прямое преобразование Лапласа с учетом исходных данных *P0(*0)=1, *Pi(0)=Pn+1(0)=0*  и с учетом того, что i(τ)*e-Sτdτ* =−*Pi(0)*+*SPj(S),* получим следующие выражения для определения вероятностей в соответствии с графом состояний (см. рисунок 1.3)

-P0(0)+SP0(S)=-λ0P0(S)+iRiPi(S),

-Pi(0)+SPi(S)=λiP0(S)-µiRiPi(S), (1.5)

-Pn+1(0)+SPn+1(S)=iRi(S),

где Pi(S)= i(τ)e-St*dτ –*искомое изображение.

При начальных условиях система уравнений (1.5) примет вид:

(S+λ0)P0(S)=iRi(S)=1,

-λiP0(S)+(S+µi)Pi(S)=0, (1.6)

-iRiPi(S)+SPn+i(S)=0.

По правилу Крамера искомые изображения определяются отношением:

Pi(S)=, *j*=1,n, (1.7)

где ∆(S)=S[(S+λ0)+µi)-iµiRi+µ*l*)] – главный определитель системы; ∆j(S) – частный определитель системы, находится из главного определителя путем замены j-го столбца коэффициентами, стоящими в правых частях уравнений (1.6).

Частные определители, полученные с помощью введения определителей по индукции, будут равны:

∆0(S)S+µ*l*),

∆i(S)=Sλ0+ µ*l*), (1.8)

∆*n+1*(S)=*iµi*R*i*+µ*l*)].

С учетом указанного и при условии, что *ρj*(S)=,*ρ*(S)= система уравнений (1.6) примет вид:

P0(S)===,

P*i*(S)===, (1.9)

P*n*+1(S)===.

Окончательно с учетом (1.8) выражения (1.9) примут вид:

Тогда из (10) следует, что вероятность благополучного исхода от воздействия на АИС n независимых потоков внутренних угроз определяется следующим выражением:а вероятность противоположного события, т.е не-благополучного исхода будет равна

Частные случаи:

1.Интенсивность парирования i-го потока угрозы µi  равно интенсивности воздействия i-го потока угрозы

Пусть µi  ,т.е интенсивность парирования последствий i-го потока угроз равна интенсивности i-го потока угроз.

Тогда изображения вероятностей можно представить следующим образом:

Функции qi(S) и ρ(S) могут быть представлены в виде полиномов с коэффициентами bi и ci , а именно :

Из выражения (1.12) следует, что изображения вероятностей Pj (S) являются правильными рациональными дробями, у которых степени полиномов числителей численно меньше полиномов знаменателей.

Тогда применяя к (1.12), табличное преобразование Лапласа, получим следующее выражение для характеристических оригиналов искомых вероятностей:

*e*Skτ , если Pj (S) =

(1.13)

*e*Skτ , если Pj (S) =

G-1(Pj(S)) =

*a* [ + ], если Pj (S) = .

где ω – количество корней *i-* го характеристического уравнения; *a -* константа.

Тогда с учетом нормированного условия , где Pj  -вероятность нахождения АИС в *i –* м состоянии, можно записать, что конечная вероятность

PБИ(τ) = (1.14)

Характеризует благополучный исход, а

QБИ(τ) =1- =Pn+1(τ)

Неблагополучный исход от воздействия на АИС различных угроз.

2. Оценки вероятностей последствий от реализации угроз безопасности ИОР с учетом воздействия на АИС одного потока угроз.Для практических расчетов наиболее часто имеет случай, когда на АИС воздействует один поток угроз, т.е. *n*=1.

Пусть на АИС, в течении времени τ, воздействует один поток угроз с интенсивностью - λ, интенсивность парирования - µ и вероятность парирования потока угроз – R/

Тогда из системы уравнений (1.13) при n=1 изображения вероятностей примут следующий вид:

P0(S) = =,

P1(S) = =, (1.16)

Pn+1(S) = =,

где ρ(S) = S2+Sc1+c0, с1=λ+µ, с0=λµR.

Применяя к (1.16) обратное преобразование Лапласа с учетом (1.14) и (1.15) получим выражения для определения искомых вероятностей, а именно:

P0(τ) P0(τ) = [(µ-λ-˄) -(µ-λ-)]; (1.17)

где

Тогда с учетом (14) и (15) вероятность благополучного исхода от воздействия на АИС одного потока угроз будет равна

P*БИ*(*τ*)=P0(*τ*)+P(*τ*), (1.20)

а вероятность неблагополучного исхода

Q*БИ*(*τ*)=Pn+1(*τ*) (1.21)

Случай, когда λ=µ. Тогда выражения (17), (18),(19) будут иметь вид:

P0(τ)=*e*-λt[τ+τ], (1.22)

P1(τ)=*e*-λt[τ-τ],

Pn+1(τ)=1- *e*-λt[τ-]

Конечные вероятности (1.17), (1.18) и (1.19) определяются используются выражения (1.22), (1.23) и (1.24).

Учитывая переходные интенсивности для матрицы (1.3), система дифференциальных уравнений имеет следующий вид:

Применяя к системе дифференциальных уравнений (1.25) принятое преобразование Лапласа с учетом исходных данных P0(0)=1, P1(0)=P2(0) = P3(0)=0 представляется возможным получить выражения для определения вероятностей P0(),P1(),P2(),P3().

Обоснована применимость Марковских случайных процессов для оценки влияния различных угроз на безопасности конфиденциальной информации. Дано понятие Марковского случайного процесса с учетом воздействия АИС различных угроз. Показано, что Марковские случайные процессы могут быть использованы для оценки вероятности благополучного или неблагополучного исхода при воздействие на АИС угроз. Для определения указанных вероятностей целесообразно представит последовательность перехода АИС из одного i-го состояния в другое j-е виде графа состояний, которые называются цепью Маркова.

# 2 Анализ системы информационной безопасности на предприятии ООО «Лазурит»

## 2.1 Краткая характеристика предприятия ООО «Лазурит»

Объектом исследования в данной работе выступает ООО «Лазурит», а конкретно салон «Леонардо», основным видом деятельности которого является продажа лакокрасочных изделий.

Рассмотрим организационную структуру, приведенную на рисунке 2.1.

Директор

Административный отдел

Бухгалтер

Работники склада

Зав. складом

Торговый агент

Склад

Отдел продаж

Коммерческий отдел

Зам. директора

Администратор зала

Обслуживающий персонал

Продавец-кассир

Продавец-консультант

Рисунок 2.1. – Организационная структура салона «Леонардо»

Как показывает рисунок 2.1, управляет данным субъектом директор, которому подчинены заместитель директора и административный отдел. В состав административного отдела входит торговый агент, в обязанности которого входят: поддержание и расширение клиентской базы; заключение договоров с поставщиками; контроль кредиторской задолженности; мерчендайзинг; презентация товаров и услуг.

В состав обслуживающего персонала входят уборщики помещений (торгового зала, склада и административного помещения).

Курированием отдела продаж и склада занимается заместитель директора. Складом управляет заведующий складом, а который координирует работу сотрудников склада.

Стоит отметить, что в организации отсутствует централизованная бухгалтерия и данный участок представлен одним бухгалтером.

Рассмотрим реализацию признаков малого бизнеса на примере ООО «Лазурит». Динамика и структура численности персонала ООО «Лазурит» приведены в таблице 2.1.

Таблица 2.1 - Динамика и структура численности работников ООО «Лазурит»

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Показатель | 2014 год | Уд. вес,% | 2015 год | Уд. вес,% | 2016 год | Уд. вес,% |
| Численность - всего: | 22 | 100 | 16 | 100 | 16 | 100 |
| руководство | 2 | 9,09 | 2 | 12,50 | 2 | 12,50 |
| администрация | 4 | 18,18 | 3 | 18,75 | 3 | 18,75 |
| администратор зала | 2 | 9,09 | 2 | 12,50 | 2 | 12,50 |
| продавец-консультант | 8 | 36,36 | 8 | 50,00 | 7 | 43,75 |
| продавец-кассир | 3 | 13,64 | 3 | 18,75 | 3 | 18,75 |
| работники склада | 3 | 13,64 | 2 | 12,50 | 2 | 12,50 |

Таблица 2.1 показывает, что динамика численности персонала ООО «Лазурит» соответствует критериям малого бизнеса, при этом необходимо отметить снижение динамики численности персонала за анализируемый период. Так же стоит отметить, что в структуре численности персонала наибольший удельный вес занимают продавцы-консультанты – более 40% по данным на 2016 год.

Далее для определения эффективности деятельности ООО «Лазурит» проанализируем результаты финансовой деятельности, представленные в таблице 2.2.

Таблица 2.2 – Анализ результатов финансовой деятельности ООО «Лазурит»

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Показатель | 2014 год | 2015 год | | 2016 год | | Отклонение 2016 года от | | | | | |
| 2014 года | | | | 2015 года | |
| тыс. руб. | | | % | тыс. руб. | % |
| Доходы и расходы по обычным видам деятельности | | | | | | | | | | |  |
| Выручка от продажи товаров, работ и услуг | 58523 | | 58033 | | 56 646 | | -1 877 | 96,79 | | -1 387 | 97,61 |
| Себестоимость | 49515 | | 32726 | | 29211 | | -20304 | 58,99 | | -3515 | 89,26 |
| Валовая прибыль | 9008 | | 25307 | | 27 435 | | 18 427 | 304,56 | | 2 128 | 108,41 |
| Коммерческие расходы | 0 | | 0 | | 0 | | 0 |  | | 0 |  |
| Управленческие расходы | 0 | | 0 | | 0 | | 0 |  | | 0 |  |
| Прибыль (убыток) от продаж | 9008 | | 25307 | | 27 435 | | 18 427 | 304,56 | | 2 128 | 108,41 |
| Прочие доходы | 171239 | | 2621 | | 2107 | | -169132 | 1,23 | | -514 | 80,39 |
| Прочие расходы | 184525 | | 27638 | | 49678 | | -134847 | 26,92 | | 22040 | 179,75 |
| Чистая прибыль (убыток) отчетного периода | 917 | | 3429 | | 2 616 | | 1699 | 285,28 | | -813 | 76,29 |

Рисунок 2.2 – Динамика выручки ООО «Лазурит», тыс. руб

Как показывает рисунок 2.2., величина выручки, полученной по результатам 2016 года составила 56 646 тыс. рублей, что соответствует критериям малого бизнеса. Так же необходимо отметить снижение величины выручки в анализируемом периоде.

Рисунок 2.3. – Динамика чистой прибыли ООО «Лазурит»

Данные, приведенные в таблице 2.2 и на рисунках 2.2. и 2.3., свидетельствуют о рентабельной деятельности ООО «Лазурит»: по результатам трех анализируемых периодов организация получает прибыль. Основной причиной снижения величины полученной прибыли в 2016 году стало снижение объемов продаж на 2,39% в сравнении с предыдущим годом. Стоит отметить, что величина убытка, полученного по результатам 2016 года вдвое больше, чем в 2014 году, и более чем в 3 раза превышает результат 2015 года.

## 2.2 Анализ и характеристика информационных ресурсов предприятия ООО «Лазурит»

Формирование структуры информационной системы ООО «Лазурит» необходимо начинать с качественного анализа информационного поля предприятия, которое можно подразделить на внутреннее и внешнее. Внутреннее информационное поле объединяет следующую информацию:

- первичные документы;

- данные внутреннего документооборота (бумажного и электронного), включая приказы и распоряжения руководителя и администрации всех звеньев;

- данные бухгалтерского учета и другой обязательной отчетности за текущий и прошлые периоды;

- результаты анализа финансово-хозяйственной деятельности;

- другие данные.

На рисунке 2.4. представлены все информационные ресурсы ООО «Лазурит» и их взаимосвязи информационными потоками.

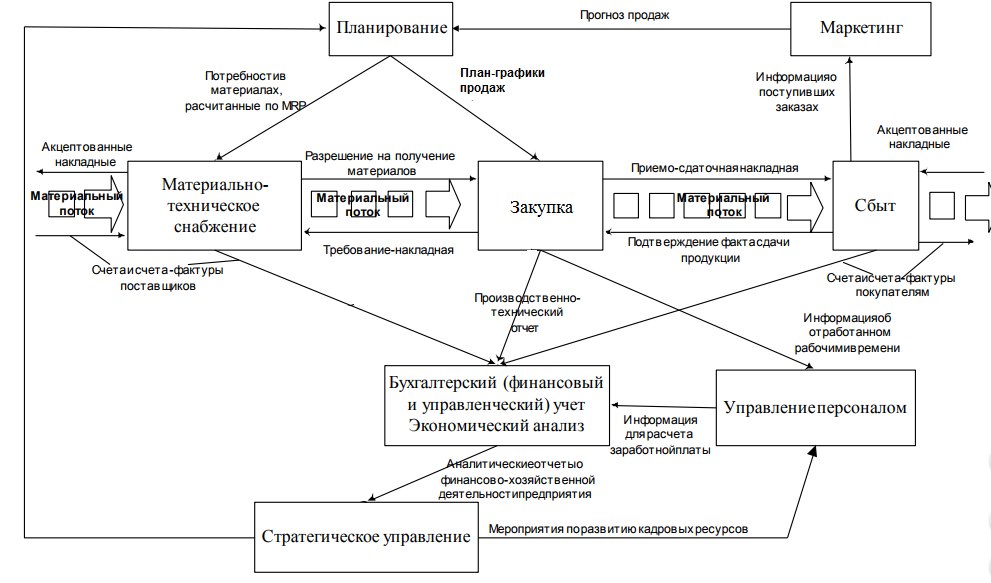


Рисунок 2.4 – Основные информационные ресурсы ООО «Лазурит», салон «Леонардо»

Информационный поток, обслуживающий движение материального потока. Материальный поток двигается от первичного источника (например, поставщика товара) через цепь транспортных и посреднических звеньев к конечному потребителю. На каждом этапе своего движения материальный поток сопровождается определенными первичными документами, которые фиксируют хозяйственные операции, и содержат информацию о состоянии материального потока.

Информационный поток, обслуживающий процесс управления ООО «Лазурит» - этот поток обслуживает основные функции управления предприятием: прогнозирование, планирование, организацию, регулирование, координацию, контроль, принятие решений и т.д. Для этого он выдает информацию о движении материального потока, но не в виде первичных документов, а в виде полученных на их основе сводных (агрегированных) показателей хозяйственной деятельности предприятия. Предоставление таких данных в информационную систему – это основная функция бухгалтерского (финансового и управленческого) учета, а также блока экономического анализа.

Важные информационные ресурсы обслуживают процесс управления персоналом предприятия. В них происходит поступление в систему бухгалтерского учета информации о количестве фактически отработанного времени, по этим данным происходит начисление заработной платы пенсионных и иных видов социальных отчислений. В рамках этого информационного потока проходят все кадровые приказы, распоряжения об изменениях штатного расписания и т.п.

Построенная модель информационных ресурсов и взаимосвязанных информационных потоков позволяет выделить логическую структуру модулей комплексной автоматизированной информационной системы ООО «Лазурит»:

1. Планирование и бюджетирование (план-прогноз продаж, планирование потребностей в товарах, распределении; финансовое планирование: синхронное планирование и оптимизация).

2. Управление сбытом (управление взаимоотношениями с клиентами CRM; ведение реестра договоров на поставку продукции; формирование приказов на отгрузку товара; управление складом; учет расчетов с покупателями, таможенное декларирование; электронная коммерция; печать приказов и страховых квитанций; формирование отчетности по отгрузке товаров; контроль ожидаемых зачетов и денежных средств в пути; ведение «кредитной линии» клиента).

3. Управление закупками (ведение реестра договоров на закупку товара; складской учет: оформление приходных и расходных документов, оформление накладных на внутреннее перемещение, оформление товарно- транспортных накладных, учет малоценных и быстроизнашивающихся предметов, формирование данных для секторов расчетов с поставщиками и подрядчиками, формирование отчетности по движению ТМЦ; учет запланированных поступлений; учет расчетов с поставщиками, управление и оптимизация цепочек поставок).

4. Управление персоналом (нормирование трудозатрат, штатное расписание и кадровый учет; табельный учет; учет «горячего стажа»; подготовка отчетности для ПФР).

5. Бухгалтерский учет (главная книга и баланс; учет основных средств: подготовка документации по поступлению, выбытию и перемещению основных средств, расчет амортизационных отчислений, формирование возрастной структуры оборудования; финансовые средства и расчеты: взаимозачетные; касса и банк; материальный учет запасов; реализация; налоговый учет; учет расчетов по подотчетным суммам; расчет заработной платы, учет кредитов сотрудникам; прочие бухгалтерские операции; подготовка отчетности для ГНИ).

6. Управление финансами и экономический анализ хозяйственной деятельности (калькуляция фактической себестоимости товара; формирование и анализ; анализ затрат на 1 рубль товарной продукции,

анализ дебиторской и кредиторской задолженности; экспортные и валютные операции; оценка текущей деятельности; анализ финансового состояния предприятия; формирование бюджетов и контроль их исполнения; анализ рентабельности).

7. Маркетинг (прогнозирование состояния рынка сбыта товаров; планирование рекламных компаний; прогноз изменения рынков сырья и основных материалов).

8. АРМы руководителя и аналитика (поддержка принятия решения DSS, стратегическое планирование).

9. Подсистема электронного документооборота (контроль исполнения

поручений; управление нормативно-технической документацией; договора на поставку товаров, на снабжение).

10. Служебное администрирование и управление политикой безопасности (управление доступом: настройка полномочий пользователей, организация пользовательских групп, ограничение доступа к данным; поддержание логической и физической целостности данных системы; операционный мониторинг действий пользователей; статистический контроль активности пользователей; мониторинг системных ошибок; контроль возникновения, анализ причины и сохранение контекста ошибок разработчика; конфигурация параметров системы: настройка на «владельца системы», настройка на специфику учета и организации хозяйственной деятельности, настройка системных параметров системы, настройка размещения данных).

Говоря о физической реализации выделенных логических блоков информационной системы ООО «Лазурит», следует отметить, что корпоративная информационная система строится как единый комплекс программно-технических и организационных решений, охватывающих все

технологические, финансовые и хозяйственные процессы, и объединяя все подразделения в единое информационное пространство.

## 2.3 Оценка угроз и определения вероятности кражи информационных данных предприятия ООО «Лазурит»

Для оценки возможных угроз информационных данных ООО «Лазурит» (салон «Леонардо») рассмотрим схему помещения салона с размещением источников информационных систем.

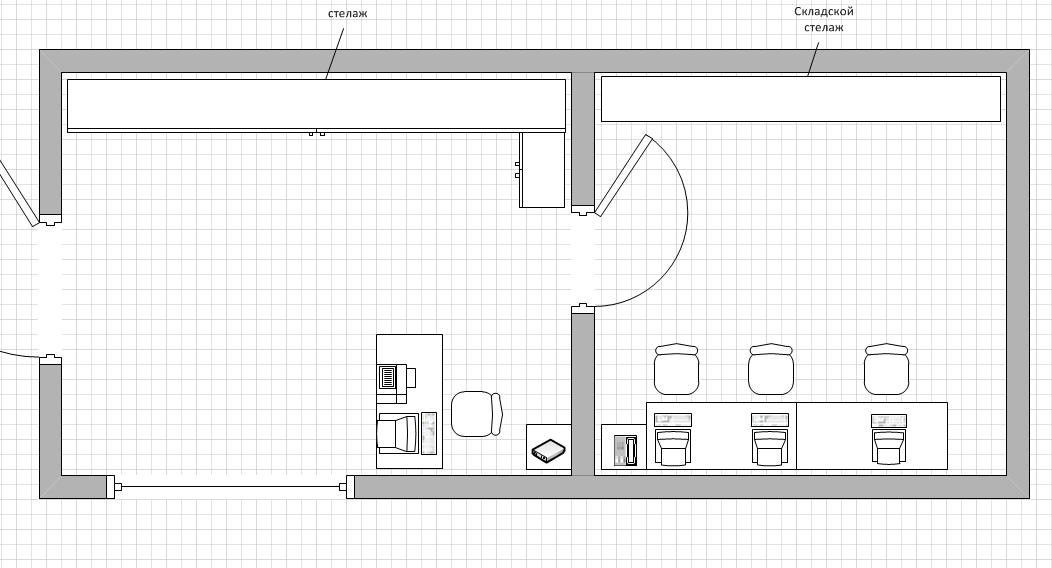


Рисунок 2.5 – Схема помещения салон

Итак, как показывает рисунок 2.5. сеть внутри салона построена по топологии «Звезда» посредством портового коммутатора. Компьютер в основном помещении подключен беспроводным соединением, 3 компьютера в подсобном помещении через кабель. Сам коммутатор подключен кабелем к серверной торгового центра.

Далее с целью оценки вероятности кражи информационных данных предприятия ООО «Лазурит» применим математическую модель, представленную в п. 1.3.

Показательный закон для исследуемого объекта будет выглядеть следующим образом:

*P(t)=1- =1 - =0,85*  (2.1)

где t – время воздействия угроз на АИС ;

λ – интенсивность воздействия;

P(t) - вероятность воздействия угрозы за промежуток времени ∆t.Частные случаи, вытекающие из выражения (2.1):

если ∆t → 0, тогда P(t)=0; если ∆t → ∞, тогда P(t)=1.

Как было показано выше, важной характеристикой потока событий является его интенсивность λ- среднее число событий в единицу времени. Интенсивность потока λ может быть постоянна (λ=const) или переменна (λ=var).

Для определения вероятности благополучного исхода при воздействии на АИС потока угроз по исследуемому объекту составим матрицу интенсивностей перехода вида.

- λ0 … λi … λn  0 -0,40 0,45 0,35 0

µi·Ri … - µi … 0 µiRi 0,25 0,40 0 0,45

ǁ λik = =

µnRn … 0 … -µn  µnRn 0,40 1 0 0,40

0 …0 …0 …0 0 0 0 0

где λ0=λ1+λ2+…+λn, *j=k=*1,2,…,*n+*2

Построенная матрица содержит совокупность состояний, которые означают:

- состояние «0» – поток угроз за время τ не проявился;

- состояние «1», …,*i* , …,n – одна из угроз проявилась;

- состояние «n+1 » – неблагополучное поглощающее состояние, при котором угроза реализовалась.

Для определения вероятностей перехода АИС в каждое возможное состояние воcпользуемся системой дифференциальных уравнений Колмогорова, в соответствии с которыми можно написать.

*=-P0(τ)Σni=2λi+ΣµiRiPi(τ) =-1 = 0,87 ,*

*=λiP0(τ) −µiPi(τ) = 0,40-0,33=0,07* (2.2)

*=Σni=1µiRiPi(τ)=Σni=10,33·1 =0,33*

Применяя к системе дифференциальных уравнений прямое преобразование Лапласа*,* получим следующие выражения для определения вероятностей:

*-P0(0)+SP0(S)=-λ0P0(S)+iRiPi(S) = -1+0=-0,45·1+ =-0,12*

*-Pi(0)+SPi(S)=λiP0(S)-µiRiPi(S) = 0+1=0,40·1-0,33=0,07,* (2.3)

*-Pn+1(0)+SPn+1(S)=iRi(S) = -1+1=* ,

где Pi(S)= i(τ)e-St*dτ –*искомое изображение.

При начальных условиях система уравнений примет вид:

(S+λ0)P0(S)=iRi(S)=1,

-λiP0(S)+(S+µi)Pi(S)=0, (2.4)

-iRiPi(S)+SPn+i(S)=0.

Частные определители, полученные с помощью введения определителей по индукции, будут равны:

*∆0(S)S+µl) = 1·+0,33) =1,33 ,*

*∆i(S)=Sλ0+ µl)= 0,40·+0,33) =0,53,*  (2.5)

*∆n+1(S)=iµiRi+µl)]=0,45·0,33·1=0,14.*

С учетом указанного и при условии, что *ρj*(S)=,*ρ*(S)= система уравнений примет вид:

P0(S)====1,

P*i*(S)====1, (2.6)

P*n*+1(S)====1.

Окончательно с учетом (2.5) выражения (2.6.) примут вид:

= = 0,74

= 0,39

Пусть µi  ,т.е интенсивность парирования последствий i-го потока угроз равна интенсивности i-го потока угроз.

Тогда изображения вероятностей можно представить следующим образом:

.

Тогда с учетом нормированного условия , где Pj  -вероятность нахождения АИС в *i –* м состоянии, можно записать, что конечная вероятность

PБИ(τ) = =0,67. (2.9)

Таким образом, полученная вероятность угроз информационных данных по исследуемому объекту составляет 0,67 (67%), что означает достаточно высокий уровень риска в рамках коммерческой деятельности.

Для предотвращения существующих угроз и ликвидации недостатков существующей системы безопасности информационных данных в ООО «Лазурит» необходима разработка направлений совершенствования.

# 3 Разработка рекомендаций по совершенствованию системы информационной безопасности

## 3.1 Методы и средства защиты информации на предприятии

В настоящее время невозможно представить направление малого бизнеса, не использующее информационные технологии для проведения финансовых расчетов, организации документооборота, рекламы своей деятельности, поиска поставщиков и покупателей, реализации онлайн-сервисов, использования информации как объекта товарно-денежных отношений.

Однако существуют факторы, которые могут не только дезорганизовать работу любого предприятия или организации, но и остановить на какое-то время всю деятельность.

Киберпреступники в последнее время большое внимание уделяют малому бизнесу, считая его сферой более легкого получения информации о персональных данных сотрудников и средств с банковских счетов работников и предприятия.

Причиной является то, что крупные компании уделяют большое внимание вопросам информационной безопасности: они имеют высококвалифицированных сотрудников IT-отделов, используют лицензионное программное обеспечение, хранят данные на собственных надежных серверах и способны вкладывать средства в обеспечение информационной безопасности.

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение. Источники угроз при этом делятся на внешние и внутренние. Источниками внутренних угроз являются:

- сотрудники организации;

- программное обеспечение;

- аппаратные средства[[11]](#footnote-11).

Внутренние угрозы могут проявляться в следующих формах:

- ошибки пользователей и системных администраторов;

- нарушения сотрудниками фирмы установленных регламентов бора, обработки, передачи и уничтожения информации;

- ошибки в работе программного обеспечения;

- отказы и сбои в работе компьютерного оборудования.

Максимальный ущерб бизнесу наносит уязвимости в программном обеспечении. Особенно остро этот вопрос стоит в случае использования бесплатного программного обеспечения, публичных облачных хранилищ данных и использования паролевой защиты для доступа к информационным ресурсам.

При установленных лицензионных информационных систем, использовании собственных серверов для хранения информации и обеспечения многофакторной защиты доступа к информационным ресурсам вероятность потерь информации значительно снижается. Однако указанные мероприятия требуют вложения средств. Одновременно существуют действия, которые одинаково вероятны и опасны в сегменте как крупного, так и малого бизнеса, например, утечка информации по преднамеренной или случайной вине сотрудников, потеря мобильных устройств сотрудниками, мошенничество сотрудников и т. д.

Причиной безответственного отношения к выполнению требований информационной безопасности является отсутствие знаний в области IT-безопасности и, соответственно, понимания важности точного соблюдения правил и требований.

К внешним источникам угроз относятся:

- компьютерные вирусы и вредоносные программы;

- организации и отдельные лица;

- стихийные бедствия.

Формами проявления внешних угроз являются:

- заражение компьютеров вирусами или вредоносными программами;

- несанкционированный доступ (НСД) к корпоративной информации;

- информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;

-аварии, пожары, техногенные катастрофы.

Внешние угрозы возникают в случае отсутствия установленных лицензионных программных продуктов, защищающих компьютер и информационную систему в целом от вредоносных программ.

Предлагаемое бесплатное или условно-бесплатное программное обеспечение никогда не будет поддерживать полный функционал средств защиты, существующих в коммерческих версиях: блокирование вирусов и шпионских программ, обеспечение безопасности покупок в Интернете, блокирование спама и фишинговых сообщений, защита конфиденциальности данных, наличие брандмауэра, предотвращение хакерских атак, защита денежных операций, предупреждение о подмене доменных адресов на мошеннические и другое[[12]](#footnote-12).

Игнорирование существующих внутренних и внешних киберугроз, низкий уровень инвестирования в средства информационной безопасности и в обучение сотрудников может привести к значительным финансовым и репутационным потерям.

Убытки от произошедших инцидентов складываются из расходов на внешнее профессиональное обслуживание, из упущенных бизнес-возможностей, а также ущерба от вынужденного простоя по причине блокирования IT-процессов компании и остановки деятельности на период восстановления информационных процессов и данных.

Существующая на предприятиях информация делится на общедоступную информацию и информацию с ограниченным доступом.

К общедоступной (открытой) информации относится:

- информация, подписанная руководством, для передачи вовне (например, для конференций, презентаций и т. п.);

- информация, полученная из внешних открытых источников;

- информация, находящаяся на внешнем web-сайте компании. Многие считают, что защищать открытую информацию не имеет смысла. Однако это не так: например, подмена информации на web-сайте компании, в зависимости от того, чем именно она будет заменена, может привести к тем или иным нежелательным последствиям различной тяжести.

Для защиты общедоступной информации достаточно применение минимальных средств и методов информационной безопасности: паролевая защита файлов и папок, использование встроенных механизмов защиты данных в MS Office. Данные средства позволяют защитить с помощью пароля файлы от ознакомления или изменения, запретить редактирование, форматирование или внесение любых изменений в документ, организовать защиту макросов, скрыть от просмотра определенные части документа, распределить ограничения для пользователей и добавить цифровую подпись.

К информации для внутреннего использования относится любая информация, используемая сотрудниками в рамках своих подразделений, тематических групп, которая:

- циркулирует между подразделениями и необходима для нормального их функционирования;

- является результатом работ с информацией из открытых источников (например, обзор рынка производимой продукции);

- не относится к информации конфиденциального характера;

- не относится к открытой информации[[13]](#footnote-13).

Для защиты информации для внутреннего использования необходимо применять все перечисленные выше механизмы защиты открытой информации, однако с гораздо большей ответственностью: при создании паролей применять пароли с увеличенным битовым пространством, использовать не только буквы и цифры, но и специальные символы, различать регистры.

Для удобства и скорости доступа паролевую защиту можно заменить на защиту на основе биометрии и ключи e-Token, применять электронную подпись, официально получаемую в удостоверяющих центрах.

Конфиденциальная информация – это документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ. Конфиденциальная информация не является общедоступной информацией и в случае разглашения способна нанести ущерб правам и охраняемым законом интересам предоставившего ее лица. Рассмотрим подробнее виды конфиденциальной информации: Персональные данные. Согласно Федеральному закону от 27.07.2006 N 152-ФЗ «О персональных данных», к персональным данным относят любую информацию, относящуюся к определенному физическому лицу (субъекту персональных данных).

Персональные данные представляют собой информацию, которая позволяет однозначно определить, о каком лице идет речь. Закон подразделяет персональные данные на три вида:

- общие;

- специальные;

- биометрические.

Общими персональными данными являются фамилия, имя, отчество, место жительства, паспортные данные, сведения об образовании и квалификации, величина заработной платы, трудовая деятельность и т. д. Данные сведения всегда имеются на предприятии.

Специальными данными являются сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья и другие. Эти данные могут содержаться в анкетах, заполняемых сотрудниками при приеме на работу, медицинских справках и т. д.

К биометрическим данным относят сведения, отражающие физиологические и поведенческие характеристики, позволяющие определить его личность. Например, отпечатки пальцев, рисунок радужной оболочки глаза, данные измерений параметров лица, формы руки, рисунка сетчатки глаза, почерка, голоса и другие. Кроме того, к биометрическим данным относятся фотографии человека, за исключением фотографий и видеозаписи, сделанных во время массовых и публичных мероприятий.

Предприятие несет ответственность перед работниками за нарушение режима защиты, обработки и порядка использования этой информации. Для защиты персональных данных используются все методы и средства, перечисленные при описании защиты информации для служебного пользования. При обнаружении незаконности сбора или распространения информации и при отсутствии согласия ее носителя на сбор или разглашение информации, возникает уголовная ответственность. Если разглашение конфиденциальных сведений о личности произошло во время выполнения служебных обязанностей, наказание ужесточается. Еще более серьезная ответственность предусмотрена за разглашение данных о несовершеннолетних.

Определившись с особенностями каждого вида информации, сформулируем основные положения, касающиеся ее оптимальной защиты в рамках использования в малом бизнесе с учетом малых финансовых затрат. Это будет возможно при создании системы безопасности, которая выполняет только необходимые обязательные функции.

1. Антивирус и брандмауэр. Крупнейшие системы безопасности предлагают программные приложения, разработанные специально для компаний, относящихся к сегменту малого бизнеса, с числом сотрудников и, соответственно, компьютеров, до 25. Данные предложения обеспечивают комплексную защиту компьютеров, файловых серверов и мобильных устройств от вредоносных программ, интернет-атак и онлайн-мошенничества с учетом всех требований закона.

2. Система аутентификации (идентификации), авторизации и администрирования (ААА). Работа предприятия малого бизнеса невозможна без обеспечения системы, имеющей аббревиатуру AAA или 3A (аутентификация, авторизация, администрирование). В некоторых случаях добавляют четвертую составляющую и четвертую «А» – аудит. Данные системы предназначены для обеспечения защиты от несанкционированного доступа к информационным системам и ресурсам. Конкретный состав и содержание организационных и технических мер по обеспечению информационной безопасности персональных данных указаны в Приказе ФСТЭК № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Системы хранения информации. Для предприятий любой величины проблема хранения, управления и восстановления в случае потери является актуальной. Система резервного копирования и восстановления данных (Backup & Recovery) позволяют с заданным интервалом создавать копии данных с целью их возможного восстановления в будущем. Кроме того, они способствуют обеспечению непрерывной деятельности предприятия или организации в случае повреждения операционной системы путем ее быстрого восстановления без потерь информации. Отметим важную особенность, которую необходимо учитывать при использовании облачных хранилищ информации. В том случае, когда предприятие использует для обработки персональных данных облачные хранилища данных, расположенные не на территории РФ, оно обязано иметь копию базы данных, расположенную в нашей стране, проводить все требуемые изменения и дополнения в этой базе данных, а затем передавать информацию в облачное хранилище. То есть на территории РФ всегда должна находиться актуализированная база данных, содержащая обрабатываемую персональную информацию.

4. Защита от утечек конфиденциальной информации Информационные системы защиты от утечек конфиденциальной информации (Data Loss Prevention, DLP) позволяют проводить отслеживание и блокирование передачи информации за пределы корпоративной сети. Данные системы способны следить за действиями сотрудников организации, записывать и анализировать их сообщения, посылаемые во время работы по электронной почте, социальным сетям, FTP, Skype, ICQ и других приложений, и протоколов, распечатываемых на принтере или сохраняемых на внешние носители информации.

Основной задачей систем DLP является обеспечение выполнения политики конфиденциальности, принятой в конкретной организации. Результатом становится предотвращение несанкционированной передачи конфиденциальной и персональной информации, минимизация рисков репутационного ущерба и повышение дисциплины сотрудников организации. Таким образом, информация является ценнейшим ресурсом бизнеса. Защита данных, содержащих государственную тайну и персональные сведения людей, регламентируется законами РФ и обязательна для исполнения. Алгоритмы защиты коммерческой тайны необходимо задавать самостоятельно, в зависимости от специфики и величины каждого предприятия или организации.

Особенностью малого бизнеса являются ограниченные финансовые возможности, выделяемые на средства и методы защиты информации. Поэтому принимаемые решения должны позволить реализовать оптимальную защиту информационной системы и данных, т. е. обеспечить максимально возможный результат при ограниченных вложениях средств.

## 3.2 Разработка мероприятий по совершенствованию системы информационной безопасности

Значительная часть новых научных разработок создается и внедряется малыми инновационными предприятиями, деятельность нуждается в обеспечении информационной безопасности. Малые предприятия, как правило, не располагают значительными финансовыми ресурсами, однако, поскольку организация защиты информации на малые предприятия строго не

регламентируется, возникает возможность ставить задачу синтеза (выбора) минимальной по стоимости СИБ, обеспечивающей достаточный уровень безопасности.

Общая постановка задачи выбора варианта СИБ имеет вид:

f(Var) - min, Var ϵ Variants\*, Variants\* ϵ Variants,

где f(Var) – стоимость реализации варианта Var, входящего в подмножество Variants\* общего множества всех возможных вариантов системы информационной безопасности Variants. Область выбора Variants\* определяется, исходя из ограничений, связанных с необходимостью противодействия конечному множеству угроз Threats={Threat1, Threat2,…,

ThreatI}. Сочетания угроз информационной безопасности образуют ситуации Situations={Situation| Situation ϵ Threats}, сочетание которых в свою очередь составляет окружающую обстановку Environment, в которой реализуется деятельность малого предприятия.

Будем полагать, что на всех уровнях построенной иерархии (на множествах Threats, Situations, Environments) существуют задаваемые экспертами отношения частичного порядка: RT ϵ (Threats)2 , RS ϵ (Situations)2 , RE ϵ (Environments)2 , для которых выполняются свойства рефлексивности, симметричности и транзитивности. Это позволяет выделить

недоминируемые угрозы (ситуации, обстановки), которым соответствуют считающиеся известными (входящие в множество Variants) варианты СИБ, и, тем самым, сократить начальная область выбора Variants до множества Variants\*.

**Анализ иерархии угроз информационной безопасности:**

- составление перечня угроз;

- составление перечня ситуаций;

- составление перечня окружающих обстановок.

**Экономическое оценивание угроз информационной безопасности предприятия:**

- оценивание уровней угроз;

- построение частичного порядка на множество угроз, ситуаций, обстановок;

- построение множеств недоминируемых угроз, ситуаций, обстановок.

**Построение области выбора СИБ:**

- составление перечня вариантов СИБ;

- определение учитываемого уровня иерархии угроз;

- построение множества вариантов СИБ, соответствующих недоминируемым угрозам (ситуациям, обстановкам).

**Нахождение рационального решения:**

- вычисление стоимости вариантов СИБ;

- нахождение нескольких вариантов с минимальной (близкой к минимальной) стоимостью;

- выбор рационального варианта.

Рисунок 3.1 – Схема процедуры выбора варианта СИБ для малого предприятия

Общая схема решения сформулированной задачи приведена на рисунке 3.1. На первом этапе процедуры проводится анализ внешней среды СИБ. На втором (наиболее трудоемком) этапе осуществляется экспертное оценивание угроз (ситуаций, обстановок), требующее применения специализированных технологий обработки данных. Третий этап состоит в построении области выбора вариантов СИБ, из которой затем (на четвертом этапе) выбирается наилучший вариант. При этом если выбор из небольшого числа вариантов не представляет трудностей, то при большом их количестве для отбора нескольких рациональных вариантов целесообразно (чтобы избежать полного перебора) использовать эвристические эволюционные методы. Необходимо отметить, что окончательный выбор решения из нескольких альтернатив производит ЛПР (лицо, принимающее решения) на основе собственных (часто неформализуемых) предпочтений.

В результате анализа системы информационной безопасности предприятия были выявлены значительные уязвимости системы. Одним из способов защиты информации является создание паролей. Пароли должны удовлетворять следующим правилам:

• пароль должен быть длинным (8-12-15 символов),

• содержать как ЗАГЛАВНЫЕ, так и прописные латинские буквы, числа;

• не должен быть словом из словаря;

• пароль не может быть связан с владельцем;

• пароль изменяется периодически или по мере необходимости;

• пароль не используется в этом качестве на разных ресурсах;

• нельзя хранить пароли в незашифрованном виде;

• необходимо изменять пароль в случае его раскрытия или подозрения о раскрытии;

• среди символов пароля должны быть буквы в верхнем и нижнем регистрах, цифры и специальные символы, пароль не должен включать легко вычисляемые последовательности символов (имена, клички животных, даты);

• изменять пароль раз в 6 месяцев;

• при изменении пароля нельзя выбирать использованные ранее пароли.

Другим методом защиты информации является разработка политики по обнаружению вирусов. В этом случае актуальны следующие правила:

• лицензионное антивирусное программное обеспечение должно быть установлено на каждой рабочей станции;

• обновление антивирусных баз на рабочих станциях с подключением к Интернету - один раз в день, без доступа в Интернет - не реже одного раза в неделю;

• установить автоматическое сканирование рабочей станции для обнаружения вирусов (частота проверок - один раз в неделю: пятница, 12:00);

• администратор может прервать обновление антивирусных баз или выполнить проверку на вирусы (защита паролем должна быть настроена на указанное действие пользователя).

Чтобы оптимизировать программное обеспечение, на предприятии был составлен список программ, которые по своей функциональности наиболее подходят для лучшей защиты корпоративной информации.

Этот список включает такие программы, как: Pandora Recovery, VirusTotal, Dr.Web. Web, Comodo и ShaMAN.

1) Pandora Recovery - предоставляет высоконадежный инструмент, который позволяет пользователю выполнять поиск с последующим восстановлением удаленных файлов либо в отформатированных дисках (локальной, сетевой или переносной) файловой системы NTFS (и других) или поврежденных носителях, либо после удаления файлов из Корзина.

После сканирования целевой системы утилита собирает информацию обо всех удаленных файлах, папках на локальном, сетевом диске или портативном носителе и отображает их список в окне проводника. Этот список дает пользователю полный контроль над файлами, в частности, можно выбрать файлы для восстановления и в какой каталог они будут восстановлены.

2) VirusTotal - результаты проверки файлов службой не зависят от одного производителя антивируса. VirusTotal использует несколько десятков антивирусных систем, которые могут позволить вам сделать более достоверные выводы об опасности файла, по сравнению с каким-либо одним продуктом. Все антивирусные базы, используемые службой, постоянно обновляются. Результаты сканирования указывают даты последних обновлений всех баз данных. После загрузки файла система вычисляет свой хэш и, если есть результаты проверки файла с тем же самым хэшем, предлагает либо просмотреть последний анализ (указав дату первой и последней проверки), либо повторить анализ. Сервис постоянно развивается, постоянно подключаются новые сканеры (антивирусы и антитрещины). VirusTotal отправляет подозрительные файлы производителям антивирусов для анализа.

3) Web - это общее название семейства программных антивирусных программ для различных платформ (Windows, OS X, Linux, мобильных платформ) и линейки аппаратных и программных решений (Dr.Web Office Shield), а также решений безопасности для все узлы корпоративной сети (Dr.Web Enterprise Suite). Он разработан компанией «Доктор Веб».

Продукты обеспечивают защиту от вирусов, троянов, шпионских программ, рекламного ПО, червей, руткитов, хакерских инструментов, шутковых программ и неизвестных угроз с помощью различных технологий проактивной защиты в режиме реального времени и проактивной защиты.

4) Comodo - это программный пакет, состоящий из антивируса и персонального межсетевого экрана, а также песочницы, системы предотвращения вторжений HIPS и виртуальная виртуальная среда Virtual Kiosk (новый компонент пакета, начиная с версии 6) для Microsoft Windows XP, Vista, Windows 7 и Windows 8. Компоненты инсталляционного пакета Comodo AntiVirus и Comodo Firewall могут устанавливаться отдельно и использоваться как отдельные продукты. Comodo Internet Security (CIS) может использоваться бесплатно как для коммерческого, так и для личного использования[[14]](#footnote-14).

Разработка направленного программного обеспечения для предприятия. В данном пункте мы рассмотрим программу под названием «ShaMAN.» Данная программа была разработана нами для предприятия в целях обеспечить лучшую защиту информации, в совокупности с остальными программами, предоставленными выше. Эта программа изначально была создана как портативный антивирус с возможностью сканировать файлы с помощью обширной базы данных, которая состоит из нескольких десятков антивирусных систем. Создано данное приложение на языке программирования PHP, и отличается универсальностью, общедоступностью и лёгким редактированием программного кода.

Установка данной программы не требует особых привилегий и мало чем отличается от установки какой-либо другой программы. После установки и запуска приложения появится следующие окно (см. рисунок 3.2.):

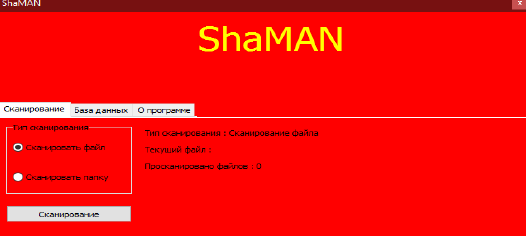


Рисунок 3.2 – Главная панель программы ShaMAN

Интерфейс был разработан с целью облегчения работы пользователя с программой. При интуитивно понятном интерфейсе функционал программы не снижается. На основной панели ПО можно увидеть основные разделы, такие как: «Сканирование», «База данных» и «О программе».

«Сканирование» дает возможность просканировать как целую папку, так и отдельный файл. После выбора метода сканирования, требуется нажать кнопку «Сканировать» для выбора определённой папки (файла) после чего сканирование запуститься автоматически. С правой стороны от выбора метода сканирования будет отображаться статус-бар, в котором отображается информация о методе сканирования, ходе сканирования и количестве вредоносных файлов.

На вкладке «База данных» (см. рисунок 3.3.) расположены кнопка «Обновить», которую следует нажать для обновления антивирусной базы, статус-бар, который предоставляет информацию о ходе обновления базы и информационная строка, на которой можно увидеть, когда в последний раз была обновлена база.

На третей вкладке «О программе» можно увидеть информацию о разработчике программы, контактные данные и среду программирования, в которой была создана данная программа. Так же в дальнейшем будет отображаться информация о версии ПО и дата выхода следующего обновления.



Рисунок 3.3 - Вкладка «База данных»

В ходе улучшения и обновления программы будут добавлены такие функции как сканирование беспроводной сети на наличие неизвестных подключённых устройств, которые могут нанести вред информации, и блокировка портативного компьютера электронным ключом, что в свою очередь сделает невозможным проникновение злоумышленника напрямую к информации.

# Заключение

Развитие информационных систем, привело в настоящее время к появлению и последующему развитию концепции открытых систем. Но, при этом стало возникать довольно большое количество проблем несанкционированного получения доступа к информации.

Защита информации, особенно информации конфиденциальной, является самой актуальной задачей, и, учитывая, что более 90% информации ныне находится в электронном виде, физические средства и методы защиты информации утратили свою былую эффективность.

Основной документ Российской Федерации, который нормирует меры и действия, обязательные для проблем разрешения информационной безопасности всех вновь создаваемых либо привлекаемых извне, а также обслуживаемых информационных разработок – это Доктрина информационной безопасности РФ, которая была еще подписана в 2000 году Президентом России В.В. Путиным.

Система защиты информации – это совокупность специальных правовых и административных мер, мероприятий, организационного характера, различных средств защиты (физических и технических), а также персонала, который предназначен для обеспечения информационной безопасности. Основной идеей защиты информации как общественного явления является установление и реализация организационных, морально-этических и нормативно правовых взаимоотношений между людьми, которые обеспечивают сбалансирование интересов человека, государства и общественности в сфере информации.

Объектом исследования в работе выступает ООО «Лазурит», а именно салон «Леонардо».

В ходе этого исследования мы сделали определенные выводы и смогли оптимизировать и обеспечить высокий уровень информационной безопасности на предприятии. Выяснилось, что основной причиной проблем компании в области информационной безопасности является отсутствие политики информационной безопасности.

Анализ системы информационной безопасности выявил существенные недостатки, в том числе:

- хранение резервных копий на сервере, резервный сервер находится в одной комнате с главными серверами;

- отсутствие надлежащих правил защиты паролем (длина пароля, правила его выбора и хранения);

- обобщение международной и российской практики в области управления информационной безопасностью предприятий позволило сделать вывод о том, что для обеспечения ее безопасности нам необходимы:

- классификация информации (для служебной или коммерческой тайны);

- прогнозирование и своевременное обнаружение угроз безопасности, причин и условий, способствующих финансовому, материальному и моральному ущербу;

- создание условий для деятельности с наименьшим риском реализации угроз безопасности для информационных ресурсов и применения различных видов ущерба;

- создание механизма и условий для эффективного реагирования на угрозы информационной безопасности на основе правовых, организационных и технических средств.

# Список использованных источников

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27 июля 2006 года.– URL:https://rg.ru/2006/07/29/informacia-dok.html
2. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г.№683. –URL:https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html
3. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646.–URL:https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html
4. Баранов, А.П. Современное состояние философии управления информационной безопасностью / А. П. Баранов// Бизнес-информатика. – 2014. – №2(28). – С. 112.
5. Ворона, В.А. Теоретические основы обеспечения безопасности объектов информатизации: Учебное пособие для вузов / В.А. Ворона, В.А Тихонов, Л.В. Митрякова. - М.: РиС, 2016. – 304 c.
6. Гафнер В.В. Информационная безопасность. – Ростов на Дону: Феникс, 2014. – 324 с.
7. Гончаров, О.И. Теория автоматического управления: курс лекций / О. И. Гончаров. – МГУ имени Ломоносова, 2014. – 209 с.
8. Донская, Е. Н. Отдельные аспекты обеспечения информационной безопасности деятельности органов местного самоуправления / Е.Н. Донская, Ю.В. Панько // Молодой ученый. — 2014. — №8. — С. 453.
9. Есаулов В.Т. Противодействие информационным угрозам как важное направление политики национальной безопасности Российской Федерации / В.Т. Есаулов // Власть. – 2012. – № 12. – С. 68–71.
10. Киселёв А.К. Актуальные проблемы обеспечения защиты информации правовыми средствами / А.К. Киселев // Юридическая наука. – 2014. – № 3. – С. 63–66.
11. Козунова, С.С. Система принятия решений инвестирования информационной безопасности предприятий в условиях полной неопределённости / С. С. Козунова, А. А. Бабенко // Информационные системы и технологии. – 2015. – №6(92). – С. 98.
12. Конотопов, М.В. Информационная безопасность. Лабораторный

практикум / М.В. Конотопов. - М.: КноРус, 2013. – 136 c.

1. Ляпина И.Р. Информационная безопасность малых инновационных предприятий/ И.Р. Ляпина, Е.В. Сибирская, Е.В. Петрухина, О.А. Строева // Теоретические и прикладные вопросы экономики и сферы услуг. – 2013. – № 9. – С. 84-89.
2. Ломазов А.В. Формирование иерархии оценочных показателей сложных динамических систем на основе экспертных технологий/ А.В. Ломазов, В.А. Ломазов, Д.А. Петросов // Фундаментальные исследования. – 2015. – № 7-4. – С. 760-764.
3. Мельников, Д.А. Информационная безопасность открытых систем учебник / Д.А. Мельников. - М.: Флинта, 2013. – 448 c.
4. Мухин И.Н. Анализ рисков управления информационной безопасностью предприятия как этап комплексной защиты объектов информатизации // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2012. – № 4-5. – С. 33-37.
5. Петров, С.В. Информационная безопасность: Учебное пособие / С.В.Петров,И.П. Слинькова, В.В. Гафнер.- М.: АРТА, 2012. – 296 c.
6. Полунин А. Информационная и сетевая защита SMB компаний / А. Полунин – Инженерный вестник, 2016. – 398 с.
7. Полякова, Т.А. Организационное и правовое обеспечение ин формационной безопасности: Учебник и практикум для бакалавриата и магистратуры. / Под ред. Т. А. Поляковой, А. А. Стрельцова. – М.: Издательство Юрайт, 2016. – 325 с.
8. Родина Ю.В. Информационная безопасность и риски информационной безопасности. интерпретация понятий // В сборнике: Экономика и менеджмент: от теории к практике, сборник научных трудов по итогам международной научно-практической конференции. Инновационный центр развития образования и науки. г. Ростов-на-Дону. – 2014. – С. 122-124.
9. Росенко А.П. Методологические основы проблемы безопасности конфиденциальной информации // Известия ТРТУ. – 2016. – № 7 (62). – С. 27-33.
10. Росенко А.П. Об одном подходе к определению вероятностей последствий от воздействия на АИС угроз безопасности конфиденциальной информации // Известия ЮФУ. Технические науки. – 2014. – № 11 (100). – С. 164-168.
11. Росенко А.П. О критерии нормирования уровня безопасности конфиденциальной информации // Обозрение прикладной и промышленной математики. – М.: Изд-во «ОП и ПМ». – 2010. – Т. 17 (2).– С. 297-298.
12. Росенко А.П. Методы определения вероятности несанкционированного доступа к конфиденциальной информации // Доклады Томского гос. ун-та систем управления и радиоэлектроники. – 2012. – № 1–2. – С. 25-28.
13. Росенко А. П., Окулов Н.С. Программа расчета количественной оценки безопасности информации ограниченного распространения // Свидетельство о государственной регистрации программ для ЭВМ № 2015619521, зарегистрированное в Реестре программ для ЭВМ от 04 сентября 2015 г. – 2015. – 387 с.
14. Савченко И.А.,Прокофьев Д.Н. Защита информации в организации // Теория и практика современной науки. – 2016. – №5 (11). – С. 812-814.
15. Сердюк, Н. Н. Архитектура информационно-аналитической системы управления безопасностью производства / Н. Н. Сердюк// Автоматизированные системы управления и приборы. – 2014. – №167. – С. 87.
16. Суглобов, А.Е. Экономическая безопасность предприятия: Учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А.Е. Суглобов, С.А. Хмелев, Е.А. Орлова. – М.: ЮНИТИ – ДАНА, 2015. – 298 с.
17. Тимофеев, А.М. Основные проблемы управления информационной безопасностью в организации / А. М. Тимофеев // Вестник Омского университета. Серия «Экономика». – 2013. – №1. – С. 34.
18. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. – 702 c.
19. Шамсуев М.Х. Теоретические аспекты изучения информационной безопасности / М.Х. Шамсуев // Теория и практика общественного развития. – 2013. – № 2. – С. 319–325.

1. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г.№683. –URL:https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html [↑](#footnote-ref-1)
2. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646.–URL:https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html [↑](#footnote-ref-2)
3. Шамсуев М.Х. Теоретические аспекты изучения информационной безопасности / М.Х. Шамсуев // Теория и практика общественного развития. – 2013. – № 2. – С. 319–325. [↑](#footnote-ref-3)
4. Ворона, В.А. Теоретические основы обеспечения безопасности объектов информатизации: Учебное пособие для вузов / В.А. Ворона, В.А Тихонов, Л.В. Митрякова. - М.: РиС, 2016. – 304 c. [↑](#footnote-ref-4)
5. Есаулов В.Т. Противодействие информационным угрозам как важное направление политики национальной безопасности Российской Федерации / В.Т. Есаулов // Власть. – 2012. – № 12. – С. 68–71. [↑](#footnote-ref-5)
6. Ляпина И.Р. Информационная безопасность малых инновационных предприятий/ И.Р. Ляпина, Е.В. Сибирская, Е.В. Петрухина, О.А. Строева // Теоретические и прикладные вопросы экономики и сферы услуг. – 2013. – № 9. – С. 84-89. [↑](#footnote-ref-6)
7. Мухин И.Н. Анализ рисков управления информационной безопасностью предприятия как этап комплексной защиты объектов информатизации // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2012. – № 4-5. – С. 33-37. [↑](#footnote-ref-7)
8. Росенко А.П. Об одном подходе к определению вероятностей последствий от воздействия на АИС угроз безопасности конфиденциальной информации // Известия ЮФУ. Технические науки. – 2014. – № 11 (100). – С. 164-168. [↑](#footnote-ref-8)
9. 2Росенко А.П. Методы определения вероятности несанкционированного доступа к конфиденциальной информации // Доклады Томского гос. ун-та систем управления и радиоэлектроники. – 2012. – № 1–2. – С. 25-28. [↑](#footnote-ref-9)
10. Росенко А. П., Окулов Н.С. Программа расчета количественной оценки безопасности информации ограниченного распространения // Свидетельство о государственной регистрации программ для ЭВМ № 2015619521, зарегистрированное в Реестре программ для ЭВМ от 04 сентября 2015 г. – 2015. – 387 с. [↑](#footnote-ref-10)
11. Савченко И.А.,Прокофьев Д.Н. Защита информации в организации // Теория и практика современной науки. – 2016. – №5 (11). – С. 812-814. [↑](#footnote-ref-11)
12. Суглобов, А.Е. Экономическая безопасность предприятия: Учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А.Е. Суглобов, С.А. Хмелев, Е.А. Орлова. – М.: ЮНИТИ – ДАНА, 2015. – 298 с. [↑](#footnote-ref-12)
13. Шамсуев М.Х. Теоретические аспекты изучения информационной безопасности / М.Х. Шамсуев // Теория и практика общественного развития. – 2013. – № 2. – С. 319–325. [↑](#footnote-ref-13)
14. Тимофеев, А.М. Основные проблемы управления информационной безопасностью в организации / А. М. Тимофеев // Вестник Омского университета. Серия «Экономика». – 2013. – №1. – С. 34. [↑](#footnote-ref-14)