МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

филиал в г.Туапсе

Кафедра «Экономики и управления на предприятии природопользования»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(бакалаврская работа)
по направлению подготовки 38.03.01 Экономика
(квалификация – бакалавр)

На тему «Анализ и оценка состояния информационной безопасности как элемента экономической безопасности предприятия»

Исполнитель Джаловян Олег Сергеевич

Руководитель к.э.н., Майборода Евгений Викторович

«К защите допускаю»

Руководитель кафедры _____

кандидат экономических наук

Майборода Евгений Викторович

«21» 01 2025 г.

Филиал Российского государственного гидрометеорологического университета в г. Туапсе
НОРМОКОНТРОЛЬ ПРОЙДЕН
«18» 01 2025 г.
Мартынова Т.В.
ПОДПИСЬ РАСШИФРОВКА ПОДПИСИ

Туапсе
2025

ОГЛАВЛЕНИЕ

Введение

Современные предприятия – это большое количество ценных и конфиденциальных данных, включая данные о клиентах, финансовые данные, интеллектуальную собственность, а также другую важную информацию. Ввиду этого, наличие эффективной стратегии по обеспечению информационной безопасности является важным фактором для эффективной и бесперебойной работы предприятий.

С развитием технологий и расширением использования цифровых технологий, количество и сложность угроз информационной безопасности предприятий постоянно увеличивается. Такие угрозы могут привести к утечкам данных, шантажу, потере конфиденциальности информации, причине нанесения ущерба репутации и финансовому обману. Кроме того, существует риск нарушения работы IT-систем и сбоях в работе предприятия.

В настоящее время большинство предприятий прилагают усилия для защиты своих информационных ресурсов. Однако постоянное совершенствование технологий требует и постоянно поиска и внедрения оптимальных методов и средств защиты для уменьшения вероятности возникновения угроз и минимизации повреждений от возможных атак.

Актуальностьвыпускной квалификационной работы обусловлена реальной потребностью предприятий в защите своей информационной сферы от возможных угроз и атак со стороны злоумышленников и конкурентов.

Объектом в данной работы выбрано общество ПАО «Звезда»

Предметом выпускной квалификационной работы являются система информационной безопасности икомплекс мер понейтрализации угроз и обеспечению информационной безопасности предприятия.

Цель выпускной квалификационной работы заключается в оценке системы информационной безопасности предприятия и разработке рекомендаций для нейтрализации угроз и уязвимостей, представляющих собой наибольшую опасность для экономической безопасности ПАО «Звезда».

Согласно определенной выше цели, были выделены следующие задачи:

1. Рассмотреть теоретические основы исследования информационной безопасности в системе экономической безопасности предприятия;

2. Осуществить анализ состояния информационной безопасности как элемента экономической безопасности предприятия ПАО «Звезда;

3. Разработать предложения по нейтрализации угроз экономической безопасности ПАО «Звезда» в части обеспечения информационной безопасности

Практическая значимость исследования заключается в предоставлении комплексного подхода к нейтрализации угроз информационной безопасности, который может быть применен на практике предприятием ПАО «Звезда».Разработка системы нейтрализации угроз информационной безопасности может помочь предприятию экономить ресурсы, снижать риски, уменьшать потери и обеспечивать безопасность информации.

Теоретическая значимость исследования заключается в расширении теоретических знаний об информационной безопасности предприятий.

Структура выпускной квалификационная работа состоит из введения, трех глав, заключения, списка использованной литературы и приложений.

1 Теоретические основы исследования информационной безопасности в системе экономической безопасности предприятия

1.1 Информационная безопасность в системе экономической безопасности предприятия

На настоящем современном этапе развития современной экономической системы всю большую актуальность приобретает вопрос экономической безопасности, как в целом для государства, так и предприятий в частности. Поскольку именно в данный момент предприятия максимально уязвимы от кризисных ситуаций, от политической нестабильности, криминализации бизнеса и от рисков, связанных с несовершенством имеющей нормативной базы, то на первом плане у каждого хозяйствующего субъекта должна стоять задача по обеспечению условий, гарантирующих стабильную деятельность и экономическую безопасность.

В классическом понимании под безопасностью было принято считать состояние защищенности от опасностей внутреннего и внешнего характера.

По мнению В. Л.Тамбовцева, «...под экономической безопасностью той или иной системы нужно понимать совокупность свойств состояния ее производственной подсистемы, обеспечивающую возможность достижения целей всей системы» [34, с. 37-42].

В. А. Савин считает, что «экономическая безопасность представляет систему защиты жизненных интересов России. В качестве объектов защиты могут выступать: народное хозяйство страны в целом, отдельные регионы страны, отдельные сферы и отрасли хозяйства, юридические и физические лица как субъекты хозяйственной деятельности» [28, с.14].

Сегодня существует два основных подхода авторов к определению безопасности. Первый подход основывается на использовании понятия угрозы. Второй – уклоняется от употребления понятия «угрозы» в определении безопасности, и базируется на экономических понятиях, связанных с достижением цели, функционирования предприятия [3].

В Стратегии национальной безопасности РФ защищенность рассмотрена в динамике позитивных изменений, при которых обеспечивается устойчивое позитивное развитие общества и государства: «обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны»[2].

Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией РФ и законодательством РФ, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.[2]. При рассмотрении взаимосвязи разных видов безопасности необходимо понимание того, что в основе каждого из них лежит безопасность конкретного человека. При этом состояние безопасности обеспечивается не только защитой от угроз, но и их нейтрализацией за счет механизмов мирного сотрудничества и взаимодействия в самых разных сферах государственной деятельности, жизни гражданского общества. В Приложении 1 представлены вызовы и угрозы экономической безопасности.

Таким образом, говоря о безопасности в целом и об экономической безопасности в частности, необходимо понимать, что она охватывает все уровни от личности до государства. То есть в рамках вопроса экономической безопасности какой-либо сферы необходимо учитывать взаимосвязь всех её уровней:

1. Международная безопасность;
2. Национальная безопасность;
3. безопасность сферы;
4. безопасность отдельных элементов в рамках сферы.
5. безопасность личности.

Аналогичное мнение о многоуровневой структуре экономической безопасности мы видим и у А.Н. Малолетко, который говорит о том, что

национальные экономические интересы Российской Федерации заключаются в достижении ряда целей:

а) на уровне экономики страны в целом;

б) на уровне отдельных видов экономической деятельности и институциональных;

в) на внутрисистемном уровне[21, с. 135].

На практике экономическая безопасность страны означает ритмичное функционирование всех сфер общественной жизни и национального хозяйства (промышленность, энергетика, финансы, образование, здравоохранение и пр.). То есть в вопросах экономической безопасности интерес вызывает не только вертикальная взаимосвязь элементов (по уровням), но и горизонтальная взаимосвязь различных сфер, образующих экономику страны.

Основой данной взаимосвязи являются информационные потоки. Обмен информацией является двигателем в рамках любого производства и деятельности. Таким образом, можно сделать вывод, что в функционировании указанных систем и сфер важное место занимает информация, и в частности её безопасность.

1. Под информационной безопасностью понимают состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений [2, с. 4].

Обобщая вышесказанное, можно сделать вывод, что функциональными подсистемами системы общей экономической безопасности страны являются интересы личности, общества, государства. На уровне отдельных сфер (в частностиинформационной безопасности и цифровизации) должны быть реализованы такие же подсистемы. При этом взаимосвязь должна иметь не только вертикальную взаимосвязь по уровням, но и горизонтальную связь с другими сферами.

Исходя из общего понимания безопасности (на любом уровне) как

защищенность от внешних и внутренних угроз и опираясь на исследования учёных, можно привести понятия безопасности, охватывающей все уровни системы обеспечения информационной безопасности (таблица 1.1).

Таблица 1.1– Понятия информационной безопасности по уровням объектов [Составлено автором на основании проведенного анализа]

Уровень	Понятие
Национальная безопасность государства (обеспечивается на международном уровне)	Защищенность государства от внешних и внутренних угроз, устойчивость к неблагоприятным воздействиям извне, обеспечение таких внутренних и внешних условий существования страны, которые гарантируют возможность стабильного прогресса общества и его граждан в сфере информационного обеспечения
Информационная безопасность (цифровая безопасность) как самостоятельная сфера (обеспечивается на государственном уровне)	Состояние кадрового, финансового, научно-исследовательского и материального потенциала, институциональных и организационно-экономических условий, обеспечивающих возможность безопасно использовать информацию и противостоять внутренним и внешним угрозам с целью обеспечения высокого уровня информационного развития общества
Информационная безопасность предприятия (обеспечивается на отраслевом уровне)	Защищенность деятельности организации от негативного влияния внешних и внутренних угроз в сфере информационного обеспечения, позволяющая сохранить и эффективно использовать свой экономический потенциал, т.е. осуществлять деятельность
Личность, участвующая в процессе обмена информации (обеспечивается на потребительском уровне)	Состояние полного физического, духовного и социального благополучия человека при использовании информации

Информационная безопасность является функциональной подсистемой системы экономической безопасности страны, а система обеспечения экономической безопасности – организационной подсистемой системы обеспечения национальной безопасности страны. То есть данные системы полностью взаимны и являются подсистемами друг друга

Таким образом можно сделать вывод, что обеспечение информационной безопасности должно реализовываться на каждом уровне, что в свою очередь в совокупности позволит обеспечить информационную безопасность страны.

При этом, являясь элементом экономической безопасности информационная безопасность на каждом уровне будет обеспечивать и экономическую безопасность каждого уровня.

Стоит отметить, что основным звеном, формирующим экономику страны, а значит, и ее экономическую безопасность, является предприятие. Именно здесь создается экономическая база развития всех отраслей промышленности и всей экономики страны. Соответственно в первую очередь необходимо обеспечивать экономическую безопасность функционирования предприятия, элементом которой также будет являться и его информационная безопасность.

Информационная безопасность предприятия, несмотря на то, чтовсё чаще рассматривается как условие и предпосылка для качественного развития экономики, рассматривается сегодня в основном в техническом аспекте. Её взаимосвязи с экономической безопасностью на уровне предприятия уделено не такое уж и большое значение.

В связи с этим самая распространенная модель информационной безопасности, базируется на обеспечении трех свойств информации – конфиденциальности, целостности и доступности:

– конфиденциальность информации подразумевает то, что с ней может ознакомиться только строго ограниченный круг лиц, установленный владельцем информации. В противном случае говорят об утрате конфиденциальности;

– целостность информации определяется ее способностью сохраняться в неискаженном виде;

– доступность информации определяется способностью системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Доступность является важным критерием для функционирования информационных систем, ориентированных на обслуживание клиентов.

Дополнительными свойствами являются аутентичность (возможность достоверно установить автора сообщения) и апеллируемостъ (возможность

доказать, что автором является именно данный субъект)[22, с. 5].

Угрозы информационной безопасности - это потенциально возможные действия, явленияили процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию. Такие угрозы, воздействуя на ресурсы, могут привести к искажению данных, копированию, несанкционированному распространения, ограничению или блокированию к ним доступа. Угрозы бывают умышленные и случайные.

В связи с этим в качестве возможных угроз информационной безопасности по аспекту информации выделяют следующие угрозы:

- угрозы конфиденциальности;
- угрозы целостности;
- угрозы доступности;
- угрозы аутентичности;
- угрозы аппелируемости.

При анализе гипотетической или практической модели угроз, которые релевантны информационной системе конкретного предприятия, в качестве отдельных единиц защиты и оптимизации рассматриваются компоненты информационной системы, на которые нацелена угроза:

- данные;
- программное обеспечение;
- аппаратное обеспечение;
- поддерживающая инфраструктура.

По природе возникновения угрозы могут быть:

- естественные угрозы;
- искусственные угрозы:
  1) преднамеренные;
  2) непреднамеренные.

Традиционно угрозы делятся на внутренние и внешние. Исходя из этого, угрозы информационной безопасности могут быть классифицированы по расположению источника угроз:

– внутри защищаемой системы (внутренние угрозы);

– вне защищаемой системы (внешние угрозы).

Подобный технический подход позволяет определить типы информационных угроз на каждом из уровней национальной системы безопасности (рисунок 1.1), но подобная классификация не учитывает тот факт, что информационная безопасность является элементом экономической..

Рисунок 1.1 – Типы информационных угроз[15]

На основании изученных подходов представим классификацию информационных угроз в таблице 2.

Результатом такого подхода является лишь технологическое развитие систем безопасности без учета развития экономической безопасности

Таблица–1.2 Классификация информационных угроз [15]

Виды угроз	Разновидности	Пояснения
1. Случайные (непреднамеренные)-действия без злого умысла	Ошибки оператора, неосознанные или не корректные действия технического персонала,	Механизм их реализации изучен достаточно хорошо, поэтому существуют разработанные методы противодействия.
	аварии, аппаратные и программные неисправности технических средств,	
	случайные непреодолимые силы, пожары, наводнения и другие стихийные бедствия.	
2.Умышленные (преднамеренные)-целенаправленные действия злоумышленника, такие как: хищение, модификация, уничтожение данных и т.д.	Оптические	Информационным носителем в оптическом канале будет считаться электромагнитное поле (элементарными частицами являются фотоны) в диапазоне видимого света 0,45-0,75 мкм и диапазоне инфракрасного излучения 0,75-14 мкм.
	Радиоэлектронные;	В радиоэлектронном канале утечка данных происходит через электрические, магнитные и электромагнитные сигналы в радиодиапазоне, а так же электрический ток.
	Акустические;	Акустический канал утеки информации характеризуется неконтролируемым распространением акустических сигналов в инфразвуковом диапазоне (до 16Гц), звуковом (16-20Гц) и ультразвуковом диапазоне (более 20кГц)[11].
	Электромагнитные	Побочные электромагнитные излучения и наводки могут стать причиной для создания случайного канала утечки информации и в случае правильного анализа частоты побочного излучения, злоумышленник в нем может выделить информативную составляющую, что и будет случайным каналом утечки информации.
	Материально-вещественные.	Источники-субъекты(люди) и материальные объекты такие как: документы, черновики, компакт-диски и другие устройства хранения.

Приведенные действия и возможные каналы утечки необходимо учитывать при обеспечении информационной безопасности и планировании политики информационной безопасности на предприятии.

1.2 Формирование системы информационной безопасности на предприятии как элемента экономической безопасности предприятия

Всё большее количество предприятий подвергается различного рода информационным угрозам и атакам. По данным подведомственному Роскомнадзору Центру мониторинга и управления сетью связи общего пользования (ЦМУ ССОП) его специалисты в 2023 году отразили 185 массированных внешних атак злоумышленников в отношении систем защищаемых субъектов [36].

Эксперты информационного агентства «СёрчИнформ» провели своё исследование среди российских промышленных предприятий в связи с информационной безопасностью [37].

По данным этого исследования, 35% промышленных организаций отметили увеличение числа внешних атак, 20% респондентов заметили, что стало больше внутренних инцидентов. По данным исследования, 78% промышленных компаний в 2023 году столкнулись с внутренними инцидентами, из них 60% фиксировали утечки информации. В 2022 году с утечками столкнулась почти половина промышленных организаций – 48%. Кроме того, участники исследования отметили другие виды инцидентов, которые фиксировали в этом году: дискредитация компании (21%), взяточничество (20%), промышленный шпионаж (16%)и внешние атаки через сотрудников (18%).

Чаще всего в 2023 году промышленные организации сталкивались с утечками технических данных и информации о клиентах и сделках. С попытками слива персональных данных столкнулось 22% промышленных организаций [38]. В 68% организаций виновниками утечек становились

линейные сотрудники, линейные руководители (30%). В 19% компаний сталкивались с инсайдерами среди руководителей направлений. Не редко виновниками инцидентов оказывались контрагенты компаний [37].

Предприятиям необходимо защищать информацию и для этого разработать комплекс мер и мероприятий с помощью системного подхода [9].

На любом предприятии разработка системы защиты информации должны соответствовать законодательству на отраслевом и на государственном уровне. В приложении 1 представлены нормативно-правовые акты в области защиты информации. Рассмотрев различные подходы к определениям конфиденциальной информации и опираясь на нормативные акты, на рисунке 1.2 предложена структура основных частей конфиденциальной информации

Рисунок 1.2 – Структура основных частей конфиденциальной информации[18]

Для начала необходимо определить, что является конфиденциальной информацией для данного предприятия, далее коммерческой и профессиональной тайной.

Конфиденциальную информацию обычно классифицируют следующим образом:

1. Персональные данные, подлежащие защите на основании норм федерального законодательства;

2. Программы, содержащие производственную и финансовую информацию, например, 1С: Предприятие;

3. Программные продукты, созданные или доработанные в интересах компании;

4. Базы документооборота;

5. Архивы электронной почты и внутренней переписки;

6. Производственная информация, документы стратегического характера;

7. Научная информация, данные НИОКР;

8. Финансовая информация и аналитика, подготавливаемая по заданию руководства предприятия.

Коммерческая тайна- эторежим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [1].

К профессиональной тайнеотносится конфиденциальная информация, охраняемая законом, полученная специалистом в ходе выполнения своих профессиональных обязанностей.

Эти определения и разграничения должны быть прописаны в Политике информационной безопасности предприятия. Этот документ содержит в себе методические, организационно-административные и технические меры защиты, что послужит основой для разработки внутренних регламентов для функционирования системы защиты информации [15].

Для эффективной и бесперебойной работы предприятия необходимо определить:

1. Основные риски -утечка информации о предприятии, сведений составляющих государственную тайну, остановка основного производства, внедрение вредоносных программ, приводящих к производственному браку;

2. Объекты защиты: конструкторская документация, инженерно-

техническая, новые разработки, информация о поставщиках и покупателях, система защиты предприятия, информационные ресурсы всех видов, система создания, использования и распространения данных, архивы и т.д.;

3. Задачи в области информационной безопасности – защита конечных устройств, чувствительной информации, критических данных и персональных данных, предотвращение утечек, соответствие требованиям регуляторов, выявление внутренних злоупотреблений и др.

4. Какие виды угроз превалируют-внутренние или внешние?

Порядок выполнения работ по созданию системы информационной безопасности (СИБ) определяется руководителем организации совместно с начальниками отделов, которые определяют компетенции и массивы задач в области защиты информации для каждого отдела и сотрудника. Система информационной безопасности является подсистемой в системе менеджмента организации.

Под системой информационной безопасности понимают организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз. Система защиты информации представляет организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз [35, с.13].

Субъектом управления в системе информационной безопасности являются организаторы процесса защиты информации вместе с техникой.

Объект управления в СИБ-это информационные ресурсосодержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных, а также средства вычислительной и организационной техники, сети и системы, управляемые множеством исполнителей.

С позиций системного подхода система информационной безопасности должна обеспечивать защиту информации непрерывно с помощью

обоснованных и рациональных методов, мероприятий, средств, элементов подсистемы, постоянно совершенствующихся процедур и систем защиты, а также в непрерывном контроле и анализе еёсостояния и соответствия новым угрозам, выявлении узких и слабых мест, детальной разработки каждой службой планов защиты.

К основным задачам такой системы относят:

1. Определение информационных массивов, подлежащих защите;
2. Защита информации с помощью неформальных и формальных средств защиты;
3. Безопасность персонала;
4. Ограничение и разграничение доступа работников к конфиденциальной информации, информационным и техническим ресурсам предприятия.

Этапы проектирования, эксплуатации,разработки и аттестации системы защиты информации представлены на рисунке 1.3.

Рисунок 1.3- Основные этапы построения системы защиты информации на предприятии [35]

Опираясь на задачи системы информационной безопасности и объектов защиты необходимо определить средства защиты информации. Они условно делятся на формальные и неформальные и представлены в таблице 1.3

Таблица1.3 - Формальные средства защиты информации[17]

Виды средств защиты	Пояснения
1. Физические	Это механические, электрические, электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним: замки, в том числе электронные, экраны, жалюзи призваны создавать препятствия для контакта дестабилизирующих факторов с системами, видеокамеры, видеорегистраторы, датчики, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения технических средств снятия информации, закладных устройств
2. Аппаратные	Это электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы. Перед внедрением аппаратных средств в информационные системы необходимо удостовериться в совместимости
3. Технические (программные) средства	Это простые и системные, комплексные программы, предназначенные для решения частных и комплексных задач, связанных с обеспечением информационной безопасности:для предотвращения утечки, переформатирования информации и перенаправления информационных потоков, защита от инцидентов в сфере информационной безопасности
4. Специфические	Это различные криптографические алгоритмы, позволяющие шифровать информацию на диске и перенаправляемую по внешним каналам связи. Преобразование информации может происходить при помощи программных и аппаратных методов, работающих в корпоративных информационных системах.

Технические средства защиты делятся на активные и пассивные. К пассивным относят: контроль и ограничение доступа, локализация излучений, экранирование технических средств передачи информации, заземление технических средств передачи информации, акустическая звукоизоляция, подавление побочных электромагнитных излучений и др.

К активным относят: применение акустического вибрационного шума с использованием специальных акустических генераторов, пространственное электромагнитное зашумление, подавление диктофонных устройств, подавление информационного сигнала в линиях электропитания, а также обнаружение и деактивация закладных устройств.

Формальные средства должны использоваться в совокупностипосле анализа и оценки информационных потоков, а также оценки ценности

информации и сравнения ее со стоимостью затрат на обеспечение защиты информации.

Таблица 1.4 - Неформальные средства защиты информации [35]

Виды средств защиты	Пояснения
1. Нормативные	Это законодательные акты РФ и нормативно-распорядительные документы, которые действуют на уровне организации. В мировой практике при разработке нормативных средств ориентируются на стандарты защиты информации– ISO/IEC 27000. На основании этих документов разрабатывается Политика информационной безопасности и Положение об информационной безопасности и другие перечни сведений, составляющих коммерческую тайну.
2. Организационно-административные	Это и архитектурно-планировочные решения, позволяющие защитить переговорные комнаты и кабинеты руководства от прослушивания, и установление различных уровней доступа к информации. Важными организационными мерами станут сертификация деятельности компании по стандартам ISO/IEC 27000, сертификация отдельных аппаратно-программных комплексов, аттестация субъектов и объектов на соответствие необходимым требованиям безопасности, получений лицензий, необходимых для работы с защищенными массивами информации и в соответствии с ПриказомФСТЭК России № 31 от 14.03.2014.
3. Морально-этические	Определяют личное отношение человека к конфиденциальной информации или информации, ограниченной в обороте. Повышение уровня знаний сотрудников касательно влияния угроз на деятельность компании влияет на степень сознательности и ответственности сотрудников.

Система информационной безопасности рассматривается как комплекс правовых, административных, организационных и технических мер, направленных на предотвращение реальных или предполагаемых угроз, а также на устранение последствий инцидентов.

Непрерывность процесса защиты информации должна гарантировать борьбу с угрозами на всех этапах информационного цикла: в процессе сбора, хранения, обработки, использования и передачи информации [17].

2 Анализ состояния информационной безопасности как элемента экономической безопасности предприятия ПАО «Звезда

2.1 Организационно-экономическая характеристика ПАО «Звезда»

В данной работе информация о деятельности предприятия представлена не в полном объёме, так как часть сведений не могут быть раскрыты на основании приказа ПАО «ЗВЕЗДА» № 8-ДСП от 14.05.2021г., изданного в соответствии с пунктом 6 статьи 30.1 Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг», ст. 92.2. Федерального закона от 26.12.1995 № 208-ФЗ «Об акционерных обществах», Постановления Правительства РФ № 400 от 04.04.2021 г. Помимо этого в марте правительство на основании Постановления Правительства РФ от 12.03.2022 N 353 (ред. от 26.12.2022) «Об особенностях разрешительной деятельности в Российской Федерации в 2022 и 2023 годах» разрешило российским эмитентам не раскрывать отчетность частично или в полном объеме, если это чревато для них введением санкций.

Таким образом до официального раскрытия информации на странице в сети Интернет, используемой эмитентом для раскрытия информации http://disclosure.1prime.ru/Portal/Default.aspx?emId=7811038760 более детальные данные компании в ВКР не могут быть раскрыты.

ПАО «ЗВЕЗДА» - крупнейший в России производитель легких компактных высокооборотных дизельных двигателей многоцелевого назначения.[44].

Сокращенное фирменное наименование эмитента: ПАО «ЗВЕЗДА»

Фирменное наименование Общества на английском языке: PUBLIC JOINT STOCK COMPANY «ZVEZDA»

Дата государственной регистрации эмитента: 29.12.1992

Номер свидетельства о государственной регистрации эмитента: 4711

Орган, осуществивший государственную регистрацию: Регистрационная Палата Санкт-Петербурга, решения №: 2259 от 29.12.92, 6820 от 22.03.94

Дата внесения записи в Единый государственный реестр юридических

лиц 20.01.2003 г.

Основной государственный регистрационный номер 1037825005085

Орган, осуществивший государственную регистрацию: Инспекция Министерства Российской Федерации по налогам и сборам по Невскому району Санкт-Петербурга

ПАО «ЗВЕЗДА» (Санкт-Петербург, основано в 1932 году) – ведущий российский разработчик и производитель высокооборотных дизелей мощностью от 500 до 7400 кВт для судостроения, железнодорожного транспорта и малой энергетики, а также тяжелых судовых редукторов мощностью до 20 000 кВт.[44].

Продукция:

– высокооборотные дизельные двигатели и агрегаты размерности ЧН18/20 и ЧН16/17 от 500 до 7400 кВт для судостроения, железнодорожного транспорта, дизель-генераторов и промышленных агрегатов

– судовые редукторные и реверс-редукторные передачи различного назначения передаваемой мощностью до 20 000 кВт

– судовые и промышленные дизель-генераторы, а также аварийно-резервные электростанции на базе дизельных двигателей собственного производства мощностью от 315 до 1000 кВт

– комплектные поставки («под ключ») судового энергетического оборудования для морской техники различного назначения

– Услуги:

– полный цикл разработки и постановки на производство дизелей, агрегатов на их базе и редукторных передач

– шеф-монтаж, пусконаладка, сервисное обслуживание, обеспечение запасными частями, ремонт, обучение, консультации

– алюминиевое литье, механообработка, включая особо точную на станках с ЧПУ, инструментальное производство и др.

Завод «ЗВЕЗДА» – это развитый комплекс машиностроительного производства, включающий собственный инженерный центр; литейное,

кузнечно-прессовое, механообрабатывающее, гальваническое, термическое, сборочно-испытательное и инструментальное производство; службу сервиса и гарантийного обслуживания.

Предприятие основано в 1932 году и с 1945 года специализируется на выпуске высокооборотных дизельных двигателей и агрегатов на их базе. Благодаря своей уникальной конструкции и характеристикам дизель-редукторные агрегаты «ЗВЕЗДЫ» позволили создать скоростной пассажирский флот СССР и Российской Федерации и наладить интенсивные пассажирские перевозки по внутренним водным путям. Одновременно выпускаемые предприятием двигатели и агрегаты обеспечили создание в стране скоростного флота патрульных катеров береговой охраны и военно-морских сил.

Кроме того, легкие двигатели завода «ЗВЕЗДА» широко применялись на дизель-моторвагонном подвижном составе для осуществления пассажирских перевозок по всей территории СССР и в странах Восточной Европы[44].

Высокоэффективные аварийно-резервные дизель-генераторные установки завода «ЗВЕЗДА» уже более 60 лет обеспечивают энергетическую безопасность объектов газотранспортной системы, нефтепроводов, узлов связи и государственных объектов особой значимости.

Начиная с 2002 года «ЗВЕЗДА» стало ведущим российским разработчиком и производителем тяжелых судовых редукторов, входящих в состав дизель-дизельных, дизель-газотурбинных и газотурбинных агрегатов мощностью до 20 000 кВт и более для морской техники различного назначения[44].

В 2011-2015 годах в рамках ФЦП «Национальная технологическая база» предприятие разработало новое семейство высокооборотных дизельных двигателей М150 мощностью от 400 до 1700 кВт. При разработке двигателей использованы самые современные технические решения мирового дизелестроения, обеспечивающие их надежность, экономичность и высокие показатели в области экологии.

Семейство двигателей М150 предназначено для перспективного

использования в транспортном машиностроении, в карьерной технике, на объектах морской техники и в малой энергетике.

Система менеджмента качества ПАО «ЗВЕЗДА» сертифицирована по стандарту ISO-9001:2015 (Bureau Veritas Quality International).

Ряд судовых дизельных двигателей предприятия сертифицирован классификационным обществом «Germanischer Lloyd», Российским Морским регистром судоходства, Российским речным регистром.

С перечнем лицензий и сертификатов можно ознакомиться на официальном сайте общества [44].

ПАО «ЗВЕЗДА» является членом Союза промышленников и предпринимателей Санкт-Петербурга, Санкт-Петербургской Торгово-промышленной палаты, Ассоциации промышленных предприятий Санкт-Петербурга, Союза машиностроителей России.

Уставный капитал Общества составляет 56 202 048 рублей и состоит из 562022480 обыкновенных именных акций номинальной стоимостью 0,10 рубля каждая.

Обыкновенные именные акции общества допущены к торгам Публичного акционерного общества «Московская Биржа ММВБ-РТС» в котировальном списке третьего уровня. Акции эмитента не обращаются за пределами Российской Федерации.

Правовое положение Публичных акционерных обществ раскрывается в ст. 97 ГК РФ [39]. Деятельность Общества строится на нормах ФЗ «Об акционерных обществах» [40], Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг» [41], Устава Общества, Положениях и иных внутренних документах Общества.

Публичное акционерное общество в России (сокр. ПАО) – форма организации акционерного общества, при которой его акционеры пользуются правом отчуждать свои акции без необходимости согласования с другими акционерами.

Особенности ПАО:

– неограниченное число акционеров;

– свободное обращение акций на рынке;

– отсутствие необходимости внесения денежных средств в уставный капитал предприятия до его регистрации и открытия накопительного счёта.

За 2023 года компания получила убыток в размере 1518718 тыс. рублей, что на 211,06% ниже убытка, полученного в 2022 году. Стоит отметить, что последний раз компания получала чистую прибыль в 2018 году. В 2021 году убыток составлял 256307 тыс. рублей, но кризис 2022 года привёл к ещё более отрицательным результатам (рисунок 2.1).

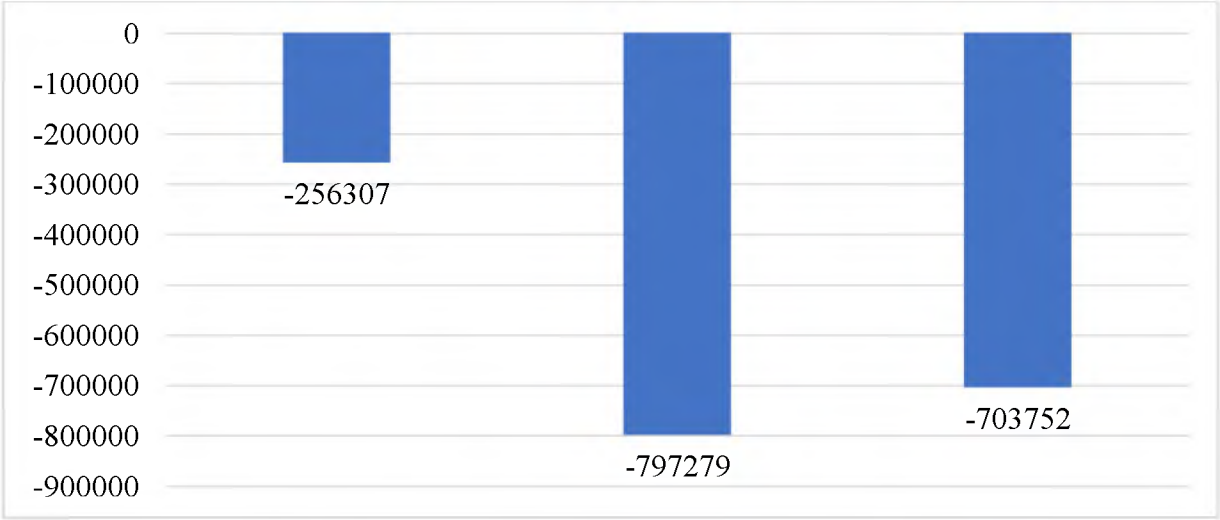

Рисунок 2.1 – Динамика чистого убытка ПАО «Звезда» за 2021-2023 гг., тыс. рублей

Отрицательный результат компании формируется ещё на стадии расходов по себестоимости, которая значительно превышают выручку (рисунок 2.2).

При этом до 2022 года себестоимость росла более быстрыми темпами чем выручка, что увеличивает разницу в их соотношении. В таблице 2.1 и 2.2 представлены показатели изменений по финансовым результатам за анализируемый период.

Темп роста выручки в 2022 году составил 94%, а в 2023 году темп роста снизился и был равен 92 %. Темп роста себестоимости 2022 года составил 114%. В 2023 году темп роста был равен 60%.

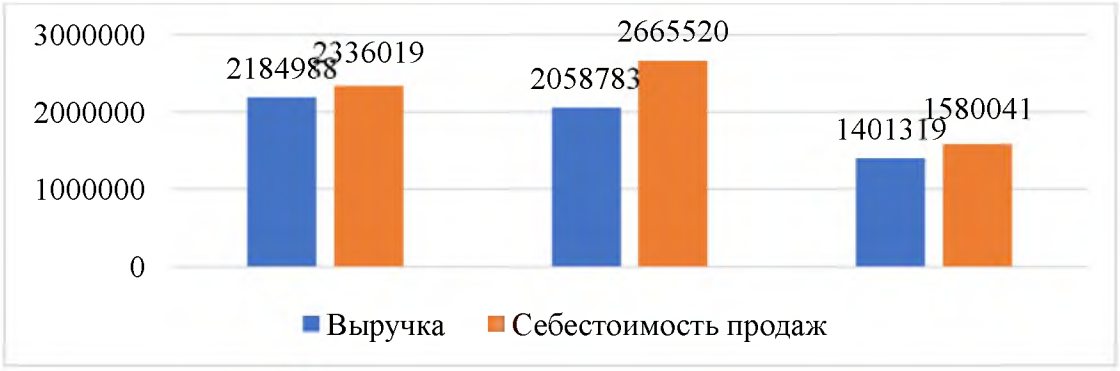

Рисунок 2.2 – Динамика выручки и себестоимости ПАО «Звезда» за 2021-2023 гг., тыс. рублей

Таблица 2.1 Основные показатели финансовых результатов в ПАО «Звезда» за 2021-2023 гг., тыс. рублей

Наименование показателя	2021 год	2022	2023
Выручка	2184988	2058783	1886878
Себестоимость	2336019	2665520	1580041
Чистая прибыль (убыток)	(256307)	(797279)	(703752)

Выручка в 2022 году уменьшилась на 6%, а в2023 году уменьшилась на 32%.

Таблица 2.2 – Показатели изменений финансовых результатов в ПАО «Звезда» за 2021-2023 гг., тыс. рублей

Наименование показателя	Изменение 2022 к 2021 году		Изменение 2023 к 2022 году	
	абсолютное	в %	абсолютное	в %
Выручка	-126205	-5,78	-657464	-31,93
Себестоимость продаж	329501	14,11	-1085479	-40,72
Валовая прибыль (убыток)	-455706	301,73	428015	-70,54
Коммерческие расходы	90	5,57	-1246	-73,04
Управленческие расходы	0		451153	
Прибыль (убыток) от продаж	-455796	298,59	-21892	3,60
Проценты к получению	-529	-65,15	-283	-100,00
Проценты к уплате	17423	20,35	11604	11,26
Прочие доходы	46783	55,08	-86440	-65,62
Прочие расходы	141064	74,28	-215864	-65,22
Прибыль (убыток) до налогообложения	-568029	165,89	95645	-10,51
Чистая прибыль (убыток)	-540972	211,06	93527	-11,73

Для нивелирования разницы во временных периодах, инфляционных изменений и оценки положения в конкретный момент и его сравнении в динамике используем относительные показатели эффективности предприятия.

В таблице 2.3 представлены показатели рентабельности.

Таблица 2.3 – Динамика показателей рентабельности ПАО «Звезда» за период 2021-2023 гг., %

Наименование показателя	2021 год	2022 год	2023 г.	Изменение 2023 к 2022 году	
				абсолютное	в %
Рентабельность затрат	-14,66	-34,16	-83,26	-49,10	143,76
Рентабельность продаж	-6,91	-29,47	-8,85	20,62	-69,97
Рентабельность производства	-2,13	-7,90	-9,05	-1,15	14,52
Рентабельность производства по себестоимости	-6,53	-22,83	-37,84	-15,02	65,79
Рентабельность собственного капитала	-193,43	-605,97			
Рентабельность активов (ROA)	-3,14	-9,09	-15,54	-6,45	71,01
Рентабельность заёмного капитала	-24,56	-50,68	-74,19	-23,51	46,38
Рентабельность валовой прибыли	-6,91	-29,47	-8,85	20,62	-69,97

Учитывая, что компания на протяжении анализируемого периода получает валовой убыток, убыток до налогообложения и чистый убыток, то показатели рентабельности отрицательны на протяжении всего периода.

При этом они не только отрицательны, но и в большинстве своём имеют тенденции к снижению в сравнении с показателями 2021 и 2022 года. Наихудшим по рентабельности для ПАО «Звезда» стал 2023 год.

Таким образом, можно сделать вывод, что ПАО «Звезда» ведёт неэффективную и нерентабельную деятельность. Компания на протяжении последних трёх лет получает убыток и находится в кризисном положении. При этом можно отметить крайне неэффективное управление себестоимостью.

Насколько эффективно использование основных средств можно судить

по ряду показателей. Значения данных показателей представлены в таблице 2.4.

Таблица 2.4 – Показатели обеспеченности и эффективности использования основных средств ПАО «Звезда» за 2021-2023 года

Показатель	2021 год	2022 год	2023 год	Изменение 2023 к 2022 году	
				абсолютное	в %
Фондовооруженность, тыс. руб./на чел.	681,22	1743,12	2202,00	458,88	26,33
Фондоотдача, руб.	2,37	0,94	0,50	-0,44	-46,80
Фондоемкость	0,42	1,06	1,99	0,93	87,97
Рентабельность (убыточность) ОПФ, %	-37,18	-41,72	-29,18	12,54	-30,05

Как мы можем увидеть, на конец 2023 г. фондовооруженность составила 2485,76 тыс. рублей на человека, что больше показателя на конец 2022 года на 42,60% (на 742,65 тыс. рублей) и практически более чем в 4 раза больше показателя 2021 года, что положительно характеризует использование основных средств, так как рост показателя происходит за счёт увеличения стоимости основных средств, стоимость которых на конец 2023 года составила 3468138 тыс. рублей.

Правда фондоотдача за данный период имеет тенденцию к снижению. Если в 2021 году на 1 рубль основных средств приходилось 2,37 рубля выручки, то в 2023 году этот показатель снизился до 60 копеек на 1 рубль выручки, что говорит о снижении эффективности и качества использования основных средств. Фондоёмкость за данный период имеет тенденцию к увеличению. Рентабельность основных производственных фондов в связи с убытком до налогообложения постоянно находится в отрицательных значениях. Стоит отметить, что на конец 2023 года данный показатель был наименьшим в анализируемом периоде. В таблице 2.5 представлены показатели эффективности использования персонала.

Из полученных данных мы видим, что производительность труда в 2023 году в среднем составила 1488,07 тыс. рублей на 1 человека, что ниже показателя 2022 года на 156,32 тыс. рублей, и ниже показателя в 2021

году.Стоит отметить, что в 2023 году среднесписочная численность персонала была ниже на 100 человек, чем в 2021 году.

Таблица 2.5 – Показатели эффективности использования персонала ПАО «Звезда» за 2021-2023 гг.

Показатели	2021 год	2022 год	2023 год	Изменение 2023 к 2022 году	
				абсолютное	в %
Выручка, тыс. руб.	2184988	2058783	1886878	-171905	-8,35
Среднесписочная численность персонала, человек	1352	1252	1268	16	1,28
Производительность за период, тыс. руб. на человека	1616,12	1644,40	1488,07	-156,32	-9,51

Снижение среднесписочной численности связано с сокращениями, которые последовала в качестве ответных реакций на кризис, связанный с локдауном, вызванным пандемией COVID-19. При этом именно в этот год отмечается наиболее высокая производительность труда. Косвенно можно судить о высокой организационной лояльности персонала, который увеличил свою выработку в столь нестабильной для предприятия ситуации.

Персоналу в ПАО «Звезда» уделяется высокое внимание. Даже в кризисный 2022 год работа с персоналом была направлена на обеспечение производства высококвалифицированными специалистами, привлечение и развитие новых молодых кадров. Выполнение этой задачи шло одновременно по нескольким направлениям:

– сохранение производственного потенциала, сложившегося в трудовом коллективе за долгие годы работы завода;

– поиск и прием новых, востребованных сегодня специалистов, их адаптация и закрепление на рабочих местах;

– повышение квалификации работников;

– профориентационные мероприятия с СУЗами и ВУЗами;

– развитие Молодежной организации ПАО «ЗВЕЗДА» ;

– реализация программ обучения по системе «Управление талантами» ;

– усиление трудовой дисциплины;

– соблюдение требований действующего трудового законодательства и обеспечение социальных гарантий, установленных законами и коллективным договором.

В 2023 году прошли обучение – 612 человек. Имея такой потенциал в человеческих ресурсах и высокую материальную базу, компания при этом находится в нестабильном финансовом положении, о чём свидетельствуют показатели ликвидности (таблицы 2.6 и 2.7) и показатели финансовой устойчивости (таблицы 2.8 и 2.9).

С целью оценки ликвидности был проведен анализ балансового соотношения между группами активов и пассивов, по результатам которых определяется тип ликвидности предприятия(таблица 2.6). На практике чаще всего встречаются такие варианты ликвидности (рисунок 2.3).

Рисунок 2.3 – Типы ликвидности [9]

Таблица 2.6 – Абсолютные показатели ликвидности баланса ПАО «Звезда» , тыс. рублей

Актив	2021 год	2022 год	2023 год
А1	189 923	112 773	106 963
А2	1 409 094	1 748 003	1 358 977
А3	3835136	3736344	3807841
А4	2570430	3949462	4729686
Баланс	8004583	9546582	10003467
Пассив	2021 год	2022 год	2023 г.
П1	6761749	6826578	8225837
П2	132444	116916	393588
П3 итог раздела IV	1105958	2209695	1765656
П4	4432	393393	-381614
Баланс	8004583	9546582	10003467
А1-П1	-6571826	-6713805	-8118874
А2-П2	1276650	1631087	965389
А3-П3	2729178	1526649	2042185
А4-П4	2565998	3556069	5111300

ПАО «Звезда» близка к нормальной ликвидности (однако помимо условия А1 и П1 нарушено также и балансирующее условие А4 и П4.

В такой ситуации платежеспособность компании снижена из-за задержек оплаты от клиентов или большой налоговой нагрузки в конкретный период. Компании следует обратить внимание на управление дебиторской задолженностью.

Для оценки платежеспособности предприятия используются также система коэффициентов ликвидности, расчёт которых для ПАО «Звезда» представлен в таблице 2.7

Коэффициент текущей ликвидности в ПАО «Звезда» на протяжении всего анализируемого периода ниже 1, а тенденции его изменения показывают ухудшение текущей ликвидности предприятия.

Таблица 2.7 – Динамика относительных показателей ликвидности ПАО «Звезда» за 2021-2023 гг., в долях

Коэффициенты	Нормативное значение	2021 год	2022 год	2023 год	Изменение 2023 к 2022 году	
					абсолютное	в %
Коэффициент абсолютной ликвидности	> 0,2	0,03	0,02	0,01	0,00	-23,59
Коэффициент критической ликвидности	0,7-1	0,23	0,27	0,17	-0,10	-36,54
Коэффициент текущей ликвидности	> 2	0,79	0,81	0,61	-0,19	-24,10

Такой низкий показатель свидетельствует о том, что у компании недостаточно средств, чтобы погасить свои краткосрочные обязательства до конца года.

Показатель быстрой ликвидности у ПАО «Звезда» находится в пределах от 0,2 до 0,3 на протяжении всего периода при необходимом нормируемом значении от 0,7 до 1, то есть погасить свои обязательства за счёт быстрореализуемых активов при необходимости предприятие также не сможет.

Аналогичная ситуация и с коэффициентом абсолютной ликвидности,

который показал, что у ПАО «Звезда» высоколиквидных активов меньше, чем краткосрочных обязательств. Нормативное значение коэффициента – больше 0,2 не выполняется с 2021 года.

Нарушенная ликвидность предприятия оказывает значительное влияние на его финансовую устойчивость, которая была оценена по абсолютным показателям состояния финансовых запасов и источников их покрытия. На основании этих данных для ПАО «Звезда» была построена трёхфакторная модель финансовой устойчивости (таблица 2.8).

На протяжении всего периода ПАО «Звезда» имеет Неустойчивое финансовое состояние М = (0, 0, 1), то есть собственных оборотных средств и долгосрочных обязательств недостаточно для финансирования запасов.

Таблица 2.8 – Анализ типа финансовой устойчивости ПАО «Звезда» , тыс. рублей

Формула расчёта	2021 год	2022 год	2023 г.	Изменение 2023 к 2022 году	
				абсолютное	в %
СОС = СК - ВОА	-2620888	-3635864	-5180161	-1544297	42,47
СДИ = СОС + ДКЗ	-1514930	-1426169	-3414505	-1988336	139,42
ОИЗ = СДИ + ККЗ	5434153	5597120	5273781	-323339	-5,78
ΔСОС = СОС – З	-6451191	-7358141	-8969307	-1611166	21,90
ΔСДИ = СДИ – З	-5345233	-5148446	-7203651	-2055205	39,92
ΔОИЗ = ОИЗ – З	1603850	1874843	1484635	-390208	-20,81
ΔСОС	0	0	0		
ΔСДИ	0	0	0		
ΔОИЗ	1	1	1		

Приходится брать краткосрочные заемные средства. Из-за этого ситуация становится напряженной в плане возврата долга. Ведь если оборачиваемость запасов длиннее по времени, чем срок кредита, то первые еще не успеют принести доход и деньги, когда наступит дата погашения обязательств.

Здесь стоит отметить, что оборачиваемость запасов в целом находится на одном уровне, но длительность оборота на конец 2023 года составила 716,56 дней, что на 56,23 больше показателя 2022 года (на 22дня меньше показателя 2021 года). Такой период оборота запасов значительно выше срока возврата краткосрочных обязательств, сумма которых в 2023 году выросла ещё больше.

Заёмные источники преобладают над собственным капиталом и занимают значительную долю в валюте баланса (таблица 2.9). Показатели финансовой устойчивости находится не в норме уже несколько лет.

Обобщая проведенный анализ, можно сделать вывод, что ПАО «Звезда» находится в кризисном финансовом положении в течении последних трёх лет. Причём по ряду показателей можно сказать, что деятельность предприятия в 2022 году, несмотря на кризис во всей мировой экономике, была эффективнее.

Таблица 2.9 – Относительные показатели финансовой устойчивости ПАО «Звезда»

Наименование показателя	Норма	2021 год	2022 год	2023 г.	Изменение 2023 к 2022 году	
					абсолютное	в %
Коэффициент финансовой независимости (Кфн)	Кфн> 0.5	-0,01	0,03	-0,05	-0,08	-237,09
Коэффициент задолженности (Кз)	0,5 ≤ Кз ≤ 0,8	-159,64	29,44	-23,21	-52,65	-178,82
Коэффициент обеспеченности собственными оборотными средствами (Ко)	≥ 0,1	-0,48	-0,65	-0,98	-0,33	51,21
Коэффициент финансовой зависимости	тенденция к снижению	-158,64	30,44	-22,21	-52,65	-172,95
Коэффициент маневренности(Км)	0,2 ≤ Км≤ 0,5.	51,94	-11,59	11,50	23,09	-199,18
Коэффициент (концентрации заемного капитала) финансовой напряженности (Кф. напр.)	0 ≤ КЗ ≤ 0,5.	1,01	0,97	1,05	0,08	8,05
Коэффициент соотношения мобильных и иммобилизованных активов(Кс)	индивидуален	2,11	1,42	1,12	-0,30	-21,32

Частично это связано с сокращением персонала и соответственно снижением затрата на него (фонд оплаты труда с отчислениями на социальные нужды в 2022 году на 1252 человека составлял 1 147 293 тыс. рублей, если бы

численность персонала была на уровне 2021 года, то ФОТ составил бы на 91 637 тыс. рублей больше).

Обобщенно экономическая эффективность использования оборотных средств предприятия представлена в таблице 2.9.

Таблица 2.10 – Динамика показателей экономической эффективности использования оборотных средств в ПАО «Звезда» за период 2021- 2023 гг.

Наименование показателя	2021 год	2022 год	2023 г.	Изменение 2023 к 2022 году	
				абсолютное	в %
Коэффициент оборачиваемости	0,35	0,37	0,35	-0,03	-7,00
Продолжительность одного оборота, дни	1045,09	977,86	1051,4	73,58	7,52
Рентабельность оборотных средств, %	-4,10	-14,45	-27,94	-13,49	93,30

Анализ экономической эффективности использования оборотных средств показал, что оборотные активы предприятия также используются крайне неэффективно. Коэффициент оборачиваемости очень низкий и на протяжении периода изменился в сторону уменьшения.Период оборота значительно повысился и составляет практически 3 года. Рентабельность оборотных средств также отрицательна и имеет тенденцию к ухудшению.

Рассмотрим показатели оборачиваемости оборотных средств более подробно (таблица 2.11 и 2.12).

Таблица 2.11 – Динамика оборачиваемости оборотных средств в ПАО «Звезда за период 2021-2023 гг., количество оборотов

Показатель	2021 год	2022 год	2023 год	Изменение 2023 к 2022 году	
				абсолютное	в %
Коэффициент оборачиваемости активов	0,27	0,23	0,19	-0,04	-17,72
Коэффициент оборачиваемости оборотных активов	0,35	0,37	0,35	-0,03	-7,00
Коэффициент оборачиваемости денежных средств	9,61	13,60	17,17	3,57	26,25
Коэффициент оборачиваемости краткосрочных финансовых вложений	2184,99				
Коэффициент оборачиваемости дебиторской задолженности	1,48	1,36	1,24	-0,11	-8,44
Коэффициент оборачиваемости запасов	0,49	0,55	0,50	-0,04	-7,85

Производственный цикл сильно затянут, даже несмотря на то, что производство продукции и её особенности требуют значительных временных затрат.

Таблица 2.12 – Динамика показателей продолжительности оборота оборотных активов, в днях

Показатель	2021 год	2022 год	2023 год	Изменение 2023 к 2022 году	
				абсолютное	в %
Продолжительность оборота активов	1346,17	1534,50	1864,99	330,49	21,54
Продолжительность оборота оборотных активов	1030,77	964,47	1037,04	72,57	7,52
Продолжительность оборота денежных средств	37,45	26,46	20,96	-5,50	-20,79
Продолжительность оборота краткосрочных финансовых вложений	0,16	0,00	0,00	0,00	
Продолжительность оборота дебиторской задолженности	243,29	265,16	289,59	24,43	9,21
Продолжительность оборота запасов	738,19	660,32	716,56	56,23	8,52

Оборачиваемость дебиторской задолженности снизалась, а длительность оборота увеличилась на 24 дня, составив при этом на конец 2023 года 290 дней. То есть по сути ПАО «Звезда» кредитует своих клиентов практически на год. При этом тенденция к увеличению срока не меняется с 2021 года

С другой стороны, в её управлении можно отметить положительный факт: её снижение в структуре баланса на конец 2023 года. Её доля значительно ниже доли кредиторской задолженности (соотношение на конец 2023 года составляло 13,48% против доли кредиторской задолженности в 82,23%). Помимо этого стоит отметить, что большинство продукции имеет длительный период изготовления и сборки, что изначально предполагает длительные сроки договоров и оплаты.

Краткосрочных финансовых вложений в компании нет, поэтому в обороте они не участвуют, а денежные средства оценивать с точки зрения оборачиваемости не имеет смысла из-за их быстрой мобильности.

Про оборачиваемость запасов и увеличение их срока оборачиваемости было сказано уже выше.

Обобщая полученные данные, можно сделать вывод, что финансовое состояние в последние годы в ПАО «Звезда» трудно назвать устойчивым.

2.2 Анализ информационных систем, функционирующих на ПАО «Звезда»

Обеспечивают деятельность предприятия различные автоматизированные системы.

Автоматизированная система ПАО Звезда основана на продуктах: InforCloudSuite Industrial (ранее ERP SyteLine) (на базе: InforCloudSuite) и ЦУП: DataCollection. Данные продукты реализованы на следующих технологиях:

Технология: APS - Системы синхронного планирования производств

Технология: ERP

Технология: MES – Управление производствами и ремонтами

Технология: SCADA

InforCloudSuite Industrial – специально разработанная информационная система для управления ресурсами среднемасштабных промышленных предприятий. Система имеет встроенный модуль InforSyteLine APS (Advanced Planning &Scheduling) – синхронное планирование и оптимизация.

Программный продукт позволяет автоматизировать управление запасами и закупками, планирование потребностей в сырье и материалах, прогнозирование производственных мощностей, обслуживание клиентов и обработку заказов.

Главное преимущество InforSyteLine – расширенные возможности для оперативной обработки заказов, гарантирующие их стопроцентное выполнение даже при большом объеме быстроменяющихся вводных.

Решение позволяет управлять производственным графиком, контролировать качество выпускаемой продукции, администрировать проекты

и финансы предприятия.

Система штрихкодирования ЦУП: Data Collection (разработана Фронтстеп СНГ для российских промышленных предприятий), доказала свою эффективность и используется во всех подразделениях: производственные цеха, планово-распределительные бюро (ПРБ), склады отдела материально-технического снабжения (ОМТС), производственные склады всех типов.

Функциональность ЦУП:Data Collection позволяет производить регистрацию полного или частичного выполнения технологических операций определенными ресурсами (станки/рабочие) в рабочих центрах, а также передачу изделий с операции на операцию между рабочими центрами.

Решение ЦУП:Data Collection является полностью российской разработкой и зарегистрировано в государственном реестре программ для ЭВМ под номером 2016662641. Легко интегрируется в качестве модуля с различными ERP/APS/MES-системами через собственную интеграционную платформу.

Система построена на технологии штрих-кодирования, и обеспечивает в режиме реального времени производственное предприятие полной и своевременной информацией.

Благодаря ЦУП:DC осуществляется оперативный ввод различных данных на всех этапах производственного процесса (рисунок 3.4)

Модуль обеспечивает возможность проверить выполнение каждого производственного задания в реальном времени, что дает дополнительные инструменты для контроля соблюдения сроков - наличие своевременного доступа к объективным данным позволяет точно планировать производственные ресурсы и отслеживать выполнение заказов.

Помимо удобства, ЦУП:DC позволяет значительно ускорить ввод данных и избежать потенциальных ошибок, связанных с «человеческим фактором» .

Сотрудники производственных предприятий могут работать с любой комбинацией устройств сбора данных.

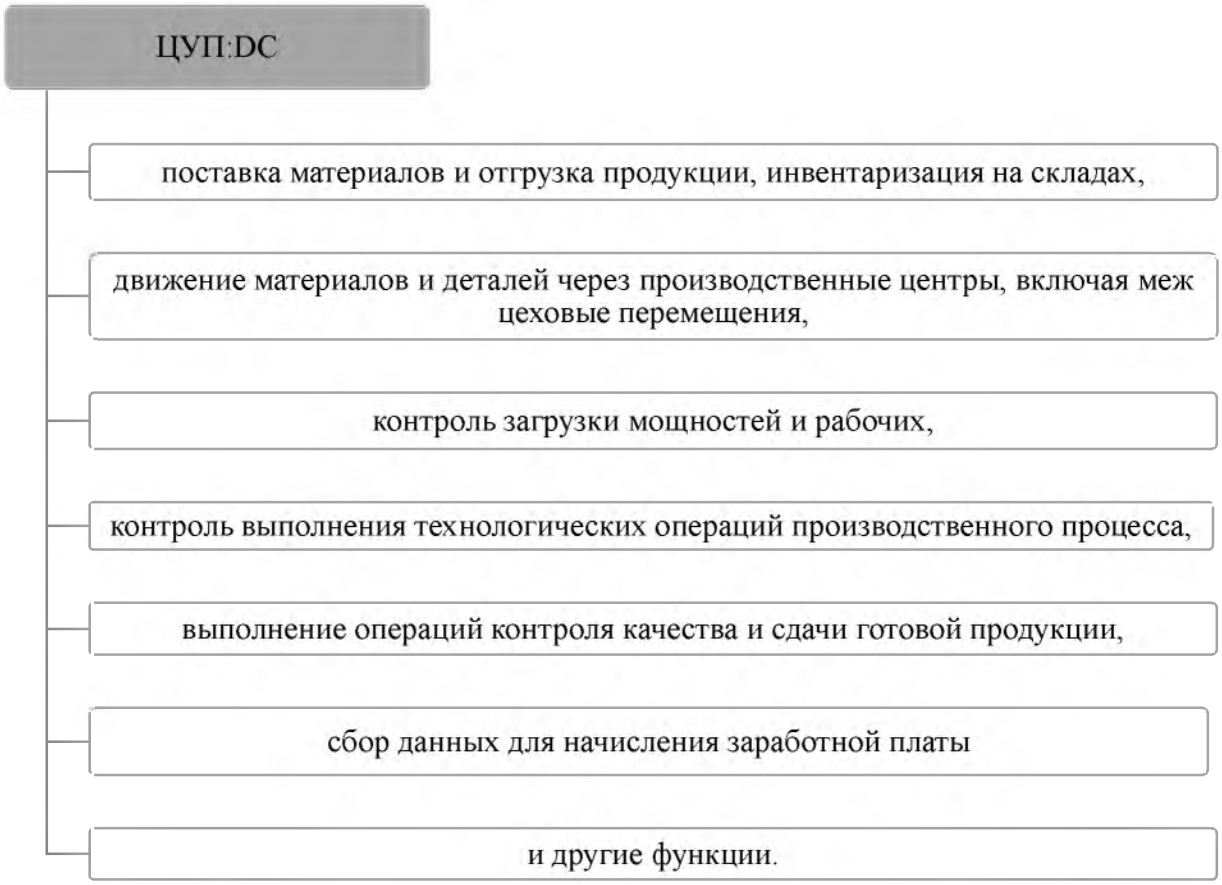

Рисунок 2.4 – Возможности система штрихкодирования ЦУП: Data Collection

Документооборот в компании построен на системе NauDoc. СЭД NauDoc предназначена для автоматизации отправки и получения корреспонденции, внутренних документов организации, ведения электронного архива документов.

NauDoc позволяет автоматизировать внутренние процессы согласования, регистрации, учета и контроля исполнения документов, вести электронный и бумажный архив. Основные преимущества использования данного ПО представлены на рисунке 3.5.

Используя СЭД NauDoc, компания получает возможность организовать единое хранилище документов с разграничением прав доступа, что позволит его сотрудникам в любой момент времени иметь доступ ко всем необходимым им документам и в кратчайшие сроки находить всю нужную информацию. При этом информация доступна вне зависимости от присутствия на рабочем месте сотрудника.

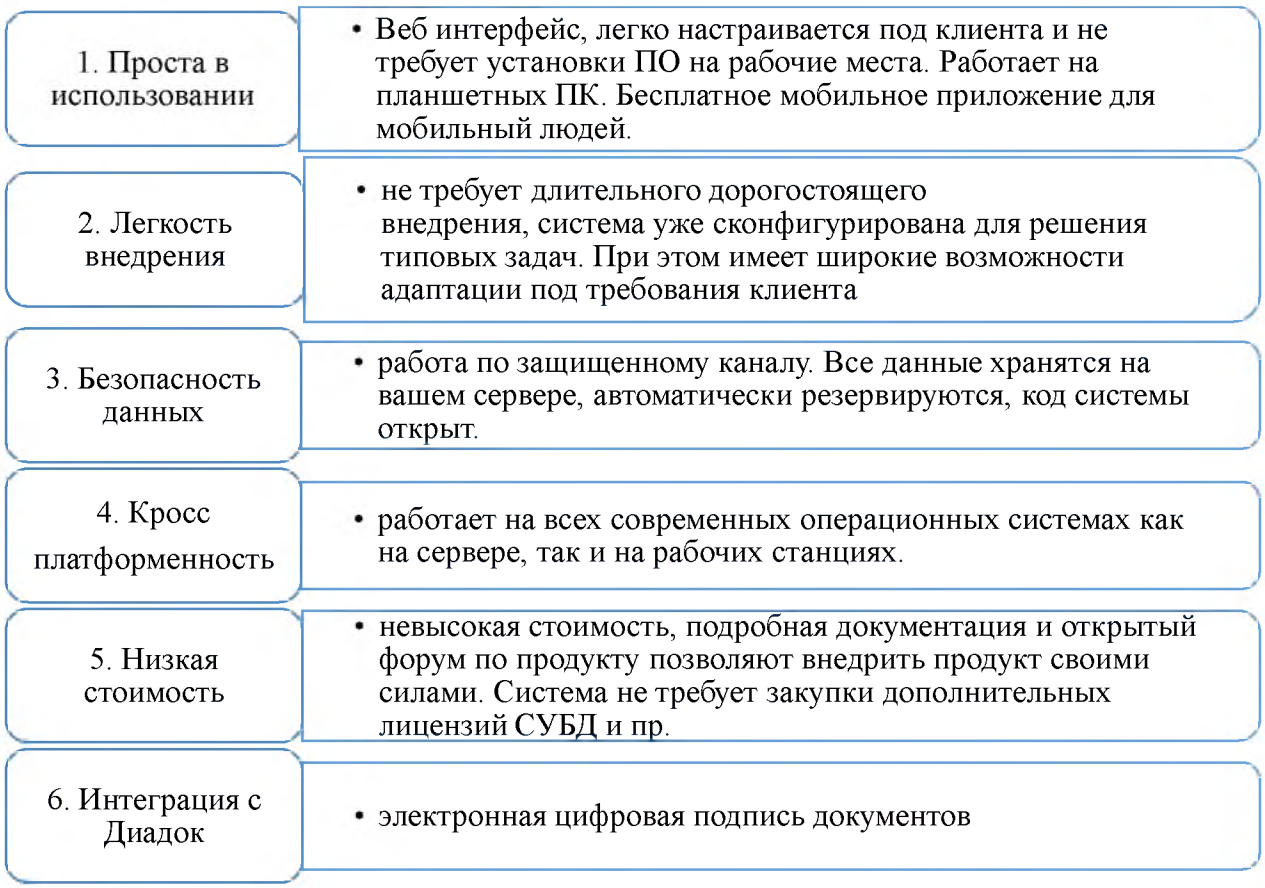

Рисунок 2.5 – Возможности системы электронного документооборота NauDoc

Журналы регистрации позволяют регистрировать входящие, исходящие и иные внутренние документы, отслеживая перемещение бумажных копий документов между сотрудниками.

Бухгалтерский учёт осуществляется при помощи 1С:Предприятие (версия 8.3.). Система программ «1С:Предприятие» состоит из технологической платформы (ядра) и разработанных на ее основе прикладных решений («конфигураций»).

В 2022 году проводилась адаптация и модификация информационной системы на базе программного продукта «1С:Документооборот КОРП» в ПАО «Звезда» . Был осуществлен проект по разработке обработок обмена контрагентами между различными базами в ПАО «Звезда».

В настоящее время на предприятии используется информационная система на базе программных продуктов «1С:Бухгалтерия предприятия» и «1С:Управление торговлей» , «1С:275ФЗ» , «1С:Документооборот 8 КОРП».

Были произведены работы по разработке синхронизации нормативно-справочной информации между существующими информационными системами.

Работы были начаты в апреле 2022 года. Работы проводились в соответствии с Техническим заданием и включали в себя следующие этапы:

1. Реализация обработок для типовой конфигурации «1С:Бухгалтерия предприятия» с возможностью запуска по расписанию, которая будет выгружать весь справочник Контрагентов в файл с заданными реквизитами;

2. Реализация обработок для типовой конфигурации «1С:Управление торговлей» с возможностью запуска по расписанию;

3. Реализация обработок для типовой конфигурации «1С:275ФЗ»

4. Реализация обработок для типовой конфигурации «1С:Документооборот8 КОРП» .

5. Настройка во всех информационных системах администраторских прав пользователей, позволяющих ввод новых контрагентов и редактирование реквизитов(рисунок 2.6).

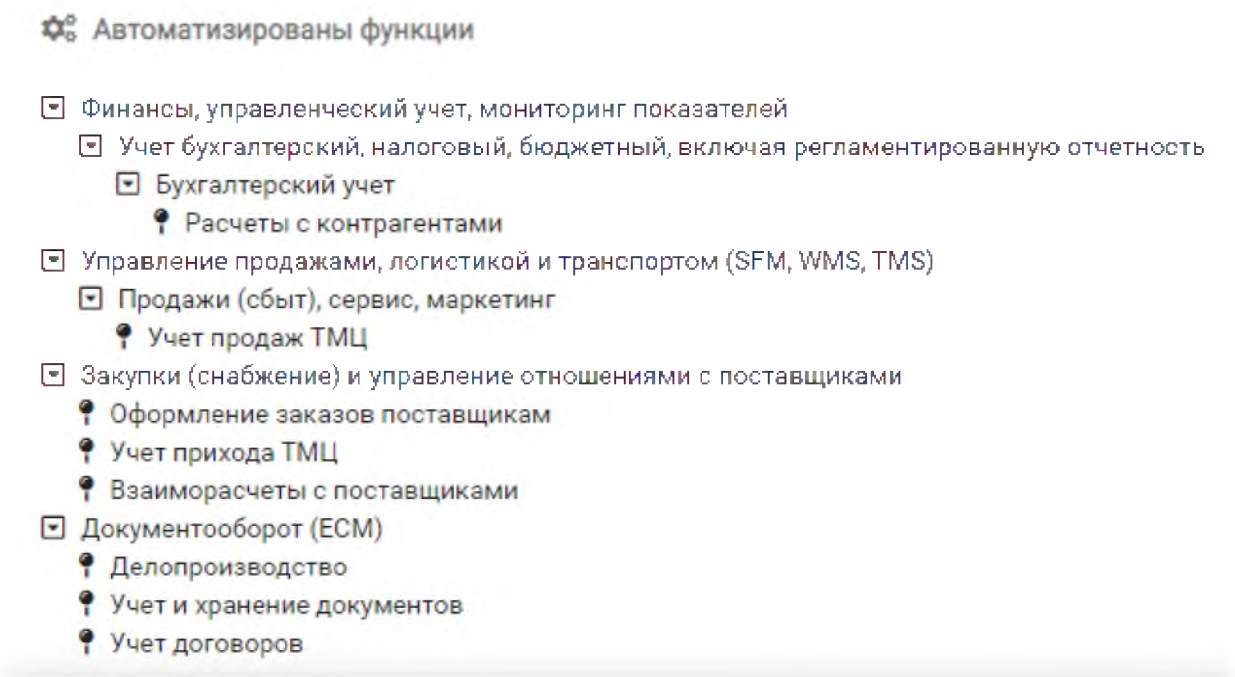

Рисунок 2.6 – Автоматизированные функции в рамках проекта Адаптация и модификация информационной системы на базе программного продукта «1С:Документооборот КОРП» в ПАО «Звезда»

Выполненные работы затрагивают следующие автоматизированные функции информационной системы:

Бухгалтерский учет (расчеты с контрагентами);

Учет договоров;Делопроизводство;Учет продаж ТМЦ;

Оформление заказов поставщикам;

Управление отношениями с поставщиками

Проект по разработке обработок обмена контрагентами между различными базами успешно завершен 20 мая 2022 года. Функционал разработан и запущен в промышленную эксплуатацию в информационной системе с расчетным количеством в 150 рабочих мест. В настоящее время ведется планирование работ по развитию функционала системы.

В результате выполнения проекта сократились трудозатраты пользователей на ввод информации, повысилось качество нормативно-справочной информации, используемой в информационной системе.Обеспечена синхронизация нормативно-справочной информации между существующими информационными системами, обеспечена возможность работы с документами, процессами и задачами.

Можно сделать вывод, что управление многими процессами в ПАО «Звезда» в большей степени является автоматизированным.

3 Разработка предложений по нейтрализации угроз экономической безопасности ПАО «Звезда» в части обеспечения информационной безопасности

3.1 Формирование мероприятий по обеспечению информационной безопасности и нейтрализации угроз в ПАО «Звезда»

Одним из главных способов защиты от угроз является нейтрализация их источников. Это может быть достигнуто за счет принятия комплекса мер, включающих в себя оценку уровня угрозы, выявление потенциальных уязвимостей, регулярное обновление систем безопасности, повышение уровня осведомленности и обучения персонала.

Согласно выявленным угрозам в главе 1 мы можем сделать вывод о том, что на данный момент компания подвержена следующим угрозам:

1. Снижение доли организаций, осуществляющих технологические инновации, что может негативно сказаться как на реализуемых проектах организации, так и на снижении уровня защиты информационных систем.

2. Риск утечки информации путём киберпреступлений против компании. Технологии компании имеют высокий интерес для конкурентов и мошенников. С учётом возможного повышения количества преступлений в сфере информационной безопасности информация предприятия может стать предметом частых атак.

3. Недостижение поставленных задач в области приёма обучающихся на программы высшего образования в сфере информационных технологий может привести к снижению доли населения трудоспособного возраста в общей численности населения в сфере информационных технологий, что может привести предприятие к дефициту рабочей силы как в области обеспечения деятельности компании и его автоматизированных и информационных систем, так и в области защиты данных систем.

4. Риск взлома ПО и простоя как на уровне предприятия, так и на уровне государственных информационных систем в результате компьютерных атак.

Взаимосвязь предприятия с государственными системами находится на достаточно высоком уровне, так как компанией выполняются оборонные заказы государства.

В приложении 2 представлены нормативно-правовые акты в области защиты информации, на которые опирается предприятие для защиты информации. В таблице 3.1 и более подробно в приложении3 представлен анализ существующих угроз для ПАО «Звезда»

Таблица 3.1. - Анализ существующих угроз для ПАО «Звезда»

Виды угроз	Типы угроз и атак	Методы НДС	Меры противодействия
1.Естественные угрозы	Пожар		оборудование помещений противопожарными датчиками и средствами пожаротушения,
2.Исусственные	Непреднамеренные	Установка программ на компьютер не входящих в список необходимых для работы, использование личных накопителей информации на рабочем неготовность пользователей к фишинговым атакам использование незащищенных беспроводных сетей, открытые USB-порты и возможность бесконтрольного использования съемных носителей;	Использование только специализированных программ и флэшкарт на рабочем компьютере, Запрет передачи информации и копирования. Резервное копирование.DLP -системы - для предотвращения утечки конфиденциальных материалов, Siem -системы для централизованного мониторинга информационной безопасности
	Преднамеренные внутренние	Недовольные сотрудники Установка программ на компьютер не входящих в список необходимых для работы	инструкции по обращению с техникой, системами, где обрабатывается конфиденциальная информация криптозащиты: шифрование файлов,разграничение доступа
	Преднамеренные Внешние: -DDoS-атака,	— DDoS-атака. Это виртуальная атака на ресурсы компании, которая приводит к замедлению или полному прекращению их работы. -	

Продолжение таблицы 3.1

	Вирусы		Антивирусы, сетевая защита
	Спам	комплекс настроек, различные средства для фильтрации нежелательных сообщений, , авторитетные почты и соответствующие ключевые слова	
	Утечки информации при обмене и передачи информации по открытой сети	Утечка инженерно-технических средств, данных автоматизированных систем. В результате - остановка производства	виртуальные частные сети (VPN), двухфакторная аутентификация пользователя.
	Попытки взлома компьютерных систем	на уровне сетевого программного обеспечения, баз данных и операционной системы	
	Радиоэлектронные каналы утечки информации	такие информационные каналы, которые возникают за счет широкого вида побочных электромагнитных излучений и наводок (ПЭМИН)	блокируется с помощью использования специальных устройств за щиты - генераторов шума
	Акусти-ческие	неконтролируемое распространение звуковых волн в звукопроводящих средах	Через дверь кабинетов-установка доводчиков дверей
	Оптические	от носятся компьютерные мониторы, информация на бумажных носителях, графи ческие изображения и схемы, а так же изображения отраженные в зеркалах и глянцевых поверхностях.	Через окно-установка жалюзи, защитная пленка на экран компьютера, которая уменьшает угол обзора до 60 градусов.
	Материально-вещественные	Неправильно утилизируется документация на бумажных и электронных носителях, кража ценных вещей и документов	и требуется приобрести уничтожители бумаги-шредеры и приобретение сейфов в кабинеты

Все мероприятия по обеспечению защиты информации должны быть целесообразными и сопоставимыми с возможным ущербом вследствие кражи или утечки конфиденциальной информации.При разработке Политики

информационной безопасности необходимо определить не только массивы информации, подлежащие защите, объекты защиты, безопасность которых позволяет защитить данные от утечек или разглашения, но и установить градации уровня секретности (конфиденциальности). Согласно статье 8 закона «О государственной тайне», на уровне государства уровень секретности информации должен соответствовать степени тяжести ущерба, который может быть нанесён безопасности государства вследствие распространения указанных сведений.В настоящее время существует три уровня секретности и соответствующие им грифы секретности: секретные, совершенно секретные, особой важности[42].

В работе предлагается предприятию ПАО «Звезда», выполняющего оборонные заказы государства, разделить конфиденциальную информацию на четыре уровня.Каждому уровню определить условную стоимость на единицу информации (Мбайт):

1) Уровень 1 -низкая степень защиты - 1000 руб.;
2) Уровень 2 - средняя степень защиты – 2500 руб.;
3) Уровень 3 - высокая степень защиты4000 руб.;
4) Уровень 4 - наивысшая степень защиты– 5000 руб.;

Общую стоимость конфиденциальных данных каждого уровня определяют произведением стоимости защищаемой информации в рублях за 1 мегабайт информации на объём защищаемой информации в мегабайтах формула 3.1.

$$C=V*Z \qquad (3.1)$$

Где С – стоимость защищаемой информации в условных единицах;

V – объем защищаемой информации в мегабайтах;

Z – цена за 1 мегабайт информации;

Данные по стоимости и объему информационных объектов представлены в таблице 3.2.

Таблица 3.2. – Объем и стоимость элементов информации согласно уровням конфиденциальности, закрепленных в Политике информационной безопасности предприятия

Перечень данных	Объём, Мбайт	Уровни конфиден-циальности	Стоимость за единицу информации в соответствии с уровнем, руб.	Стоимость информации, руб.
1.Сведения о структуре управления, методика обучения персонала.	100	Уровень 1	1000	100 000
2.Персональные данные сотрудников	500	Уровень 2	2500	1 250 000
3. Информация об источниках финансирования	100	Уровень 3	4000	400 000
Автоматизированные системы:InforCloudSuiteIndustrial (на базе: InforCloudSuite) и ЦУП: DataCollection. : Технология: APS - Системы синхронного планирования производств Технология: ERP Технология: MES – Управление производствами и ремонтами Технология: SCADA	15000	Уровень 3	4000	60 000 000
«1С:Документооборот8 КОРП»:-1С:Бухгалтерия, -1С:Управление торговлей, 1С:275ФЗ(Бухгалтерский учет (расчеты с контрагентами); Учет договоров; Делопроизводство;Учет продаж ТМЦ;Оформление заказов поставщикам)	25000	Уровень 3	4000	100 000 000
Документооборот в системеNauDoc	20 000	Уровень 3	4000	80 000000
Инженерно-техническая документация для производства продукции по оборонным заказам документы стратегического характера; научная информация, данные НИОКР(сведения об изобретениях и о полезных моделях; сведения)	60 000	Уровень 4	5000	300 000 000

Продолжение таблицы 3.2

Инженерно-техническая документация для производства продукции по обычным заказам	20 000	Уровень4	5000	100 000 000
Сведения об организации и технических решениях по системе охраны (система контроля доступа) производственных помещений.	800	Уровень 4	5000	4000 000
Информация о клиентах, банковских операциях, номера счетов и кредитных карт.	600	Уровень 4	5000	3 000 000
Сведения, содержащие клиентскую базу, данные о покупателях и заказчиках, данные о поставщиках, коммерческие связи.	1000	Уровень 2	2500	2500 000
Архивные сведения	10 000	Уровень 2	2500	25 000 000
Условия по сделкам и соглашениям, условия кон трактов, в т.ч. оборонных	4000	Уровень 4	5000	20 000 000
Сведения о расчетах тарифов, структуре и расчете цен, о продажной калькуляции, затратах.	100 000	Уровень 3	4000	400 000 000
Итого:				1 097150 000

Таким образом, ПАО «Звезда» располагает конфиденциальными данными на сумму 1 097 150 тыс. руб. Общий объем конфиденциальных данных и их структура представлены в таблице 3.3.

Таблица 3.3- Общий объем и структура конфиденциальных данных в ПАО «Звезда»

Уровень конфиденциальности	Объём , Мб	Стоимость информации в руб.	Структура, %
Уровень 1	100	1000 000	0,1
Уровень 2	11500	28750 000	2,9
Уровень 3	160100	640 400 000	58
Уровень 4	85400	427000000	39
Итого	257100	1 097 150 000	100,0

Анализ каналов утечки информации позволил локализовать все угрозы информационной безопасности: оптический съем данных через окно,

оптический и акустический съем данных через открытую дверь, перехват ПЭМИН, получение доступа к документам, при неправильной утилизации; хакерские атаки, утечки информации при обмене и передачи информации по открытой сети и использование компьютерных вирусов.

3.2 Экономическое обоснование предложений и комплекса мер информационной безопасности ПАО «Звезда»

На современном рынке средств информационной безопасности достаточно широко представлено оборудование и программное обеспечение от простых и бюджетных моделей, до уникальных и дорогих комплектов и систем. Исходя из этого, любой организации без затруднений можно подобрать наиболее подходящие ей средства защиты информации учитывая свои потребности. Анализ каналов утечки информации позволил локализовать все угрозы информационной безопасности:

- оптический съем данных через окно;
- оптический и акустический съем данных через открытую дверь;
- перехват ПЭМИН;
- получение доступа к документам, при неправильной утилизации;
- хакерские атаки,
- использование компьютерных вирусов;
- неготовность пользователей к фишинговым атакам;
- использование незащищённых беспроводных сетей;
- открытые USB-порты и возможность бесконтрольного использования съёмных носителей;
- наличие устаревших версий компонентов.

Для достижения полной защиты информации следует локализовать все выявленные угрозы. Наиболее эффективный и экономичный способ решения проблемы оптической утечки информации через оконные проемы в помещениях с циркулирующими конфиденциальными данными - это установка

жалюзи, что позволяет исключить возможность утечки информации через окна.Установка доводчиков на каждую дверь помещений как жилых, так и административных, позволит исключить возможность утечки информации сразу по 2-м каналам: акустическому и оптическому. Благодаря этой мере снизится вероятность слежки методом подслушивания и подсматривания. Кроме этого, необходимо расположить столы и рабочее оборудование таким образом, чтобы у злоумышленника не было невозможности видеть мониторы компьютеров. Дополнительным решением для защиты мониторов от по сторонних глаз является защитная пленка-антишпион, которая уменьшает угол обзора до 60 градусов. Данное средство защиты можно приобрести по цене 2000 руб./штука для 200 рабочих мест.Для возможности утилизации бумажных носителей без возможности по следующего извлечения из них информации требуется приобрести уничтожители бумаги-шредеры-Гелеос УМ22-5 стоимостью 18000 руб. в количестве 5 штук.

Чтобы исключить возможность кражи или не правильного использования важной документации или других ценностей предприятия, было принято решение установить два сейфа в бумажном архиве, стоимостью 150 000 руб. каждый.

Неконтролируемое распространение конфиденциальных данных по каналу ПЭМИН блокируется с помощью использования специальных устройств за щиты - генераторов шума. В Российской Федерации уделяется большое внимание вопросам подавления побочных электромагнитных излучений и наводок, поэтому современный рынок достаточно широк в плане выбора подобных устройств. Например, генератор шума «Соната-Р2» стоимостью 5000 руб. штука в количестве 50 штук.Устройство «Соната-Р2» является техническим средством защиты информации, от утечки информации за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума и соответствует требованиям «Норм защиты информации, обрабатываемой средствами вычислительной техники и в автоматизированных системах, от утечки за счет

побочных электромагнитных излучений и наводок» и технических условий ЮДИН.665820.003 ТУ. Устройство может устанавливаться в выделенных помещениях до 1 категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. Соответствие подтверждается сертификатом ФСТЭК России

Для защиты информации на предприятии имеется отдел безопасности и системный администратор. Эти специалисты ведут мониторинг всех событий, выявляют, анализируют и предотвращают атаки.Однако система безопасности не отвечает своевременно на все современные угрозы. Кроме того, утечки информации невозможно обнаружить сразу же, они выявляются уже после последствий. Для круглосуточного мониторинга необходимо использовать специальный программный комплекс – DLP-систему -Data LeakPrevention. Она следит за перемещением информации по сети и компьютерам предприятия. Предотвращает попытки скопировать конфиденциальную информацию, анализирует и контролирует всю информацию, отправляемую через почту, браузер, копируемую на съёмные носители или в облако. Она предупредит специалиста безопасности о потенциально опасных действиях работников,обнаружит на рабочих станциях документы, которых здесь быть не должно, вход в системы без допусков. Кроме того, она ведёт учёт рабочего времени, оценивает его производительность.

Для защиты необходимы инструменты: VPN, антивирусы, защита от DDoS-атак, а такжеSiem-системы,DLP-систему обеспечивающие закрытие всех потенциальных каналов утечки информации и перехват исходящего трафика.

Для работы с госзаказом в России в сфере мониторинга деятельности сотрудников и защиты данных оптимально подходит DLP-система StaffCop Enterprise[43].

Программное обеспечение Staffcop Enterprise предназначено для обеспечения информационной безопасности и улучшения эффективности работы организаций и предприятий.

Staffcop Enterprise состоит из двух частей: сервера и службы-агента.

Агент запускается на рабочих станциях сотрудников или терминальных серверах, собирает данные действий пользователя и события, передает и сохраняет их на сервере для обработки и визуализации. В дальнейшем сервер позволяет собирать, анализировать, обрабатывать, визуализировать и осуществлять поиск информации [43].Staffcop может работать как в рамках локального закрытого периметра, так и с учетом компьютеров, находящихся за его пределами, в том числе и на ПК сотрудников, которые работают удаленно.

Это решение имеет сертификацию ФСТЭК и отвечает требованиям российского законодательства по защите информации, что делает его подходящим для проектов, связанных с государственным заказом. Рассчитаем ориентировочный бюджетстоимости оборудования и мероприятий для обеспечения информационной безопасностидля предприятия на 200 рабочих мест.

1. Лицензия и поддержка StaffCop[43]

Стоимость лицензии: Разовая лицензия на StaffCop для 1 сотрудника от 3000 до 5000 руб. Возьмем среднее значение-4000 руб. Тогда для200 сотрудников (на 200 ПК) 200х4000 руб.=800 000 руб.

Поддержка и обновления: Годовая техническая поддержка и обновления, обеспечивающие поддержку продукта в актуальном состоянии, обойдутся примерно в 150,000 рублей в год.

Итого: лицензия на StaffCopи поддержка -950 000 руб. в год.

2. Сертификация и соответствие ФСТЭК и ФСБ

Для соответствия требованиям государственных стандартов потребуется:

А) Закупка сертифицированного ПО и оборудования: версия StaffCop с сертификацией ФСТЭК стоит на 30–50% дороже.

В результате лицензия и годовая поддержка могут стоить 950 000х1,3=

1 235 000 рублей.

Б) Прохождение сертификации: Компания может пройти сертификацию на соответствие требованиям ФСТЭК и ФСБ. Этот процесс обычно требует как

внешнего аудита, так и выполнения требований сертификационной организации.

Стоимость сертификации инфраструктуры для компаний среднего размера может составить от 500,000 до 1,000,000 рублей. Эта сумма включает подготовку документов, внешний аудит, настройку инфраструктуры под требования безопасности, а также регулярные проверки на соответствие стандартам. Чтобы поддерживать соответствие стандартам, компании необходимо будет проходить ежегодные проверки, стоимость которых составит примерно 100,000–300,000 рублей.

Итак: сертификацияинфраструктуры -500 000 руб., ежегодные проверки на соответствие стандартам-100 000 руб.

Итого: 1235 000 +500 000+ 100 000руб.= 1 705 000 рублей на первый год, включая сертификацию, проверку и поддержку.

3. Инфраструктура для выполнения требований ФЗ-242 и ФЗ-152

Чтобы соответствовать требованиям ФЗ-242 (локализация данных в РФ) и ФЗ-152 (персональные данные), необходима защита инфраструктуры, где будет храниться и обрабатываться информация.

На хранение и защиту данных в соответствии с требованиями потребуется серверное оборудование, желательно с избыточностью и защищенным каналом связи. Стоимость сервера с возможностью локального хранения и бэкапов — около 200000–400000 рублей (в зависимости от требований к защите данных).

Итого: серверное оборудование и защита данных- 300 000руб.

4.Резервное копирование и защита данных: Ежегодные затраты на резервное копирование и поддержку защиты информации составляют примерно 50,000–100,000 рублей.

Итого:Резервное копирование и защита данных -100 000 руб.

5. VPN и контроль каналов связи. Для предотвращения утечек потребуется организовать защищенные каналы связи и, возможно, интегрировать VPN. Это добавит еще 80 000–100000 рублей к единовременным

затратам на оборудование и 10000–30 000 рублей на обслуживание.

Итого: VPN и контроль каналов связи-100 000 +30 000=130 000 руб. на первый год (включая оборудование и базовое обслуживание).

6.Обслуживание и аудит информационной безопасности

Ежегодные аудиты информационной безопасности: стоимость проведение ежегодных проверок на соответствие стандартам ФСТЭК и ФСБ составляетоколо 100000–300000 рублей в зависимости от сложности и глубины проверки. Аудит-200 000руб.

7.Выявление уязвимостей и мониторинг: постоянный мониторинг и анализ уязвимостей с регулярными отчетами. Затраты могут составить 30,000–50,000 рублей в месяц (аутсорсинг), или 360,000–600,000 рублей в год.

8. Внутренний специалист по информационной безопасности.Для обеспечения мониторинга и анализа можно выделить сотрудника (специалиста по безопасности), либо отдать эти функции на аутсорсинг. Внутренний сотрудник может обходиться компании примерно в 80000–150000 рублей в месяц или 960000–1800000 рублей в год.

Тогда как аутсорсинг мониторинга и анализа уязвимостей составит: 30 000 руб.х12 месяцев=360 000руб. в год.

Итого: Обслуживание, аудит информационной безопасности и поддержание соответствия стандартам безопасности-100 000 руб., аутсорсинг мониторинга и анализа уязвимостей- 360 000 руб.

Итого затраты на приобретение программного продукта StaffCop Enterprise, сертификатов и оборудования для обеспечения защиты:

1235 000+500 000+100 000+300 000+100 000+130 000+200 000+360 000=

=2 925 000 руб.

Представим расчёт всех предложенных мероприятий в таблице 3.4

И далее необходимо провести расчет эффективности предложенных мероприятий, оценить стоимости информации циркулирующей на предприятии, рассчитать стоимость ущербов от утечки информации.

Таблица 3.4 –Расчёт стоимости оборудования и мероприятий для обеспечения информационной безопасностидля ПАО «Звезда»

Категории затрат	Стоимость, руб.
1. Защитная плёнка-антишпион 2000 руб./штука для 200 рабочих мест.(2000*200=400000)	400 000
2. Сейф – огневзломостойкий европейского качества, с высоким уровнем защиты как от пожара, так и от кражи 150 000 руб. 2 штуки (150 000*2=300 000)	300 000
3. Уничтожители бумаги-шредеры -Гелеос УМ22-5 стоимостью 18000 руб. в количестве 2 штук (18000*2=36000)	36000
4. Генератор шума Соната-Р2 стоимостью 5000 руб. штука в количестве 50 штук (5000*50=250000)	250 000
5. StaffCop лицензия и годовая поддержка 6. 200х4000 руб.=800 000 руб. Годовая поддержка 150 000руб.	950 000
7. Сертификацией ФСТЭК, версии StaffCop 30% от стоимости лицензии 950000*0,3=286 500 руб.	286 500
8. Сертификация инфраструктуры -500 000 руб., ежегодные проверки на соответствие стандартам-100 000 руб.(500 000+100 000=600 000)	600 000
9. Серверное оборудование и защита данных- 300 000руб.	300 000
10. Резервное копирование и защита данных -100 000 руб.	100 000
11. VPN и контроль каналов связи- 100 000 +30 000=130 000 руб. на первый год (включая оборудование и базовое обслуживание).	130 000
12. Обслуживание, аудит информационной безопасности и поддержание соответствия стандартам безопасности-100 000 руб.	200 000
13. Аутсорсинг мониторинга и анализа уязвимостей- 360 000 руб.	360 000
Итого затраты на обеспечение информационной безопасности для первого года использования лицензии	3 912 500

Для оценки эффективности мероприятий необходимо оценить какую часть от стоимости информации циркулирующей на предприятии составляют затраты на проведение мероприятий.

Рассчитать долю от стоимости информации, циркулирующей на предприятии, возможно по формуле 3.2:

$$P=(C_з*100)\backslash C_{инф} \quad (3.2)$$

Где: Р- доля от стоимости информации, циркулирующей на предприятии;

$C_з$ -стоимость затрат на проведение мероприятий;

$C_{инф}$-стоимость информации циркулирующей на предприятии.

Р=(3 912 500*100)\ 1 097 150 000=0,35%.

Спроектированный комплекс оценивается в 3912 000 руб., что составляет 0,35% от стоимости информации (1 097150 000руб.) циркулирующей на предприятии. Это соответствует принципу разумной достаточности.

С учетом предложенных мероприятий рассчитаем их экономическую эффективность.Для начала необходимо затраты на приобретение и использование системы защиты информации соотнести с потенциальным ущербом от утечки информации.

$$Э_{эф}=У_{у\ инф}- С_з \quad (3.3)$$

Где $Э_{эф}$-Экономическая эффективность от внедрения мероприятий по защите информации;

$У_{уинф}$ -Ущерб от предполагаемой утечки информации;

$С_з$ -стоимость затрат на проведение мероприятий.

Ущербы от утечек информации имеют разные направления и последствия.

1.1Утечка информации (в т.ч. сведений, составляющих государственную тайну), приводит к остановке производства, а заброс вредоносных модификаций приводит к производственному браку. Остановка производства может быть от 3 до 60 дней. Ущерб здесь будет состоять из недополучения выручки и выплате заработной платы рабочим, т.к. простой не по вине работающих. Примем условно остановку производства один месяц. Недополучение выручки -3 040 733 000:12 месяцев=253 394 416 руб. Выплата заработной платы рабочим-84 556 866 рублей. Итого ущерб-337 951 282 руб.

1.2 Утечка информации при использовании нелицензионного оборудования и несоответствия федеральному закону № 187-ФЗ, а также приказам ФСТЭК России № 235, № 239 и другим. Согласно этим законам , предприятия -объекты КИИ обязаны перейти на отечественное ПО и сетевое оборудование. Иначе, законом предусмотрены штрафы для должностных лиц

от 10 до 50 тысяч рублей по всем нарушениямдля юридических лиц:50–100 тысяч рублей при выявлении ошибок по организации и обеспечению безопасности, нарушений по срокам предоставления информации об утвержденной категории КИИ;100–500 тысяч рублей при несоблюдении установленного порядка работы с компьютерными инцидентами, в том числе по обмену информацией, срокам и порядку передачи данных в ГосСОПКА. Итого ущерб может составить-650 000 рублей.

1.3Ущерб от утечки наукоемких данных и инженерно-технических решений и как следствие - потери конкурентоспособности. Потеря таких данных грозит не только остановкой деятельности предприятия, через утечку данных компания может потерять базу существующих и потенциальных клиентов. В краткосрочном периоде это отобразится на продажах, ведь конкуренты получат прямой выход на готовых покупать товар или услуги клиентов. А в средне- и дальнесрочных перспективах клиенты могут испытывать потребность в дополнительном утверждении безопасности данных и обратной связи от продавца.В таблице 3.5 представлен анализ основных заказчиков и конкурентов ПАО « ЗВЕЗДА»

Таблица 3.5 Анализ основных контрагентов ПАО«Звезда» в 2023г.[44]

Заказчики			Конкуренты (Список конкурентов составляется в результате анализа участия компании в тендерах и гос. закупках)		
Наименование	Количество контрактов	Сумма, тыс.руб.	Наименование	Количество контрактов	Сумма, тыс.руб.
Минпромторг России	5	1173500	ООО «Компания Энергоремонт» Выручка: 135 000 тыс.руб	53	710564, 3
ФГУП «13 СРЗ ЧФ» Минобороны России	3	164 591, 1	ООО»Дизельзипсервис» Выручка: 915 000тыс. руб.	177	1111 852, 1
ОАО «РЖД»	4	126 776, 7	ООО «РедиаПлюс»Выручка: 22 000 тыс.руб.	125	508 127
ПУ ФСБ России по Сахалинской области	9	101 825,4			

Продолжение таблицы 3.5

АО «ЦС «Звездочка»	9	79 212,2			
Другие гос.контракты	65	154 055			
Итого гос.контракты		1799960,4			

Утечки наукоемких данных и инженерно-технических решений влекут за собой потери государственных контрактов контрактов, штрафы за неисполнение сроков договоров. Контракты начнут «перетекать» к конкурентам, что ослабит конкурентную позицию и уменьшит занимаемую нишу. Ущерб можно рассчитать как риск от недополучения выручки от суммы заключенных контрактов, в среднем по отрасли он равен –10-20%.

Итого ущерб=1 799 960 421х0,1=179 996 042руб.

1.4Ущерб от утечки персональных данных. Если предположить, что у предприятия произошла утечка информации в 100 000 строк содержащей информацию о 1000 сотрудников их ФИО, номерах телефонов, e-mail. В результате утечки информации предприятие проведёт следующие действия:

а)как минимум два сотрудника отдела безопасности на протяжении 3-х днейбудут анализировать информацию об утерянных данных и пострадавших. Зарплата составит- 35 000 руб.;

б)Необходимо привлекать стороннего аудитора информационной безопасности для поиска и обнаружения источника инцидента-50 000руб.;

в)Оплатить услуги связи и телефонии для рассылки уведомлений пострадавшим об утечке персональных данных каждого, с уточнением типов утечек-30000руб.;

г)Необходимо принимать решение о проведении комплексного анализа уязвимостей ИБ с помощью уже привлеченной компании и сотрудников, а также составить политику безопасности, которая уточняет правила пресечения инцидентов в будущем-150 000руб.;

д) Принять и выплатить штраф от регулятора в размере 200 000 руб.

е)Сформировать и выплатить ущерб пострадавшим по их обращению

1000чел.х5000руб.=5000 000руб.

Итого затраты на устранение ущерба=5465 000руб.

Применение DLP-систем сводит к минимуму вероятность утечки таких данных, а значит, и экономит компании сумму возможного штрафного взыскания, которое необходимо заплатить.Рассмотрим другие затраты компании, которые можно минимизировать или вовсе предотвратить с помощью DLP-систем.

2.Организационные затраты. Это тип затрат на выявление, организацию защиты, устранение и последующее пресечение рисков информации. Как правило, сюда входят:

а) затраты на аудит бизнес-процессов и рисков информации, ранжирование их по степени значимости-450 000 руб.

б) затраты на приведение инфраструктуры предприятия в соответствие с нормами регуляторов в области ИБ, затраты на покупку, установку и техподдержку программного обеспечения и оборудования для соответствия этим нормам-3500 000 руб.

в) составление и введение в использование организационно-распорядительной документации-180 000 руб.;

г) затраты на обучение персонала компании -250 000 руб.

Итого организационные затраты – 4 380 000руб.

2. Ущерб от вирусов и хакерских атак равен стоимости восстановления и ремонта вычислительной техники, сетей и иного оборудования. В среднем на ремонт 1 ПК необходимо от 10 000 руб. На предприятии приблизительно 200ПК, тогда ущерб=10000*200=2000 000руб.

Представим потенциальный ущерб в таблице 3.6

Таблица 3.6- Потенциальный ущерб от утечек информации до внедрения мероприятий по защите информации, тыс. руб.

Наименование	Сумма, тыс. руб.
Утечка информации (в т.ч. сведений, составляющих государственную тайну), приводящая к остановке производства	337 951, 0

Продолжение таблицы 3.6

Утечка информации при использовании нелицензионного оборудования и несоответствия ФЗ № 187-ФЗ, а также приказам ФСТЭК России № 235, № 239 и другим	650, 0
Ущерб от утечки наукоемких данных и инженерно-технических решений и как следствие - потери конкурентоспособности	179 996, 0
Ущерб от утечки персональных данных	5 465, 0
Организационные затраты	4 380, 0
Ущерб от вирусов и хакерских атак, приводящий к поломкам ПК и сетей	2000, 0
Итого ущерб ($У_{уинф}$)	530 442,0

Чтобы рассчитать экономический эффект и срок окупаемости инвестиционных затрат по внедрению мероприятий СИБ от потенциальных угроз воспользуемся оценкой вероятности риска наступления данных событий. Согласно классификации рисков [10] по вероятности наступления слабовероятные события имеют вероятность до 10 процентов, маловероятные – от 10 до 40 процентов, вероятные от 40 до 60 процентов, весьма вероятные от 60 до 90 процентов. И почти возможные от 90 до 100%. Мы имеем дело с постоянно возрастающими угрозами и определим их как «весьма вероятные события « с вероятностью 65%.

$$У_{у\ инфРi}=Р_i*\ У_{у\ инф}/100 \qquad (3.4)$$

Где$У_{у\ инф\ Рi}$-это потенциальный ущерб от утечек информации до внедрения СИБ с учётом риска по вероятности наступления события

$У_{у\ инф}$-ущерб от предполагаемой утечки информации

$У_{у\ инф\ Рi}=Р_i*\ У_{у\ инф}$ /100=65*530 442 000/100=344 787 300

Преобразуем формулу 3.3 и рассчитаем экономический эффект:

$Э_{эф}=У_{у\ инф\ Рi}- С_з$=344 787 300-3 912 500= 340 874 800руб.

Как видно затраты на информационную безопасность незначительны по сравнению с потенциальным ущербом утечки информации. Они больше затратна 340 874 тысяч рублей или превышают их в 88 раз. Следовательно, предложенная система защиты информации и затраты на нее являются

разумными и целесообразными.

Рассчитаем срок окупаемости инвестиционных вложений в систему информационной безопасности

$$Т_{ок} = С_{з} / У_{у\ инф\ Pi} \quad (3.5)$$

$Т_{ок}$=3 912 500/344 787 300=0,011 года

Вариантов негативного воздействия на экономическую стабильность компании очень много, и цена конфиденциальной информации в определенных случаях даже может равняться цене всей компании. При этом стоимость DLP-систем даже для целого предприятия хоть и варьируется в зависимости от решения по продажам (лицензии и их комплектности, срокам использования), однако соизмеримо ниже, чем полная цена потери бизнеса или простой от ухода большой части клиентов. К тому же всегда существуют неизвестные риски, и с помощью комплекса правил безопасности в DLP-системе можно предупредить наступление таких рисков.

Исходя из методики расчёта экономической эффективности по потенциальному ущербу, затраты на информационную безопасность незначительны по сравнению с ущербом утечки информации. Они больше затрат на 340 874 тысяч рублей или превышают их в 88 раз. И срок окупаемости здесь еще более короткий-0,01 года. А главное правило -стоимость средств защиты не должна превышать стоимость защищаемых данных.

Все предложенные мероприятия направлены на максимальное противодействие возникающим угрозам. Утечки конфиденциальных данных являются недопустимым событием с крайне негативнымипоследствиями. За 2023 год такие угрозы увеличились в 6 раз по сравнению с 2022 годом. Внедряя данные мероприятия предприятие сможет:

1. Разделить ресурсы на конфиденциальные и не конфиденциальные;
2. Соблюдать требования регуляторов;
3. Обнаруживатьи предотвращать потенциальные угрозы;

4. Контролировать каналы передачи информации;

5. Защищать конфиденциальные данные и управлять эффективностью сотрудников на рабочем месте;

6. Предотвращать коррупцию, порчу, подделку документов;

7. Защитить нематериальные активы и объекты интеллектуальной собственности от неправомерного использования третьими лицами;

8. Заручиться поддержкой правовых институтов – суда и правоохранительных органов, в случае нарушений прав законного обладателя путем создания и предоставления доказательной базы в случае инцидентов.

Заключение

В части информационной безопасности большинство работ направлены на техническую сторону данного вопроса. Исходя из этого, а также основных параметров безопасности информации, традиционно угрозы информационной безопасности классифицируются по признакам, не имеющих взаимосвязи с экономической безопасностью. Подобный подход отрывает информационную безопасность от экономической безопасности, элементом которой она является. На основе этого вывода нами было решено определить возможные показатели информационной безопасности с точки зрения экономической безопасности предприятия.

В рамках выпускной квалификационной работы были достигнуты все поставленные перед исследованием цели, успешно решены ключевые задачи.На основании рассмотренного материала, были сформулированы выводы, в соответствии с поставленными во введении задачами.

Первая часть работы посвящена теоретическим и методическим исследованиям основ информационной безопасности предприятия.

Во второй части работы был проделан анализ финансово-хозяйственной деятельности ПАО «Звезда».Была представлена организационно-экономическая характеристика данной компании. На основании анализа были сделаны следующие выводы:ПАО «Звезда» ведёт неэффективную и нерентабельную деятельность. Компания на протяжении последних трёх лет получает убыток и находится в кризисном положении. При этом можно отметить крайне неэффективное управление себестоимостью.

Также во второй главе был проведён анализ информационных систем предприятия. Автоматизированная система ПАО Звезда основана на продуктах: InforCloudSuite Industrial (ранее ERP SyteLine) (на базе: InforCloudSuite) и ЦУП: DataCollection. Программный продукт позволяет автоматизировать управление запасами и закупками, планирование потребностей в сырье и материалах, прогнозирование производственных мощностей, обслуживание клиентов и

обработку заказов.

Документооборот в компании построен на системе NauDoc. СЭД NauDoc предназначена для автоматизации отправки и получения корреспонденции, внутренних документов организации, ведения электронного архива документов.

Бухгалтерский учёт осуществляется при помощи 1С:Предприятие (версия 8.3.). Система программ «1С:Предприятие» состоит из технологической платформы (ядра) и разработанных на ее основе прикладных решений («конфигураций»).1С:Бухгалтерия предприятия» и «1С:Управление торговлей» , «1С:275ФЗ» , «1С:Документооборот 8 КОРП».

На предприятии многие операции автоматизированы, а потому, требования информационной безопасности крайне важны.

В третьей главе был произведен анализ каналов утечки информации, который позволил локализовать все угрозы информационной безопасности. На его основе предложен расчёт стоимости оборудования и мероприятий для обеспечения информационной безопасности для ПАО «Звезда».Для анализа эффективности предложенных мероприятий была оценена стоимость циркулирующей на предприятии информации. И далее эту стоимость сопоставили с затратами на проведение мероприятий. Для полноты картины был определен и рассчитан потенциальный ущерб от утечек информации до внедрения мероприятий по защите информации.

Исходя из методики расчёта экономической эффективности по потенциальному ущербу, затраты на информационную безопасность незначительны по сравнению с ущербом утечки информации. Они больше затрат на 340 874 тысяч рублей или превышают их в 88 раз. И срок окупаемости здесь еще более короткий-0,01 года. А главное правило -стоимость средств защиты не должна превышать стоимость защищаемых данных.

Вариантов негативного воздействия на экономическую стабильность компании очень много, и цена конфиденциальной информации в определенных случаях даже может равняться цене всей компании. При этом стоимость DLP-

систем (одного из предложенного мероприятия) даже для целого предприятия хоть и варьируется в зависимости от решения по продажам (лицензии и их комплектности, срокам использования), однако соизмеримо ниже, чем полная цена потери бизнеса или простой от ухода большой части клиентов. К тому же всегда существуют неизвестные риски, и с помощью комплекса правил безопасности в DLP-системе можно предупредить наступление таких рисков

Таким образом, данное исследование является актуальным и важным в свете того, что информационные технологии и цифровые платформы, используемые на предприятиях, продолжают развиваться и стали неотъемлемой частью бизнеса. В настоящее время, особенно после значительного увеличения количества переходов к удаленной работе, информационная безопасность стала ещё более важной и неотъемлемой частью экономической безопасности предприятия.

Цели выпускной квалификационной работы достигнуты, задачи решены.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, N 31 (1 ч.), ст. 3448. [Электронный ресурс]. URL: consultant.ru›document/cons_doc_LAW_61798/ (дата обращения: 11.11.2024)

2. Указ Президента РФ от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации». В соответствии с федеральными законами от 28 декабря 2010 г. N 390-ФЗ «О безопасности» и от 28 июня 2014 г.. Электрон, дан. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 11.11.2024)

3. Баланов, А. Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие.- М.: Инфра-Инженерия, 2024.- 156 с.

4. Барков, А.В., Киселев, А.С. Влияние цифровизации на правовое обеспечение информационной безопасности государства и бизнеса в условиях современных геополитических вызовов // Безопасность бизнеса. -2022.-№ 3. - С. 3 — 7.

5. Барков, А.В., Киселев, А.С. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур // Банковское право.- 2022. -№ 4.- С. 20 — 27.

6. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем.- М.: МГТУ им. Н. Э. Баумана, 2024.- 252 с.

7. Васильева, Т. Ю., Куприянов, А. И., Мельников, В. П. Информационная безопасность: учеб. - М.: КноРус, 2023. -372 с.

8. Галыгина Л. В., Галыгина И. В. Социальные аспекты информационной безопасности. Лабораторный практикум. М.: Лань. 2021. 64 с.

9. Герасименко, А.В. Финансовая отчётность для руководителей и начинающих специалистов: практическое пособие / А.В. Герасименко; ред. М.

Савина. – 5-е изд. – М.: Альпина Паблишер, 2016. – 432 с.

10. Грачев, С.А., Гундорова, М. А Оценка и управление рисками : учеб. пособие / Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Изд. 2-е., испр. и доп. – Владимир :Изд во ВлГУ, 2022. -144 с.

11. Дубень, А.К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению // Международное право и международные организации. -2022. -№ 1.- С. 24 — 30.

12. Дугенец, А.С., Павлова, Л.В. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России // Административное право и процесс. -2023. -№ 5. -С. 22 — 25.

13. Еремин, А. Л. Информационная и цифровая гигиена. -М.: Лань, 2023. -92 с.

14. Жарова, А.К. Защита информации ограниченного доступа, получаемой по цифровым каналам передачи информации о совершаемых коррупционных правонарушениях // Государственная власть и местное самоуправление. -2023.-№ 9. -С. 37 — 41.

15. Зенков, А. В. Информационная безопасность и защита информации. М.: Юрайт, 2023.- 108 с.

16. Зиборов, О.В., Кардашевская, М. В, Березина М.Г. Административная деятельность полиции // Московский университет МВД России им. В.Я. Кикотя. – 3-е изд., перераб. и доп. – Москва: Юнити, 2021. – с.22

17. Казарин, О. В., Шубинский, И. Б. Основы информационной безопасности: надежность и безопасность программного обеспечения. - М.: Юрайт, 2023. - 343 с.

18. Корабельников, С. М. Преступления в сфере информационной безопасности. -М.: Юрайт, 2024. - 112 с.

19. Куприянов А. И., Мельников В. П. Информационная безопасность:

учеб. - М.: КноРус, 2022. - 268 с.

20. Максуров, А. А. Обеспечение информационной безопасности в сети Интернет. Монография. - М.: Инфра-М, 2023. - 226 с.

21. Малолетко, А.Н. Концепция экономической безопасности развития системы высшего образования России: диссертация ... доктора экономических наук: 08.00.05 / Малолетко Александр Николаевич; [Место защиты: Моск. ун-т МВД РФ]. – Москва, 2009. – 327 с

22. Мирошников, А. И. Основы информационной безопасности и защита информации: учеб. пособие / А. И. Мирошников, А. С. Сысоев. — Липецк: Липецкий ГТУ, 2022. – 107 с

23. Нестеров, С. А. Основы информационной безопасности.- М.: Лань, 2023. - 324 с.

24. Осавелюк, Е. А. Информационная безопасность государства и общества в контексте деятельности СМИ. Монография. - М.: Лань, 2023. - 92 с.

25. Полякова, Т.А., Смирнов, А.А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Российский юридический журнал. -2022. - № 3.- С. 7 — 15.

26. Прохорова, О. В. Информационная безопасность и защита информации.- М.: Лань, 2024. -124 с.

27. Родичев, Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации. -СПб.: Питер, 2023. - 384 с.

28. Савин, В.А. Некоторые аспекты экономической безопасности России / В.А. Савин // Международный бизнес России. - 1995.- № 9. - С. 14.

29. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации.- М.: Директмедиа Паблишинг, 2022.- 128 с.

30. Смирных, С.Е. Международная информационная безопасность как гарантия осуществления права народов на самоопределение // Международное право и международные организации. -2022. -№ 2. -С. 20 — 30.

31. Соколов, А.Ю., Солдаткина О.Л. Разработка регионального

модельного нормативного акта о правовом информировании как направление правовой политики в сфере информационной безопасности // Вестник Пермского университета. Юридические науки. -2023. -№ 4. -С. 602 — 612.

32. Суворова, Г. М. Информационная безопасность. - М.: Юрайт, 2023.- 278 с.

33. Сычев, Ю. Н. Защита информации и информационная безопасность: учеб. пособие. -М.: Инфра-М, 2023.- 201 с.

34. Тамбовцев, В.Л. Экономическая безопасность хозяйственных систем: структура, проблемы / В.Л. Тамбовцев // Вестник МГУ. — 1995. – №3. — С. 37-42.

35. Ясенев, В.Н Информационная безопасность: учеб. пособие // Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. -213с

36. Роскомнадзор привёл статистику борьбы с киберугрозами в Рунете за 2023 год. // d-russia.ru: электронный журнал. [Электронный ресурс]. URL: https://d-russia.ru/roskomnadzor-privjol-statistiku-borby-s-kiberugrozami-v-runete-za-2023-god.html?ysclid=m37biiklc5420315220 (дата обращения: 20.10.2024).

37. В 2023 году 60% промышленных предприятий столкнулись с утечкой информации // «СёрчИнформ» : электронный журнал. [Электронный ресурс]. URL: https://searchinform.ru/news/company-news/2023/12/22/in-2023-60-of-industrial-enterprises-faced-information-leakage/?ysclid= m37ayx3jo72687 85748 (дата обращения: 20.10.2024).

38. Перечень лицензий и сертификатов // Официальный сайт Прайм Раскрытие. [Электронный ресурс] URL: http://www.zvezda.spb.ru/index.php/o-predpriyatii (дата обращения: 15.1 1.2024)

39. Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 N 51-ФЗ (ред. от 16.04.2022) // КонсультантПлюс. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 15.11.2024)

40. Федеральный закон от 26.12.1995 N 208-ФЗ (ред. от 07.10.2022, с

изм. от 19.12.2022) «Об акционерных обществах» (с изм. и доп., вступ. в силу с 01.01.2023) // КонсультантПлюс. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_8743/ (дата обращения: 15.11.2024)

41. Федеральный закон от 22.04.1996 N 39-ФЗ (ред. от 20.10.2022, с изм. от 19.12.2022) «О рынке ценных бумаг» // КонсультантПлюс. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_10148/ (дата обращения: 15.11.2024)

42. Федеральный закон Российской Федерации от 21 июля 1993 года № 5485-I «О государственной тайне» (Российская газета, 1993, 21 сентября; Собрание законодательства Российской Федерации, 1997, № 41, Федеральный закон от 04.08.2023 г. № 432-ФЗ • Президент России. [Электронный ресурс] URL: http://www.kremlin.ru/acts/bank/49712/page/1 (дата обращения 12.12.2024)

43. Контур Staffcop: электронный журнал. [Электронный ресурс]. URL: https://www.staffcop.ru/?ysclid=m3hondoeqm33314089 (дата обращения 10.11.2024)

44. Публичное акционерное общество «ЗВЕЗДА» Финансовая отчетность в соответствии с Международными стандартами финансовой отчетности и Аудиторское заключение независимого аудитора 31 декабря 2023 года [Электронный ресурс]. URL:https://cdn.financemarker.ru/reports/2023/MOEX/Z/ZVEZ_ 2023_12_Y_%D0%9C%D0%A1%D0%A4%D0%9E.pdf (дата обращения 15.12.2024)

Приложение 1

Вызовы и угрозы экономической безопасности

1) стремление развитых государств использовать свои преимущества в уровне развития экономики, высоких технологий (в том числе информационных) в качестве инструмента глобальной конкуренции;

2) усиление структурных дисбалансов в мировой экономике и финансовой системе, рост частной и суверенной задолженности, увеличение разрыва между стоимостной оценкой реальных активов и производных ценных бумаг;

3) использование дискриминационных мер в отношении ключевых секторов экономики Российской Федерации, ограничение доступа к иностранным финансовым ресурсам и современным технологиям;

4) повышение конфликтного потенциала в зонах экономических интересов Российской Федерации, а также вблизи ее границ;

5) усиление колебаний конъюнктуры мировых товарных и финансовых рынков;

6) изменение структуры мирового спроса на энергоресурсы и структуры их потребления, развитие энергосберегающих технологий и снижение материалоемкости, развитие «зеленых технологий»;

7) деятельность создаваемых без участия Российской Федерации межгосударственных экономических объединений в сфере регулирования торгово-экономических и финансово-инвестиционных отношений, которая может нанести ущерб национальным интересам Российской Федерации;

8) подверженность финансовой системы Российской Федерации глобальным рискам (в том числе в результате влияния спекулятивного иностранного капитала), а также уязвимость информационной инфраструктуры финансово-банковской системы;

9) исчерпание экспортно-сырьевой модели экономического развития, резкое снижение роли традиционных факторов обеспечения экономического роста, связанное с научно-технологическими изменениями;

10) отсутствие российских несырьевых компаний среди глобальных лидеров мировой экономики;

11) недостаточный объем инвестиций в реальный сектор экономики, обусловленный неблагоприятным инвестиционным климатом, высокими издержками бизнеса, избыточными административными барьерами, неэффективной защитой права собственности;

12) слабая инновационная активность, отставание в области разработки и внедрения новых и перспективных технологий (в том числе технологий цифровой экономики), недостаточный уровень квалификации и ключевых компетенций отечественных специалистов;

13) истощение ресурсной базы топливно-сырьевых отраслей по мере исчерпания действующих месторождений;

14) ограниченность масштабов российского несырьевого экспорта, связанная с его низкой конкурентоспособностью, недостаточно развитой рыночной инфраструктурой и слабой вовлеченностью в мировые «цепочки» создания добавленной стоимости;

15) низкие темпы экономического роста, обусловленные внутренними причинами, в том числе ограниченностью доступа к долгосрочным финансовым ресурсам, недостаточным развитием транспортной и энергетической инфраструктуры;

16) несбалансированность национальной бюджетной системы;

17) недостаточно эффективное государственное управление;

18) высокий уровень криминализации и коррупции в экономической сфере;

19) сохранение значительной доли теневой экономики;

20) усиление дифференциации населения по уровню доходов;

21) снижение качества и доступности образования, медицинской помощи и, как следствие, снижение качества человеческого потенциала;

Продолжение приложения 1

22) усиление международной конкуренции за кадры высшей квалификации;

23) недостаточность трудовых ресурсов;

24) неравномерность пространственного развития Российской Федерации, усиление дифференциации регионов и муниципальных образований по уровню и темпам социально-экономического развития;

25) установление избыточных требований в области экологической безопасности, рост затрат на обеспечение экологических стандартов производства и потребления.

Приложение 2

Нормативно-правовые акты в области защиты информации

Правовой документ	Пояснения
Конституция Российской Федерации» 12.12.1993, Статья 23. 1	«Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»
Указ Президента Российской Федерации от 05.12.2016 г. № 646 Об утверждении Доктрины информационной безопасности Российской Федерации	Реализация положений новой Доктрины информационной безопасности призвана не только защитить информационную инфраструктуру РФ от посягательств, на бизнес и граждан от ущемления их интересов, но и усилить влияние России на геополитические процессы на основе норм международного права
Закон РФ №5485-I от 21.07.1993г. «О государственной тайне» (в ред. Федерального закона от 06.10.1997 N 131-ФЗ	Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.
№ 149 - ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006	Определяет ключевые термины в области информации. Поясняет что такое конфиденциальная информация, сайт, электронное сообщение, поисковая система, обмен данными. Необходим при составление нормативной документации по информационной безопасности в организациях.
Федеральный закон РФ № 152-ФЗ «О персональных данных». вступил в силу 26.01.2007	Закон регулирует работу с персональными данными — личными данными конкретных людей. Его обязаны соблюдать те, кто собирает и хранит эти данные. Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца, держать их в секрете, защищать от посторонних, удалить по требованию
Федеральный закон РФ № 98-ФЗ «О коммерческой тайне» от 29.07.2004	Закон определяет, что такое коммерческая тайна, как ее охранять и что будет, если передать ее посторонним. В нем сказано, что коммерческой тайной считается информация, которая помогает компании увеличить доходы, избежать расходов или получить любую коммерческую выгоду.

Продолжение приложения 2

Федеральный закон РФ № 63-ФЗ «Об электронной подписи» от 06.04.2011	Закон поясняет и определяет все что касается электронной подписи — цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки. Закон определяет, что такое электронная подпись, какую юридическую силу она имеет и в каких сферах ее можно использовать.
Федеральный закон РФ №187-ФЗ «О безопасности критической информационной инфраструктуры РФ»	Этот закон касается компаний, которые работают в сферах, критически важных для жизни государства — таких, что сбой в их работе отразится на здоровье, безопасности и комфорте граждан России. Описывает правила защиты IT-инфраструктуры на предприятиях, работающих в сферах, критически важных для государства. К таким сферам относится здравоохранение, наука, оборона, связь, транспорт, энергетика, банки и некоторая промышленность
Приказ ФСТЭК России № 31 от 14.03.2014»Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».	предприятия ОПК обязаны защищать информацию, обработка которой осуществляется АСУ ТП на критически важных объектах

Приложение 3

Анализ существующих угроз для ПАО «Звезда»

Виды угроз	Типы угроз и атак	Методы НДС	Меры противодействия
1.Естественные угрозы	Пожар		оборудование помещений противопожарными датчиками и средствами пожаротушения, назначение специалистов ответственный за противопожарную безопасность.
2.Исусственные	Непреднамеренные	Установка программ на компьютер не входящих в список необходимых для работы, использование личных накопителей информации на рабочем месте и потеря их в транспорте, неготовность пользователей к фишинговым атакам использование незащищенных беспроводных сетей, открытые USB-порты и возможность бесконтрольного использования съемных носителей;наличие устаревших версий компонентов, отключение защиты, ошибки пользователей	Использование только специализированных программ и флэшкарт на рабочем компьютере, Запрет передачи информации и копирования. Резервное копирование.DLP -системы - для предотвращения утечки конфиденциальных материалов, Siem -системы для централизованного мониторинга информационной безопасности, сбора и анализа данных от инструментов кибербезопасности. Организация безопасного удаленного доступа к сети и создания зашифрованного канала связи с помощью средств криптографической защита информации (СКЗИ) и VPN
	Преднамеренные внутренние	Недовольные сотрудники Установка программ на компьютер не входящих в список необходимых для работы	инструкции по обращению с техникой, системами, где обрабатывается конфиденциальная информация криптозащиты: шифрование файлов,разграничение доступа
	Преднамеренные Внешние: -DDoS-атака,	— DDoS-атака. Это виртуальная атака на ресурсы компании, которая приводит к замедлению или полному прекращению их работы. -	
	Вирусы	Они проникают на	Антивирусы, сетевая защита

		компьютер, ставят шпионское ПО, которое пересылает файлы с корпоративных систем третьим лицам;выводят из строя жесткий диск;стираютданные;шифруют файлы на диске и требуют за них выкуп	
	Спам	комплекс настроек, различные средства для фильтрации нежелательных сообщений, например, «белые» и «черные» списки, списки адресов, авторитетные почты и соответствующие ключевые слова	
	Утечки информации при обмене и передачи информации по открытой сети	Утечка инженерно-технических средств, данных автоматизированных систем. В результате -остановка производства	виртуальные частные сети (VPN), двухфакторная аутентификация пользователя. При входе в программу, личный кабинет или веб-сервис система требует указывать логин, пароль и код из смс
	Попытки взлома компьютерных систем	на уровне сетевого программного обеспечения, баз данных и операционной системы	
	Радиоэлектронные каналы утечки информации	такие информационные каналы, которые возникают за счет широкого вида побочных электромагнитных излучений и наводок (ПЭМИН	блокируется с помощью использования специальных устройств за щиты - генераторов шума
	Акусти-ческие	неконтролируемое распространение звуковых волн в звукопроводящих средах	Через дверь кабинетов-установка доводчиков дверей
	Оптические	от носятся компьютерные мониторы, информация на бумажных носителях, графи ческие изображения и схемы, а так же изображения отраженные в зеркалах и глянцевых поверхностях.	Через окно-установка жалюзи, защитная пленка на экран компьютера, которая уменьшает угол обзора до 60 градусов.
	Материально-вещественные	Неправильно утилизируется документация на бумажных и электронных носителях, кража ценных вещей и документов	и требуется приобрести уничтожители бумаги-шредеры и приобретение сейфов в кабинеты