Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»
Институт Высшая школа экономики и менеджмента
Кафедра экономики и управления на металлургических и машиностроительных предприятиях

Допустить к защите

Зав. кафедрой, профессор, д.э.н.

_____Н.Р. Кельчевская

«___» _____ 2017 г.

Управление рисками при внедрении информационных технологий на промышленных предприятиях

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Направление подготовки **38.04.02 – Менеджмент**
Магистерская программа «Управление бизнес-процессами в промышленности»

Научный руководитель _____ Кельчевская Н.Р.
д.э.н., профессор

Нормоконтроль _____ Черненко И.М.
к.э.н., доцент

Магистрант группы _____ Криницын К.А.
ЭММ-250204

Екатеринбург
2017

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность работы. В век информатизации автоматизация бизнес-процессов предприятия, использование различных информационных сервисов для обработки информации – это залог эффективности и конкурентоспособности на рынке.

Управленцы различных уровней постоянно сталкивается с проблемой получения достоверной информации о ситуации на подконтрольном участке предприятия. Внедрение различных информационных систем на предприятии позволяет решить вопросы полноты, достоверности и конфиденциальности получаемой информации.

Использование таких систем на предприятии сопровождается усложнением задач по управлению информационной средой. Наиболее важными из них являются рациональное использование инвестиций и минимизация появляющихся рисков, связанных с информационными процессами на предприятии.

Управление рисками нарушения информационной целостности является основной задачей информационной безопасности компании, а ее обеспечение главным критерием качества выполнения информационных процессов в частности и информационной инфраструктурой предприятия в целом.

Проблематика управления рисками достаточно полно описана международными стандартами и специальной литературой. Но при этом отсутствует конкретная методика управления информационными рисками на предприятии, которая бы предоставила конкретный инструмент для менеджеров различных уровней на основе взаимосвязанных методов, моделей и алгоритмов для достижения конкретных результатов по управлению информационными рисками.

Отсутствие комплексного подхода не позволяет правильно установить взаимосвязи информационных рисков и экономических показателей, что, в свою очередь, ведет к падению эффективности предприятия.

Степень разработанности проблемы. Существует ряд международных и российских стандартов как по информационной безопасности в целом так и управлению информационными рисками в частности, которые описывают информационные риски как со стороны информационных технологий так и со стороны менеджмента.

Главный международных стандартов управления информационной безопасностью – стандарт BS 7799 . Этот документ является практическим руководством по управлению информационной безопасностью в организации. В нем описано 10 областей и 127 механизмов контроля, необходимых для построения систем управления информационной безопасностью, определенных на основе лучших примеров из мировой практики [1].

В стандартах серии ISO 27000 определено все, что касается управления информационными рисками. Прежде всего это стандарт ISO/IEC 27005:2008, и BS 7799-3:2006. Они являются основой для методологии управления рисками и применяются повсеместно. В них описаны практические правила управления информационной безопасностью и во многих вопросах эти стандарты дополняют друг друга [3].

В работах многих ученых, таких как Мескон М., Альберт М., Хедоури Ф., Круи М., Галай Д., Марк Р. и др. разработаны общие принципы управления экономическими рисками, проведен анализ, классификация рисков по различным критериям, их систематизация, а также даются научно-методические и практические рекомендации по управлению рисками в различных областях экономики [4,5,6].

В разное время риск изучался как аспект игры (например, у Б.Паскаля, Х. Гюйгенса), элемент задачи оценки в страховании (например, у Д. Бернулли). Были введены функции полезности, как количественно (у того же

Д. Бернулли, Г. Госсена, и позднее у Дж. фон Неймана и О. Моргенштерна), так и качественно (например, в работах В. Парето) описывавшие выбор определенного решения. Как и начальные работы, большинство из них основано на понятии риска и связанных с ним характеристиках системы [7].

В то же время использование системного подхода позволяет разбить сложную проблему по управлению рисками на множество целей, со своими критериями эффективности системы. Данный подход позволяет построить множество отдельных, более эффективных стратегий, что в конечном счете, будет влиять на скорость и качество принимаемых решений по управлению рисками.

Вместе с тем информационные риски как разновидность экономических рисков рассматриваются лишь в работах отдельных ученых. Результатом такого подхода является недооценка важности управления информационными рисками и экономических методов управления информационными рисками.

Целью данной работы является исследование информационных рисков, разработка методического подхода к управлению информационными рисками на предприятиях.

Для достижения этой цели поставлены следующие задачи:

- изучить и исследовать понятийный аппарат информационных рисков, классифицировать информационные риски;

- изучить и влияние информационных рисков на деятельность промышленных предприятий;

- разработать методический подход по управлению информационными рисками на предприятиях.

Объектом исследования являются промышленные предприятия, на которых применяются информационные технологии или есть необходимость в их использовании для автоматизации бизнес-процессов.

Предметом исследования является организационно-экономические отношения возникающие при управлении информационными рисками на промышленных предприятиях.

Структура и объем работы. Магистерская работа состоит из введения, трех глав, заключения, списка литературы и 54 источников. Основное содержание изложено на 107 страницах, работа включает 12 таблиц, 12 рисунков и 2 приложения.

Основное содержание работы. В первой главе «Сущность информационных рисков» определены основные понятия, связанные с управлением рисками, информационными технологиями, оценкой рисков. Описана классификация информационных рисков по различным критериям, рассмотрены общепринятые принятые методы анализа и управления рисками.

Во второй главе «Роль информационных рисков в деятельности промышленных предприятий» проведен анализ тенденций развития информационных технологий на промышленных предприятиях, проведен анализ использования систем управления рисками на промышленных предприятиях. Так же в этой главе проведен анализ влияний информационных рисков на деятельность промышленных предприятий на примере ООО «ВИЗ-Сталь».

В третьей главе определено понятие систему управления информационными рисками (СУИР) и предложено использовать ее в деятельности как основного элемента по минимизации влияния информационных рисков. Ключевым элементом для этой системы стала разработанная классификация информационных рисков.

Основные научные результаты и новизна:

- Предложен подход к управлению информационными рисками, основанный на использовании правовых норм, организационных мероприятий, технических, программных и человеческих ресурсов

предприятия для обеспечения противодействия информационным рискам и компенсации ущерба от их наступления;

- Разработана методика анализа информационных рисков, в основу которой положена классификация информационных рисков, включающая специфические для них признаки, такие как аспект информационной безопасности, характер угрозы информационного актива, механизм воздействия на информационную среду, позволяющая идентифицировать риски, и проводить дальнейшее исследование по их влиянию на деятельность промышленных предприятий.

1 ИНФОРМАЦИОННЫЕ РИСКИ: СУЩНОСТЬ, КЛАССИФИКАЦИЯ, МЕТОДЫ АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ

На современном уровне развития автоматизация процессов представляет собой один из подходов к управлению процессами на основе применения информационных технологий. За счет использования программных и аппаратных ресурсов этот подход позволяет минимизировать участие человека и управлять операциями, данными, информацией и ресурсами.

Основной целью автоматизации является повышение качества и скорости выполнения бизнес-процессов на предприятии. Автоматизированный процесс обладает более стабильными характеристиками, чем процесс, выполняемый в ручном режиме. Во многих случаях автоматизация процессов позволяет повысить производительность, сократить время выполнения процесса, снизить стоимость, увеличить точность и стабильность выполняемых операций.

Но при принятии решения об автоматизации перед руководителем предприятия стоит очень важный вопрос – оценка рисков, возникающий в процессе внедрения и использования информационных технологий в бизнес-процессах предприятия. Для сокращения негативных последствий от наступления рисков, необходимо уметь правильно и эффективно управлять рисками [8].

Управление риском - процесс принятия и выполнения управленческих решений, направленных на снижение вероятности возникновения неблагоприятного результата и минимизацию возможных потерь, вызванных его реализацией [9].

Особой разновидностью рисков при автоматизации бизнес процессов и использовании информационных технологий являются информационные риски.

Информационные технологии (ИТ, также – информационно-коммуникационные технологии) – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [10].

Информационный риск (IT-риск) – это опасность возникновения убытков или ущерба в результате обработки, хранении и передачи информации с помощью автоматизированных информационных систем а так же сбоев в работе этих систем.

IT-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи.

Под автоматизированной информационной системой понимается совокупность программно-аппаратных средств, предназначенных для автоматизации деятельности, связанной с хранением, обработкой и передачей информации.

1.1 СУЩНОСТЬ ИНФОРМАЦИОННЫХ РИСКОВ

Основными определяющим источником появления информационных рисков является информационный актив, к которым относится любая информация, представляющая ценность для организации. К ней относится информация напечатанная или записанная на бумажном носителе, пересылаемая по почте или демонстрируемая в видеозаписях, передаваемую устно, информация, хранимая в электронном виде на серверах баз данных, вебсайтах, мобильных устройствах, электронных носителях, информация, обрабатываемую в корпоративных информационных системах (КИС) и передаваемая по каналам передач данных, а также программное обеспечение: операционные системы, приложения, программную документацию и т.п.

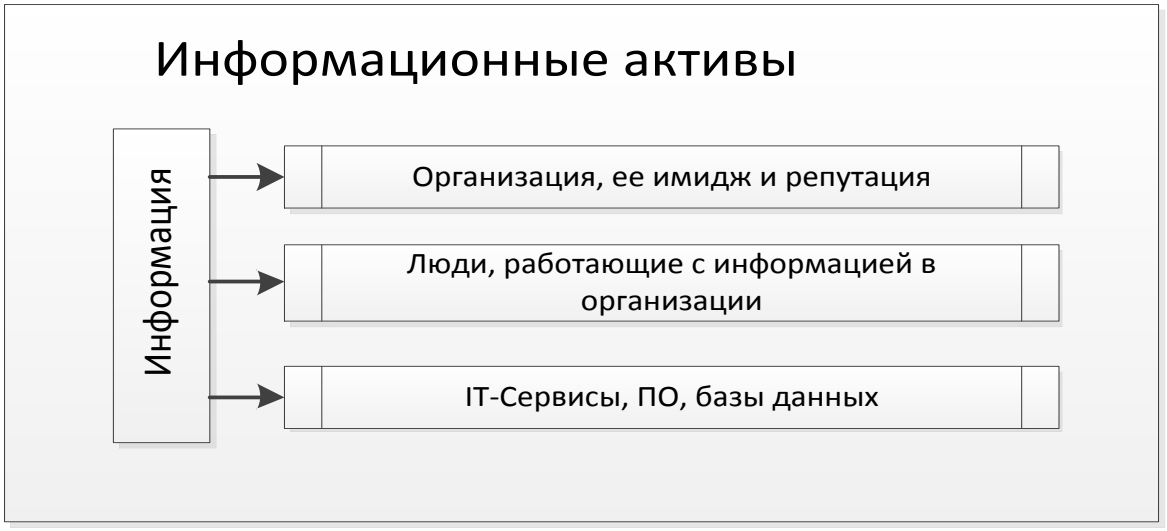

Рисунок 1 – Влияние информационных активов

Кроме информации у организации так же есть и другие виды материальных и нематериальных активов, которые она использует для своего функционирования. Это имущество организации, имущественные и неимущественные права, интеллектуальная собственность, кадровые ресурсы, а также имидж и репутация организации. Современные международные стандарты также определяют еще одну категорию активов – это процессы, а также информационные и неинформационные сервисы. Это агрегированные типы активов, которые оперируют другими активами для достижения бизнес-целей.

Виды активов организации:

- материальные;
- финансовые;
- имущественные и неимущественные права;
- интеллектуальная собственность;
- кадровые;
- информационные;
- процессы и сервисы;
- имидж и репутация.

Множество всех активов в организации можно условно разделить на *основные и вспомогательные активы*. Вокруг основных активов построены основные бизнес-процессы организации, а вспомогательные выполняют второстепенную роль. При использовании или внедрении информационных технологий на предприятия информационные активы выступают как основные, т.к. все технические, экономические, финансовые инструменты предприятия опираются на работоспособность информационных сервисов на предприятии.

Между всеми видами активов существует взаимосвязь. Успешная реализация угроз в отношении одного вида активов может привести к нарушению безопасности других. Например, незаконное проникновение в помещение с оборудованием, например, серверной, может привести к возможности несанкционированного доступа с хранимой на серверах информации, которую злоумышленники могут использовать в своих корыстных целях. В дальнейшем эти действия могут привести к падению имиджа и репутации компании на рынке. Или выход из строя серверного оборудования влияет на доступность хранящихся на нем приложений, сервисов и информации, а для восстановления доступа необходимо выделить кадровые, материальные и финансовые ресурсы.

Работа по минимизации IT-рисков заключается в предупреждении несанкционированного доступа к активам, аварий и сбоев оборудования, обеспечении доступности необходимых для работы сервисов и приложений. Процесс минимизации IT-рисков следует рассматривать комплексно: сначала выявляются возможные проблемы, а затем определяется, какими способами их можно решить или предупредить [11].

Целью управления информационными рисками является минимизация суммы расходов предприятия на противодействие информационным рискам и суммарного ущерба от этих рисков.

Основной сложностью при управлении риска при автоматизации является его оценка.

Оценка рисков – это определение количественным или качественным способом величины (степени) рисков.

Известный американский эксперт в области управления рисками Б. Берлимер предложил при анализе оценки рисков использовать следующие допущения [12]:

- потери от риска независимы друг от друга;
- вероятность потери по одному направлению деятельности не обязательно увеличивает вероятность потери по-другому (за исключением форс-мажорных обстоятельств);
- максимально возможный ущерб от негативного эффекта при наступлении риска не должен превышать финансовых возможностей организации.

1.2 КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ РИСКОВ

Не смотря на значительное количество различных классификаций угроз в области информационной безопасности, в изученной литературе отсутствует установленная классификация информационных рисков. Они рассматриваются как один из видов операционных рисков предприятия.

Как правило, все виды информационных рисков взаимосвязаны и оказывают влияния на деятельность предприятия. При этом изменение одного вида риска может вызывать изменение большинства остальных.

Классификация рисков означает объединение совокупности рисков на основании определенных признаков и критериев. Такими критериями, положенными в основу классификации информационных рисков, могут являются:

- основные аспекты информационной безопасности;
- время возникновения;
- источник возникновения;
- природа информационного актива;
- природа информационного актива;

- характер угрозы информационной безопасности;
- характер последствий;
- механизм воздействия.

Основными аспектами информационной безопасности являются: доступность, целостность и конфиденциальность информации.

Под доступностью понимается возможность доступа субъекта к данным по запросу в любое предусмотренное расписанием работы время. Возможность получения данных по запросу зависит от работоспособности и загруженности элементов информационной системы и ее каналов передачи данных.

Риск нарушения доступности информации может зависеть как от неисправности оборудования и сбоев в программном обеспечении в компании, так и от успешно реализованных сетевых атак на информационную систему из вне.

Данный тип риска напрямую зависит от надежности аппаратных и программных компонентов информационной системы, а так же от уровня компетенций персонала, управляющего их работой. Нарушение доступности так же возникают из-за несоблюдения требований различных стандартов как на этапе проектирования так и на этапах производства или эксплуатации системы.

Под целостностью понимается актуальность и непротиворечивость информации, уровень ее защиты от разрушения и несанкционированного изменения и удаления.

Риск нарушения целостности обеспечивается вероятностями отказа оборудования и программного обеспечения, степенью продуманности алгоритмов и надежностью средств доступа пользователей системы, имеющих право на редактирование информации, вероятностью наличия в системе недокументированных возможностей, несовершенством организационной структуры ИС, а так же несоблюдением требований стандартов на этапе проектирования, производства и эксплуатации системы.

Под конфиденциальностью понимается уровень защиты информации от несанкционированного доступа.

Риск нарушения конфиденциальности так же зависит от уровня алгоритмов аутентификации пользователей, вероятностью наличия недокументированных ситуаций при работе с ИС, несовершенством организационной структуры, несоблюдением стандартов и человеческим фактором [13].

По времени возникновения информационные риски распределяются на *ретроспективные, текущие и перспективные риски*. Анализ ретроспективных рисков, их характера и методов их минимизации позволяет точнее прогнозировать текущие и перспективные риски.

По среде возникновения риски делятся на внешние и внутренние.

На внешние риски не влияет внутренняя составляющая предприятия, они не связаны с прямой деятельностью предприятия и никак не может повлиять на их уровень. Их уровень обусловлен политической обстановкой в стране и между государствами, экономической ситуацией на рынке, социальным уровнем граждан и т.д.

К внутренним информационным рискам относятся риски, зависящие от непосредственной деятельности предприятия и его персонала. На их уровень могут влиять следующие факторы: производственный потенциал организации, уровень технического оснащения, степень квалификации персонала, наличие средств защиты информации, наличие должностных инструкций при работе с ИС [14].

По природе информационного актива информационные риски можно разделить на риски аппаратные и программные.

Аппаратные риски возникают при выходе из стоя комплексов ИС, таких как: серверы, персональные компьютеры, сетевые коммутаторы и маршрутизаторы, производственное оборудование, станки и т.д. *Программные риски* непосредственно связаны со сбоями в работе программного обеспечения предприятия, действия вредоносного

программного обеспечения, операционных систем пользователей ИС, а так же связанные с утечкой информации и действия сетевых атак. Формируя классификацию, связанную с характером угрозы информационной безопасности, можно выделить следующие риски:

Организационные риски – это риски, связанные деятельностью персонала, эксплуатирующего и обслуживающего ИС, проблемами системы внутреннего контроля, плохо разработанными правилами работ, то есть риски, связанные с внутренней организацией работы компании.

Технические риски связаны с оборудованием, программным обеспечением, их задачами, способами проектирования, разработки и эксплуатации ИС. Эти риски напрямую связаны с жизненным циклом ИС.

К природным информационным рискам относятся риски, которые не зависят от деятельности человека. Они способны нанести ущерб, который можем привести к полной остановке функционирования предприятия. Они связаны с деятельностью природных явлений, таких как землетрясения, наводнения, штормы, ураганы, и т.д.

Помимо вышеприведенных классификаций, риски можно классифицировать по характеру последствий.

Допустимый риск - это риск, при наступлении которого, организации понесут потери, не превышающие величину ожидаемой прибыли от деятельности предприятия и его деятельность продолжает быть целесообразной.

Критический риск – это риск, в результате наступления которого, предприятию грозят потери, превышающие предполагаемую прибыль от деятельности предприятия и могут привести к потере всех средств, вложенных в реализацию проекта.

Если ущерб наступления риска предприятие превышает его прибыль от прямой деятельности или превышают имущественное состояние предприятия, то такие риски называют *катастрофическими.* К ним так же относят риски, связанные с опасностью для жизни и здоровья людей или

возникновением экологических катастроф, а так же риски, ущерб от которых наносит промышленному предприятию непоправимый вред.

Механизм воздействия составляет самую большую классификационную группу информационных рисков. По этому признаку информационные риски можно разделить на:

- Ошибки специалистов
- Сбои и отказы технических средств
- Сбои и отказы сетевого оборудования
- Сбои и отказы программных средств
- Вредоносное ПО
- Шпионские программы
- Несанкционированный доступ
- Нарушение авторских прав
- Распространение ложной информации
- Аварии

Схематическая классификация информационных рисков по различным критериям приведена на рисунке 2.

1.3 МЕТОДЫ АНАЛИЗА РИСКОВ

Ф. Найт впервые упомянул о риске как количественной мере неопределенности появилось в своим труде «Риск, неопределённость и прибыль». Он определил риск как «измеримую неопределенность», «вероятностную (стохастическую) определенность». Так же им установлена взаимосвязь понятий «неопределенность» и «риск» и дана вероятностно-математическая трактовка риска [5].

Анализ рисков можно подразделить на два взаимно дополняющих друг друга вида: *качественный и количественный.*

Специфической особенностью качественного подхода в исследовании рисков является первостепенная идентификация рисков проекта, на основании которой выявляются все возможные риски, с которыми может столкнуться организация. Следующим этапом качественного анализа

является стоимостная оценка последствий от наступлений таких рисков и методы борьбы с ними. Проведение качественного анализа должно проводиться на стадии планирования деятельности предприятия. Количественный анализ, который основан на механизмах и методах теории вероятности и математической статистики, определяет в числовом измерении уровень влияния рисковых факторов проекта на изменение эффективности проекта. Он основывается на результатах проведенного качественного анализа и бизнес-план проекта [15].

Рисунок 2 – Схематическая классификация информационных рисков

Основной задачей качественного анализа является идентификация всех возможных рисков. При его выполнении определяются факторы возникновения, области появления риска, при которых возникает данный риск. Величина же ущерба от этих рисков, источники их появления и вероятную величину потерь предприятия от наступления этих рисков определяют с помощью количественного анализа.

В настоящее время наиболее распространенными являются следующие методы анализа рисков [16]:

- статистический;
- экспертных оценок;
- аналитический;
- оценки финансовой устойчивости и платежеспособности;
- оценки целесообразности затрат;
- анализ последствий накопления риска;
- метод использования аналогов;
- комбинированный метод.

Статистический метод заключается в изучении статистики потерь и прибылей, имевших место на данном или аналогичном предприятии, с целью определения вероятности события, установления величины риска. Вероятность означает возможность получения определенного результата.

В последнее время стал популярен метод статистических испытаний - метод «Монте-Карло».

Главной особенностью этого метода является возможность оценить разные факторы риска в рамках одного подхода и проанализировать разнообразные сценарии реализации проекта.

Главным недостатком данного метода является использование вероятностных характеристик, что затрудняет его использование в практическом применении.

Метод экспертных оценок. *Экспертная оценка* — это выявленное по специальной методике мнение экспертов по определенному вопросу.

Главным отличием этого метода метод сбора информации для построения кривой риска. Оценки различных специалистов и экспертов, оценивающих возможность возникновения потерь от наступления рисков – это основной источник информации для анализа. Сложность применения этого метода возрастает при увеличении количества показателей оценки.

Метод экспертных оценок используется регулярно как в отечественной, так и в зарубежной практике. В различных этапы развития проекта роль экспертных заключений для определения различных показателей существенно возрастает, т.к. используемые для расчета показатели не являются неизменными.

Результат экспертной оценки может быть получен как после проведения специальных исследований по определенно теме, так и при использовании накопленного опыта ведущих специалистов в данной области.

Возрастание риска при осуществлении проекта требует более тщательной оценки критических моментов его реализации. Множество исходных показателей, часто конкурирующих между собой, предполагает использование экспертных оценок для конструирования критерия качества проекта. Поэтому система оценки инвестиций в современных условиях в силу необходимости становится «человеко-алгоритмической», причем роль человека-эксперта является определяющей.

Постадийная оценка рисков основана на том, что риски определяются для каждой стадии проекта отдельно, а затем находится суммарный результат по всему проекту. Обычно в каждом проекте выделяются стадии:

- подготовительная (выполнение всего комплекса работ, необходимых для начала реализации проекта);

- строительная (возведение необходимых зданий и сооружений, закупка и монтаж оборудования);

- функционирования (вывод проекта на полную мощность и получение прибыли).

Все расчеты выполняются дважды – на момент составления проекта и после выявления наиболее опасных его элементов.

Характер инвестиционного проекта как чего-то совершаемого в индивидуальном порядке по существу оставляет единственную возможность для оценки значений рисков – использование мнений экспертов.

Каждому эксперту, работающему отдельно, представляется перечень первичных рисков по всем стадиям проекта и предлагается оценить вероятность наступления рисков в соответствии со следующей системой оценок:

0-25 – риск рассматривается как несущественный;

25-50 –маленькая вероятность реализации риска;

50-75 – о наступлении данного события ничего определенного сказать нельзя;

75-99 – высокая вероятность реализации риска;

100 – риск реализуется

Оценки экспертов подвергаются анализу на непротиворечивость полученных данных, который выполняется по определенным правилам. Максимально допустимая разница между оценками двух экспертов по любому фактору не должна превышать 50. Сравнения результатов заключений проводятся по модулю (знак плюс или минус не учитывается), что позволяет устранить недопустимые различия в оценках экспертами вероятности наступления отдельного риска. Если количество экспертов больше трех, то оценкам подвергаются попарно сравнимые мнения [17].

Распространенным метод экспертного анализа является метод Дэльфи. Его особенностью является управляемая обратная связь. Членов комиссии физически разделяют, что обеспечивает им невозможность группового обсуждения поставленных вопросов. После обработки результата обобщенный результат сообщается каждому члену комиссии. Основная цель такого действия — позволить ознакомиться с оценками других членов

комиссии, не подвергаясь влиянию чужого мнения, кто конкретно дал ту или иную оценку. После этого оценка может быть повторена [18].

Главной задачей при использовании этого метода является подбор компетентных экспертов, так как от их мнений зависит выбор управленческого решения по проекту.

Еще один важный метод исследования риска — *моделирование задачи выбора с помощью «дерева решений»*. Данный метод предполагает графическое построение вариантов решений, которые могут быть приняты. По ветвям «дерева» соотносят субъективные и объективные оценки возможных событий. Следуя вдоль построенных ветвей и используя специальные методики расчета вероятностей, оценивают каждый путь и затем выбирают менее рискованный.

Однако этот метод очень трудоемкий. Кроме того, в «дереве» учитываются только те действия, которые намерен совершить предприниматель, и только те исходы, которые с его точки зрения могут иметь место. При этом совсем не учитывается влияние внешней среды на деятельность предпринимательской фирмы, а предприниматель не всегда может предвидеть действия партнеров, конкурентов.

Аналитический метод. Аналитический способ построения кривой риска наиболее сложен, поскольку лежащие в основе его элементы теории игр доступны только очень узким специалистам. Чаще используется подвид аналитического метода — *анализ чувствительности модели*. Он состоит из следующих шагов: выбор ключевого показателя, относительно которого и производится оценка чувствительности (внутренняя норма доходности, чистый приведенный доход и т. п.); выбор факторов (уровень инфляции, состояние экономики и др.); расчет значений ключевого показателя на разных этапах осуществления проекта (закупка сырья, производство, реализация, транспортировка, капитальное строительство и т. п.). Сформированные таким образом последовательности затрат и поступлений финансовых ресурсов дают возможность определить потоки фондов

денежных средств для каждого момента (или отрезка времени), т. е. определить показатели эффективности. Строятся диаграммы, отражающие зависимость выбранных результирующих показателей от величины исходных параметров. Сопоставляя между собой полученные диаграммы, можно определить так называемые ключевые показатели, в наибольшей степени влияющие на оценку доходности проекта.

Методом морфологического анализа пользуются при наличии малого объема информации по изучаемой проблеме.

Это метод применяется при изучении рисков высокой степени. Такие риски возникают при формировании новых потребностей потребителей, новых рынков сбыта.

Данный подход позволяет получить систематизированные данные по возможным решениям изучаемой проблемы. Он позволяет аккумулировать данные для последующих исследований, связать между собой объекты, явления и концепции. Принципиальным отличием морфологического подхода является использование полной совокупности знаний об объекте. В процессе анализа все процессы и объекты разбиваются на группы, которые подвергаются тщательному анализу.

Ниже приведены этапы морфологического анализа:

- Точная формулировка риск-проблемы;

- Тщательный анализ всех параметров, важных с точки зрения решения данной проблемы риска.

- Построение "морфологического ящика", потенциально содержащего все решения. Такой "ящик" является многомерным пространством. Если проблема решена, то каждое отделение такого "ящика" будет содержать только одно возможное решение, либо вообще не будет его иметь (появление двух и более решений в одном отделении указывает, что не все параметры

были учтены или введены в систему, поэтому производится поиск упущенных параметров);

- "Морфологический ящик" строится в виде "дерева" или матрицы, в клетках которой помещены соответствующие параметры. Последовательное соединение одного такого параметра первого уровня с одним из параметров последующих уровней представляет собой одно из возможных решений проблемы. Общее число возможных решений равно произведению чисел параметров, взятых по строкам. Так как часть решений практически неосуществима, действительное число решений будет несколько меньшим. На основе такого набора общих характеристик объекта можно путем перестановок и различных сочетаний выработать вероятностные характеристики, которые не существуют, но могут существовать.

Следующий этап – изучение полученных решений. С помощью графиков можно отобразить эффективность различных решений (топологические характеристические карты). Это наиболее слажной этап морфологического метода, т.к. отсутствуют формальные методы определения функциональной ценности.

Следующим этапом является *выбор наиболее желательных конкретных решений и их реализация*.

В итоге после морфологического анализа вырабатывается обновленная информация об объекте, рисках, связанных с ним, а так же определяются возможные варианты управления этими рисками.

После выявления рисков, с которыми может столкнуться фирма в процессе производственной деятельности, определения факторов, оказывающих влияние на уровень риска, и проведения оценки рисков, а также выявления связанных с ними потенциальных потерь, перед фирмой стоит задача разработки программы минимизации выявленных рисков с помощью различных методов управления рисками.

1.4 МЕТОДЫ УПРАВЛЕНИЯ РИСКАМИ

Анализ рисков целесообразен на начальном этапе, для определения категории риска, его степени влияния на экономическую составляющую предприятия и для определения последствий после наступления этого риска. Для минимизации последствий рисков необходимо использовать методы управления рисками.

В условиях действия разнообразных внешних и внутренних факторов риска могут использоваться различные способы снижения риска, воздействующие на те или иные стороны деятельности предприятия [19].

Все методы управления рисками принято разделять на 4 группы [20]:

- методы уклонения от рисков;
- методы локализации рисков;
- методы диверсификации рисков;
- методы компенсации рисков.

В Предпринимательской деятельности чаще всего используются Методы уклонения от рисков, которые подразделяются на:

- *отказ от ненадежных партнеров*. Суть этого метода заключается в отказе от рискованных инновационных проектов, где требуется поиск новых партнеров для их выполнения, а так же введение больших инвестиций.

- *отказ от рискованных проектов* основывается на отказе от инновационных и иных проектов, выполнение или эффективность, которых вызывает сомнение;

- *страхование рисков* является основным приемом по снижению влияния риска. Основой этого метода является повышение ответственности лиц, которые принимают решения, тем самым выступая гарантом и защитой от принятия неудачных решений в компании. Главной проблемой этого метода является его применимость при создании или использовании новой продукции или технологий. В такой ситуации у страховых компаний нет достаточного количества данных для проведения расчетов и анализа.

- целью *поиска гарантов* является перенос риска на какое-либо третье лицо. Предполагаемого гаранта необходимо заинтересовать уникальным продуктом или услугой от совместной реализации проекта, т.е. сделать полезность взаимной. Гарантом могут выступать различные фонды, государственные и частные организации и предприятия и т.д.

- *увольнение некомпетентных работников* [20].

Методами локализации рисков пользуются в тех редких случаях, когда есть возможность четко определить источники возникновения рисков и идентифицировать их. Эти методы позволяют выделить в отдельные структурные подразделения наиболее опасные этапы бизнес-процессов, тем самым увеличив возможность контроля над ними. К данным методам относятся:

- *создание специальных структурных подразделений* (с обособленным балансом) внутри организации для выполнения рискованных проектов;

- *создание венчурных предприятий*. Данный метод предлагает создавать отдельное дочернее предприятие, т.е. отдельное юридическое лицо для высоко рискованных проектов. Это позволяет использовать научный и технический ресурс материнского предприятия, в то время как рискованная часть будет локализоваться в дочернем предприятии.

- *заключение договоров о совместной деятельности для реализации рискованных проектов.*

Методы диверсификации рисков заключаются в распределении общего риска и подразделяются на:

- *распределение ответственности между участниками проекта* применяется при необходимости распределения ответственности и сферы действия каждого участника проекта. При использовании данного метода необходимо юридически закрепить, а так же однозначно определить зоны ответственности каждого участника проекта;

- *диверсификация видов деятельности и зон хозяйствования* это увеличение числа применяемых технологий, расширение ассортимента

выпускаемой продукции или оказываемых услуг, ориентация на различные социальные группы потребителей, на предприятия различных регионов;

- *диверсификация сбыта и поставок* может быть применена в тех случаях, когда есть уверенность, что убытки на одном рынке будут покрыты прибылью на других, менее рискованных и однозначных рынках. Так же этот метод может применяться при закупке сырья у различных поставщиков. В данном случает предприятие может почти безболезненно начать взаимодействие с другими поставщиками аналогичного продукта при нарушении поставок от основного;

- *диверсификация инвестиций* предполагает за место выполнения одного крупномасштабного инвестиционного проекта несколько небольших по вложениям. В таком случает у предприятия остается возможность не использовать все ресурсы предприятия, а задействовать их по мере необходимости одного из небольших проектов;

- *распределение риска во времени (по этапам работы),* т.е. необходимо распределять и фиксировать риск во времени при реализации проекта.

Методы компенсации рисков основаны на результатах обширной аналитической работы. Они наиболее трудоемки и направлены на создание механизмов предупреждения опасности [22].

- *стратегическое планирование деятельности* направлен на идентификацию источников появления рисков, разработать методы их минимизации, а так же выявление узких мест проекта. Данный метод является эффективным при разработки стратегии предприятия, охватывающей все сферы деятельности.

- *прогнозирование внешней обстановки* направлено на проработку общеэкономического прогнозирования, поведения партнеров по бизнесу, а так же действия конкурентов.

- суть метода *создания системы резервов* состоит в создании внутри предприятия страховых запасов материалов, сырья, денежного фонда, а так же планов использования этих ресурсов при наступлении кризисных

ситуаций. Данный метод похож на страхование, но направлен на внутреннюю среду предприятия;

- *мониторинг социально-экономической и нормативно-правовой среды* позволяет оперативно отслеживать информацию о протекающих бизнес-процессах. Для использования данного метода важнейшим фактором является достоверная информация и ее постоянное обновление. Данный метод опирается на результаты прогнозно-аналитических исследований, информацию полученную от экспертов и консультантов. Достоверность и оперативность данной информации позволяют определить танденции взаимоотношений между субъектами, принять меры по минимизации потерь и скорректировать оперативные и стратегические планы по развитию предприятия и его процессов.

- *обучение персонала и его инструктирование* применяется повсеместно. Этот метод направлен не только на поддержание уровня знаний и умений персонала, но так же на минимизацию ущерба от наступления рисковых ситуаций и избежание частоты их появления[22].

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

На данном этапе проделана следующая работа:

- Уточнен понятийный аппарата информационных рисков, исходя из которого можно выделить информационный риск как отдельную категорию рисков, возникающих на предприятиях при внедрении информационных технологий;

- Проведена классификация информационных рисков по различным критериям;

Рассмотрены различные методы анализа и управления рисками, проведен их сравнительный анализ. Наиболее подходящими для использования применительно к информационным рискам являются статистический метод и метод экспертных оценок.

В связи со своей специфичностью и связью с информационными активами, определить их влияние на экономические показатели предприятия без разработки методического подхода к их управлению почти невозможно.

2 РОЛЬ ИНФОРМАЦИОННЫХ РИСКОВ В ДЕЯТЕЛЬНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Влияние информационных технологии на жизнь промышленных предприятий очень велико. Они позволяют связать все системы предприятия в одну, оперативно получать сводки по интересующим параметрам, управлять производством, хозяйственной деятельностью предприятия, хранить и обрабатывать различные типы данных, строить аналитические отчеты, оказывают помощь в принятии решений. Современное состояние, уровень развития, эффективность предприятия неразрывно связаны с обеспечением информационной поддержки бизнес-процессов, поэтому сегодня практически ни у кого не вызывает сомнений необходимость построения информационной системы предприятия. Большинство людей, принимающих решения в этой области, разделяют мнение, что вопросы построения информационной системы следует решать в контексте задач совершенствования бизнес-процессов. Существует и ясное понимание того, что максимально эффективной будет система, обеспечивающая непрерывное информационное сопровождение производственного цикла.

2.1 ТЕНДЕНЦИИ В РАЗВИТИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

В таблице 1 приведены статистические данные по использованию информационных технологий на промышленных предприятиях за 16 лет.

Таблица 1 – Основные показатели использования информационных технологий

Название	Количество предприятий по годам					В процентах от общего числа обследованных предприятий				
	2000	2004	2008	2012	2016	2000	2004	2008	2012	2016
Число обследованных предприятий, шт	8536	8870	9023	9103	9370	100	100	100	100	100

Название	Количество предприятий по годам					В процентах от общего числа обследованных предприятий				
	2000	2004	2008	2012	2016	2000	2004	2008	2012	2016
Использовали локальные сети	6235	7653	8806	9095	9370	73	86	98	100	100
Использовали глобальные информационные сети	6025	8034	8300	8654	9325	71	91	92	95	100
Имели вэб-сайты	4569	6954	7632	8542	9303	54	78	85	94	99
Использовали информационные системы	3653	6562	7958	8212	9065	43	74	88	90	97
Число персональных компьютеров (на 100 человек)	21	34	68	78	92	21	34	68	78	92

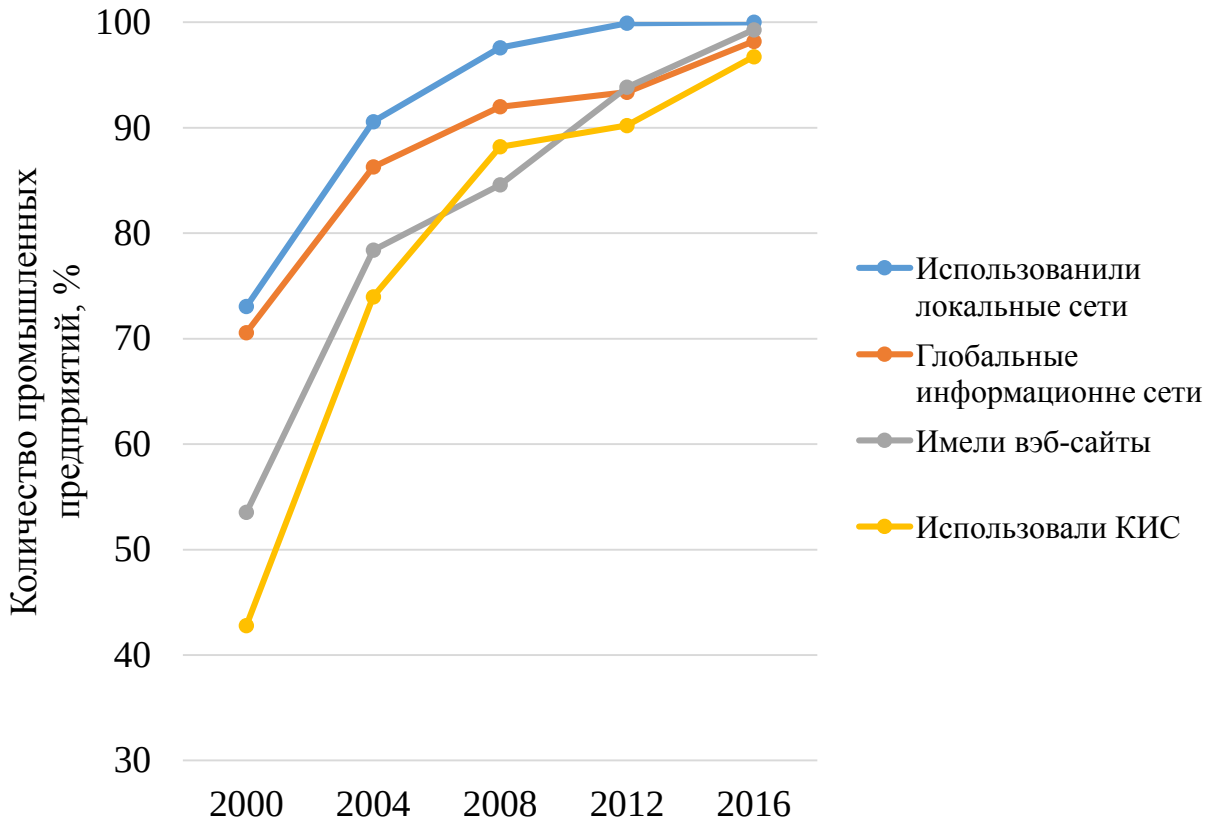

Рисунок 3 – Использование информационных технологий на промышленных предприятиях

Из графика видно, что использование информационных технологий в деятельности предприятий с каждым годом растет, появляются новые виды

технологий, применение которых может ускорить производственные процессы, улучшить качество выпускаемой продукции, сократить время обработки информационных ресурсов, что, в свою очередь, позволяет увеличить скорость получения экономического эффекта.

Но при увеличении уровня автоматизации предприятия необходимо так же учитывать и возможный негативный эффект при использовании информационных технологий – информационных рисков, которые присутствуют в каждом виде деятельности, нанося материальный и нематериальный вред организации.

Несмотря на возрастание значения информации и информационных технологий для каждого предприятия оно так же сопровождается усложнением задач управления информационной сферой. Важнейшими из них являются рациональное использование инвестиций в информационные технологии и снижение рисков, связанных с информационными процессами предприятия.

Рост расходов на развитие информационных технологий во всех видах деятельности с каждым годом растет. По подсчетам экспертов компании IDC, рост расходов в период с 2015 по 2020 составит порядка 3,3% в год.

В 2016 г. мировые ИТ-расходы увеличились на 0,6% по сравнению с 2015 г. до $3,54 трлн.

Тенденция увеличения затрат на развитие информационных технологий присутствует и на промышленных предприятиях. С 2008 по 2016 года примерно в 2 раза увеличились затраты организаций на развитие информационного комплекса [29].

В таблице 2 и рисунке 4 приведены данные Росстата по затратам промышленных предприятий на развитие информационных технологий за последние 8 лет [30].

Таблица 2 – Статистика затрат на информационные и телекоммуникационные технологии промышленными предприятиями

Затраты на информационные и телекоммуникационные технологии (в процентах от общего числа)	Годы				
	2008	2010	2012	2014	2016
На приобретение вычислительной техники	52,3	41,3	37,7	35,6	32,8
На приобретение программных средств	7,7	11	11,3	13,5	15,3
На модернизацию каналов передач данных	20,9	25,9	29,4	30,7	31,5
На обучение сотрудников	0,7	1,4	0,8	0,7	2,4
На оплату услуг сторонних организаций и специалистов по информационным технологиям	11,3	14,7	15,2	16,5	17,7
Прочие затраты	7,1	5,7	5,6	3	0,3

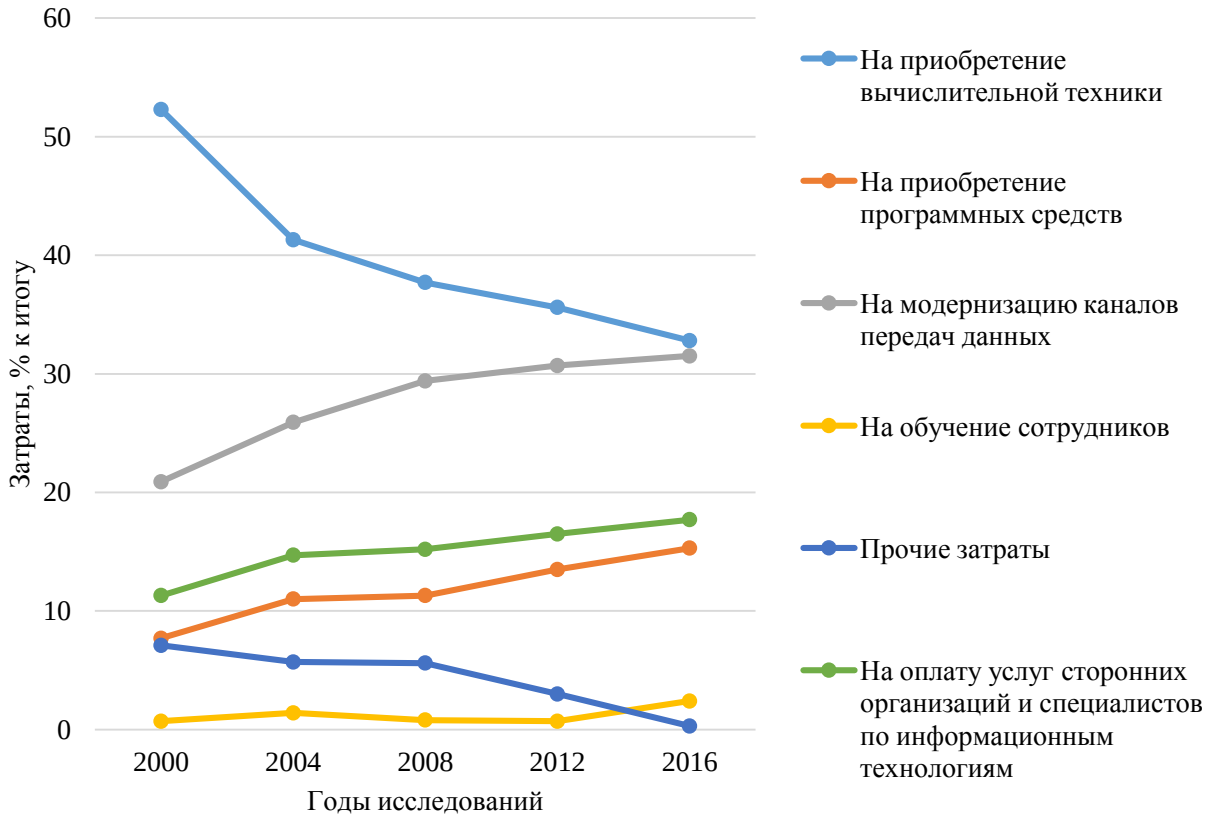

Рисунок 4 – Статистика затрат предприятий на информационные технологии

Из диаграммы видно, что затраты на приобретение вычислительной техники сократились, а на приобретение программных средств увеличиваются с каждым годом. Это связано с тем, что вычислительная техника еще не успела морально устареть или выйти из строя, а новые разработки в сфере ПО растут с каждым годом.

На 6,4% увеличились расходы предприятий на оплату услуг сторонних организаций и специалистов. Этот рост связан с развитием сложных корпоративных информационных систем и их модулей, которые внедряются на предприятия. Содержать высококлассных специалистов по таким системам в штате предприятия становится не выгодно, поэтому поддержание их работоспособности отдается на аутсорсинг.

Необходимость успешного функционирования в условиях жесткой конкурентной среды диктует свои требования к эффективности бизнес-процессов предприятия. Решение задачи повышения эффективности неразрывно связано с обеспечением информационной поддержки процессов с помощью внедрения различных программных средств.

Данные Росстата по использованию предприятиями различных программных средств за последние 16 лет приведены в таблице 3 [30].

Таблица 3 – Данные Росстата по использованию программных средств предприятиями.

Название	Количество предприятий по годам					В процентах от общего числа обследованных предприятий				
	2000	2004	2008	2012	2016	2000	2004	2008	2012	2016
Организации, использовавшие специальные программные средства - всего, шт.	8536	8870	9023	9103	9370	100	100	100	100	100
Для решения организационных, управленческих и экономических задач	5863	6956	7896	8653	9100	69	78	88	95	97

Название	Количество предприятий по годам					В процентах от общего числа обследованных предприятий				
	2000	2004	2008	2012	2016	2000	2004	2008	2012	2016
Антивирусные программы	-	1365	4653	6356	9125	-	15	52	70	97
Для осуществления финансовых расчетов в электронном виде	3652	5698	6657	8542	9205	43	64	74	94	98
Для управления продажами и логистикой	-	-	2658	4698	8654	-	-	29	52	92
АСУТП или отдельными технические средства	3128	3956	4856	5896	7896	37	45	54	65	84
КИС (MRP, ERP, CRM)	-	-	2015	4523	8456	-	-	22	50	90

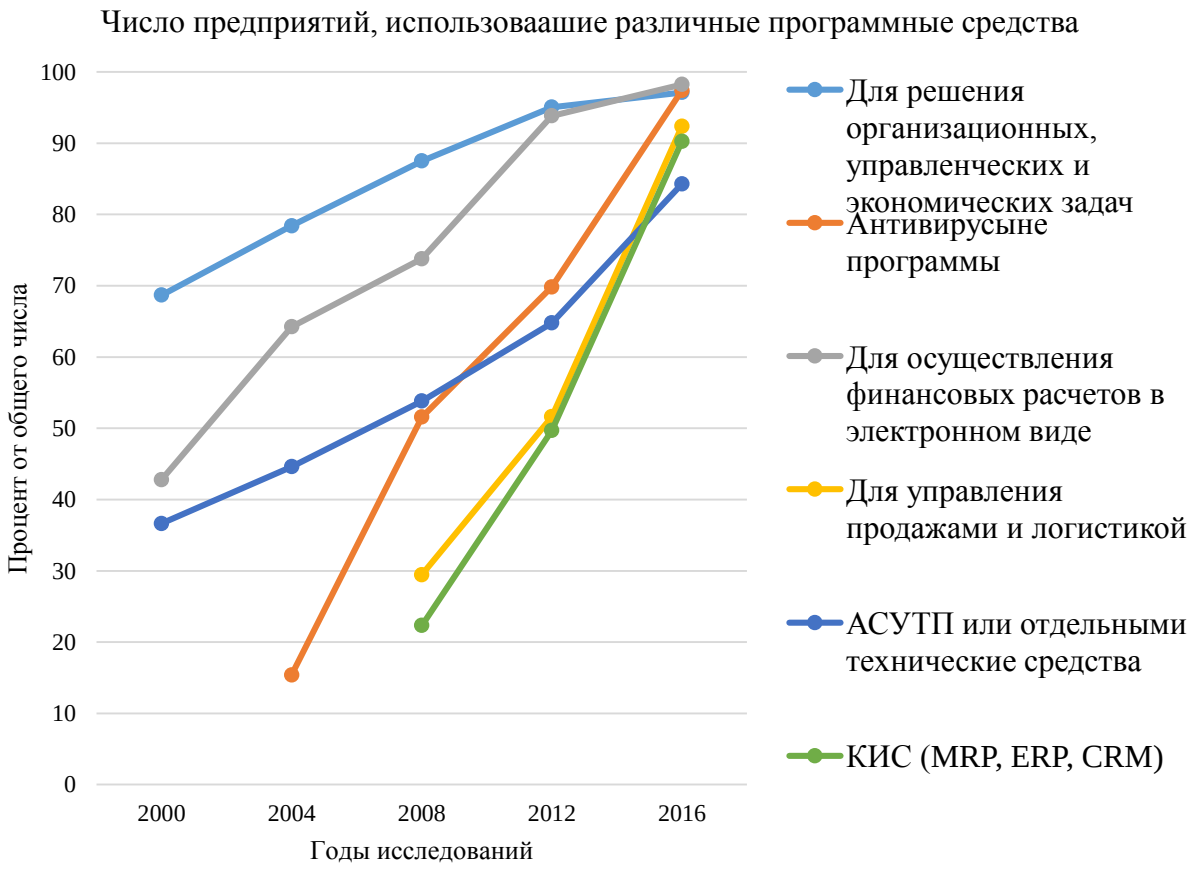

Рисунок 4 – Число предприятий использовавшие различные программные средства в разные годы

Из графика видно, что на протяжении рассмотренного периода наблюдается только рост использования программных средств предприятиями. Так же, следует отметить, что предприятия внедряют новые программные комплексы, ранее не использовавшиеся на предприятиях.

Растущее влияние web-технологий не обходит стороной и промышленные предприятия. Возможности объединения различных систем как одного предприятия так и нескольких в одну, получение мобильной отчетности, облачные хранилища данных является ключевыми факторами успеха компании на рынке и не обходятся без значительных вложений в модернизацию каналов передач данных.

Таким образом, использование новых аппаратных и программных комплектов ИСП, внедрение новых КИС, web-технологий кроме своего положительно влияния так же могут создавать места для нарушения информационной безопасности объекта, а значит, создавать новые факторы для появления информационных рисков на предприятиях.

2.2 АНАЛИЗ ИСПОЛЬЗОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

Для анализа эффективности управления информационными рисками на предприятиях было проведено анкетирование среди руководителей, менеджеров различных отделов, IT специалистов на промышленных предприятиях г. Екатеринбурга. В число предприятий вошли: ООО «Виз-Сталь», ПАО «Машиностроительный завод им. М.И. Калинина», ПАО «Уралмашзавод». В общей сложности было опрошено 120 человек. Анкета разбита на 3 условных блока: управление рисками, информационные риски, информационная безопасность. Рассмотрим каждый из них подробнее.

Блок «Управление рисками» включает ряд вопросов, касающихся наличия и уровня системы управления рисками, стандартов, основных подходов, а так же действий по обработке рисков на предприятиях.

Большинство опрошенных (45%) отметили отсутствие системы управления рисками на своих предприятиях, и только 21% опрошенных указали на применение таких систем на своих предприятиях.

У 28% опрошенных определены основные подходы к оценке рисков в организации, при этом 71% опрошенных не имеет представления о подходах к оценке рисков и не использует их в деятельности своих предприятий.

В блок «Информационные риски» вошли вопросы, посвященные разновидностям информационных рискам на предприятиях, стандартах и уровнях анализа и оценки этих рисков в деятельности предприятий.

75% опрошенных указали, что самой частой разновидностью информационных рисков оказался выход из строя оборудования. На втором месте по значимости для предприятий оказались ошибки персонала при работе с информационными технологиями предприятий. Самым редко проявляемым оказались сетевые атаки.

Детализация результатов опроса по основным разновидностям рисков приведена в таблице 4 и рисунке 5.

Таблица 4 – Результаты анкетирования блока информационных рисков

Вид информационного риска (по механизму воздействия)	Сумма рангов	Средняя оценка
Стихийные бедствия	52	0,4
Пожары	120	1,0
Ошибки специалистов при работе с IT	486	4,1
Сбои и отказы технических средств	564	4,7
Сбои и отказы сетевого оборудования	386	3,2
Сбои и отказы программных средств	428	3,6

Вид информационного риска (по механизму	Сумма	Средняя
Вредоносное ПО	318	2,7
Шпионские программы	240	2,0
Несанкционированный доступ	320	2,7
Нарушение авторских прав	196	1,6
Аварии	142	1,2

Рисунок 5 – Частота наступления информационных рисков

Из таблицы и рисунка видно, что, по мнению опрошенных, самым частым информационным риском на предприятии являются сбои и отказы технических средств (4,7 балла). Вторым по частоте появления являются ошибки специалистов при работе с информационными технологиями (4,1 балла). Частота сбоев и отказов программных средств на промышленных предприятиях так же велика - 3,6 балла.

Не смотря на наличие на некоторых предприятиях системы управления рисками, анализ, оценка и идентификация информационных рисков

проводится только на предприятиях у 21% опрошенных. Большинство (65% опрошенных) указали на отсутствие методик и обучения по необходимым действиям в случае выявления информационных рисков на рабочих местах.

Ряд вопросов посвящен информационной безопасности на промышленных предприятиях и их связи с информационными рисками вошли в блок «Информационная безопасность».

Информационная безопасность организации - состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие [31].

Ущерб от нарушения информационной безопасности может выражаться как в экономических показателях, так быть и не материальным (снижение репутации и уровня доверия, потеря конфиденциальной информации).

Учитывая важность связи между информационными рисками и информационной безопасностью, лишь 34% опрошенных указали на проведение мероприятий по выработке рекомендаций и методик анализа и минимизации рисков на основе инцидентов, вязанных с информационной безопасностью.

Не смотря на достаточно большое количество стандартов по информационным рискам, управлению рисками, опыт мировых промышленных предприятий, было выявлено, что информационные риски, как категория рисков, связанных с непосредственным использованием информационных технологий, почти не учитываются в системах управления рисками, используемыми на предприятиях.

Таким образом, можно сделать вывод, что, не смотря на наличие информационных рисков в деятельности, отсутствует комплексный подход по их управлению.

2.3 АНАЛИЗ ВЛИЯНИЯ ИНФОРМАЦИОННЫХ РИСКОВ НА ДЕЯТЕЛЬНОСТЬ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ НА ПРИМЕРЕ ООО «ВИЗ-СТАЛЬ»

Для проведения анализа по влиянию информационных рисков, необходимо определиться с местами их возможного появления на промышленном предприятии. В широком смысле местами могут выступать любые отделы, подразделения, где применяются IT-технологии, т.е. используется аппаратное и программное обеспечение, каналы передач данных, есть доступ в Интернет.

С точки зрения системного анализа информационная система предприятия (ИСП) представляет собой открытую систему, состоящую из множества взаимосвязанных информационных элементов, с помощью которых происходит получение, обработка, хранение и передача необходимой информации в целях эффективного функционирования предприятия [32]. Все информационные элементы системы можно условно разделить на субъекты и объекты информационных процессов. Субъектами выступают сотрудники предприятия, имеющие отношение к получению, обработке, хранению и передаче информации. Объектами являются корпоративные информационные системы предприятия (КИС), информационные ресурсы, каналы передач данных, программные и аппаратные средства информационных систем предприятия.

Внешнюю информационную среду предприятия образуют объекты, субъекты, процессы и явления внешней среды, оказывающие влияние на элементы информационной системы предприятия и на информацию во внешней среде, имеющую отношение к предприятию, его бизнес-процессам.

Во внешней среде можно выделить элементы двух типов. К элементам первого типа относятся объекты, субъекты, процессы и явления, которые оказывают влияние на информационную систему предприятия. Эти элементы в свою очередь могут быть разделены на две группы. Первую группу

образуют элементы информационного взаимодействия с информационной системой предприятия. Такое взаимодействие определяется лишь информационными ресурсами и характером взаимодействия по обмену информацией. Примерами таких элементов могут служить средства массовой информации; партнеры по бизнесу; потребители продукции или услуг; государственные структуры; злоумышленники, использующие программные средства воздействия и т.д.

Ко второй группе относятся элементы внешней среды, которые оказывают неинформационное воздействие на элементы ИСП. Это природные явления; техногенные аварии; злоумышленники, оказывающие воздействие на материальные объекты информационной системы и другие элементы. Особенностью элементов этой группы является преимущественное одностороннее воздействие этих элементов на объекты информационной системы.

Элементы внешней среды второго типа оказывают информационное воздействие на внешнюю среду, в результате которого изменяются условия во внешней среде для ведения бизнеса предприятием. Во внешней среде целесообразно ограничиться анализом только элементов, оказывающих информационное воздействие на внешнюю среду. Это объясняется отсутствием реальных механизмов у предприятия оказания воздействия на элементы, которые опосредовано влияют на информационные элементы внешней среды.

Существует три основных пути причинения ущерба предприятию в результате реализации информационного риска.

Во-первых, использование в работе информации, качество и достоверность которой были нарушены, могут привести к ущербу для предприятия.

Во-вторых, существуют риски, которые напрямую воздействуют на объекты информационной системы предприятия и могут нарушить работоспособность или сломать объекты информационной системы. Такими

информационными рисками могут выступать аварии, стихийные бедствия и пожары, сбои и отказы технических средств, утрата баз данных, несанкционированный доступ и др. Для восстановления работоспособности объектов информационной системы после воздействия таких рисков предприятию необходимо задействовать человеческие, экономические и временные ресурсы [33].

Изменение состояния внешней среды, которая влияет на эффективность функционирования предприятия, является третьим путем причинения ущерба.

Примером может являться потеря конфиденциальной информации. Из-за этого может произойти срывы важных переговоров с партнерами по бизнесу, может измениться конъюнктура рынка, что, в конечном результате, может привести к ущербу в материальных и интеллектуальных ресурсах предприятия. Критической является ситуация, когда из-за утраты конфиденциальных сведений предприятию наносится такой ущерб, который может привести к банкротству.

В результате, информационные риски воздействуют на информационные элементы ИСП, вызывая изменение внутренних и внешних условий функционирования предприятия. В результате этих изменений предприятие терпит убытки, ему наносится определенный ущерб. Основными местами появления информационных рисков в ИСП предприятия являются информационные системы различного класса и аппаратно-программные комплексы, которые применяются в деятельности предприятия [34].

Основные информационные системы, которые используются на промышленных предприятиях представлены на рисунке 2.

Рисунок 5 – Основные информационные уровни промышленного предприятия

Информационные системы предприятий имеют различный функционал и различное применение.

АСУТП (автоматические системы управления технологическим процессом) - группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

MES (Manufacturing Execution System, система управления производственными процессами) - специализированное прикладное программное обеспечение, предназначенное для решения задач синхронизации, координации, анализа и оптимизации выпуска продукции в рамках какого-либо производства. MES-системы относятся к классу систем управления уровня цеха, но могут использоваться и для интегрированного управления производством на предприятии в целом.

ERP (англ. *Enterprise Resource Planning*, *планирование ресурсов предприятия*) – организационная стратегия интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и

оптимизацию ресурсов предприятия посредством специализированного интегрированного пакета прикладного программного обеспечения, обеспечивающего общую модель данных и процессов для всех сфер деятельности.

Модульный принцип организации позволяет внедрять ERP-системы поэтапно, последовательно переводя в эксплуатацию один или несколько функциональных модулей, а также выбирать только те из них, которые актуальны для организации. Кроме того, модульность ERP-систем позволяет строить решения на основе нескольких ERP-систем, выбирая из каждой лучшие в своём классе модули. Разбивка по модулям и их группировка различная, но у большинства основных поставщиков выделяются группы модулей: финансы, персонал, операции [35].

BI-системы или системы бизнес-аналитики (Business Intelligence)- это аналитические системы, которые объединяют данные из различных любых источников информации, обрабатывают их и предоставляют удобный интерфейс для всестороннего изучения и оценки полученных сведений. Данные полученные в результате такого анализа помогают достигать поставленных бизнес-целей с помощью оптимального использования имеющихся данных. Комплексный анализ данных по всем направлениям бизнеса позволяет повысить его эффективность и снизить издержки. Таким образом, системы бизнес-анализа (BI-системы) - это единый прозрачный источник данных о бизнесе компании для ее руководства. Сегодня генерация отчетности и выполнение анализа это вовсе не роскошь, которую компании могут себе позволить или от которой они могут отказаться. Действительно, в той или иной форме отчетность требуется как для всего бизнеса так и для различных слагающих его частей - будь то корпоративное транзакционное приложение, база данных или же процесс, исполняемый на регулярной основе. Решения для подготовки отчетности охватывают все аспекты бизнеса, их наличие считается обязательным, а сами они рассматриваются как корпоративный стандарт наряду с другими базовыми технологиями.

Каждая из описанных систем представляет собой сложный аппаратно-программный комплекс со сложной клиент-серверной архитектурой и может являться средой для появления информационных рисков предприятия.

Для определения влияния информационных рисков необходимо получить данные по реализации информационных рисков на конкретном предприятии.

В качестве предприятия по сбору статистических данных и проведения исследования по влиянию информационных рисков выступило предприятие ООО «Виз-Сталь».

Компания создана в 1998 году на базе Верх-Исетского завода, одного из старейших российских предприятий черной металлургии, путем выделения из структуры предприятия комплекса цеха холодной прокатки. С 2006 года ВИЗ-Сталь входит в состав одного из крупнейших мировых металлургических холдингов – Группу НЛМК и в настоящее время совместно с аналогичным производством в Липецке контролирует 100% производства трансформаторной стали в России.

ВИЗ-Сталь входит в пятёрку крупнейших мировых производителей трансформаторной стали после Nippon Steel (Япония), ThyssenKrupp (Германия) и AK Steel Holding (США). Предприятие – одно из потенциальных центров экономического роста, как производитель элитной металлургической продукции, а также приоритетной ориентированности сбыта на экспорт [30].

Деятельность данного предприятия не обходится без использования IT-технологий в большинстве отделов, а значит существуют предпосылки для появления информационных рисков на предприятии.

ВИЗ-Сталь является активным участником инвестиционного процесса, проводит масштабную программу технического перевооружения производства, стремится соответствовать самым высоким стандартам в области экологии и ресурсосбережения. Компания создает безопасные условия труда, совершенствуя процессы, инвестируя в повышение

квалификации сотрудников и применяя лучшие мировые практики в области охраны труда и развитие информационных технологий.

Наиболее важными для деятельности предприятия ООО «Виз-Сталь» отделами являются:

- Производство;
- Логистика/закупки/поставка;
- Отдел сервиса/отдел планирования ремонтов;
- Экономический отдел/бухгалтерия;
- Руководство.
- IT-отдел;

Каждое направление деятельности связано с другими с помощью КИС предприятия. На исследуемом предприятий используется ERP система SAP R/3.

Последний крупный модуль этой системы был внедрен в июле 2015 г. Внедрение модуля технического обслуживания и ремонта оборудования (ТОРО) стало продолжением перехода предприятия на новую учетную систему на основе SAP, которое направлено, в первую очередь, на повышение качества планирования и учета ремонтных работ, а также обоснованности и прозрачности затрат на их проведение [31]. Его реализация потребовала масштабных организационных усилий, поскольку изменения затронули ежедневную работу всех подразделений предприятия, задействованных в производственном процессе. В настоящий момент система SAP ERP предприятия поддерживает следующие функциональные модули: «бухгалтерский учет», «основные средства, «финансы», «управление себестоимостью — контроллинг», «управление проектами и инвестициями», «управление материальными потоками», «управление сбытом продукции», «производство», «планирование».

В процессе внедрения ПО специалисты ООО «ВИЗ-Стали» создали справочники технических объектов, единиц оборудования и технические

карты ремонтов, упорядочили и систематизировали инструкции, спецификации материалов.

В ходе качественного анализа IT-рисков на предприятии была сделана сводная таблица, в которой для каждого направления деятельности соотнесены возможные источники появления IT-рисков.

Таблица 4 – Таблица соответствия информационных рисков на предприятии ООО «Виз-Сталь»

Направления деятельности производства	Источники появления риска
Производство	АСУТП - автоматизированная система управления технологическим процессом; MRP (manufacturing resource planning) - система планирования производственных ресурсов)
Логистика/закупки/поставка	CRM (*Customer Relationship Management)* – система управления взаимоотношениями с клиентами/заказчиками; SRM (Supplier relationship management) - система управления взаимодействием с поставщиками. доступ в Internet
Сервис/отдел планирования ремонтов	MRP, доступ в Internet, ТОРО – модуль технического обслуживания и ремонта оборудования
Экономический отдел/бухгалтерия	FRM (finance resource management) – система управления финансами; доступ в Internet
Руководство	BI (business intellegense) – оперативная отчетность, стратегическое планирование; HRM (human resource management) – система управления человеческими ресурсами; доступ в Internet
IT-отдел	Модули ERP/MRP систем;

Направления деятельности производства	Источники появления риска
	Каналы передач данных; Уровень компетенций сотрудников;

В ходе сбора статистических данных с предприятия ООО «Виз-Сталь» были получены следующие статистические данные по времени устранения проблем, связанных, связанным с информационными технологиями по основным направлениям деятельности предприятия:

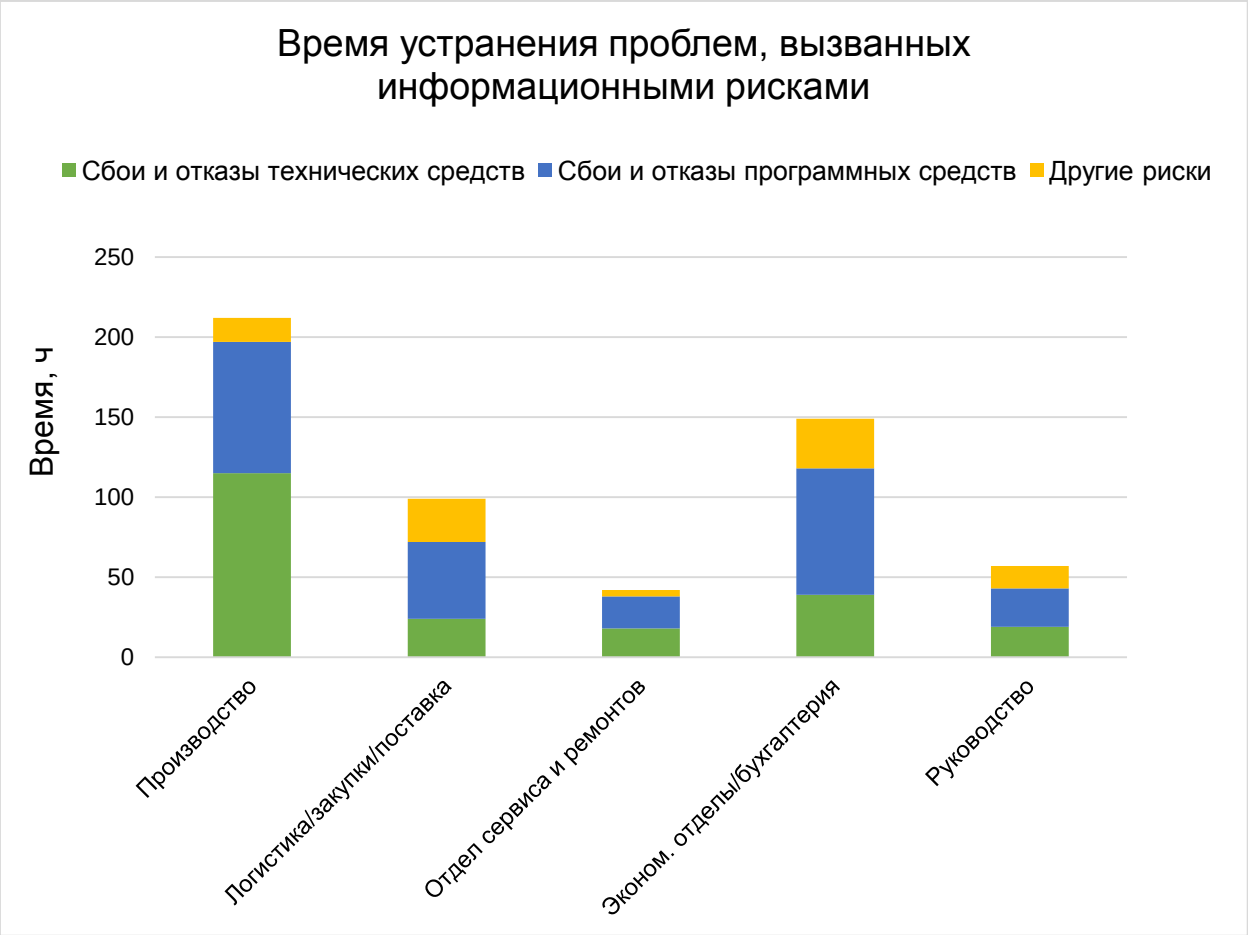

Рисунок 6 – Время устранения проблем, связанных с ИР по основным видам деятельности ООО «Виз-Сталь»

Из диаграммы видно, что наибольшее число простоев приходится на основной вид деятельности – производство (212 ч). Это связано с наличием огромных технических мощностей предприятия. Основным фактором появления информационных рисков на данном направлении деятельности являются SCADA-системы, которые представляют собой программно-

аппаратный комплекс для управления производственными процессами на различных участках производства. Кроме сложности самой системы, огромную роль в управлении данными системами играет компетентность оператора, управляющего системой.

Так же велики простои оборудования в экономической сфере предприятия. Ключевыми факторами для появления простоев оборудования в этой сфере является модуль управления финансовыми потоками, который так же является сложной информационной системой, состоящей из компонентов базы данных, программного обеспечения.

Уровень развития сетевых коммуникаций предприятия и защитных механизмов информационных систем на прямую влияют на доступность, целостность и конфиденциальность используемых данных. Нарушение работоспособности системы безопасности может привести к потере конфиденциальных данных, вредоносное программное обеспечение может вывести из строя не только отдельные элементы, но и всю систему в целом.

Таким образом, суммарное время простоя оборудования и различного оборудования информационных систем, предприятия во всех основных сферах деятельности предприятия составляет 517 часов, т.е. 21 сутки, что в значительной степени влияет на экономические показатели и ведет к экономическим потерям, поскольку, во-первых, специалисты на своих рабочих местах не могут выполнять свои прямые обязанности, а во-вторых для устранения возникших проблем необходимо задействовать специалистов сервисных и IT-служб,.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

- во-первых, увеличение инвестиций на модернизацию аппаратно-программных комплексов и внедрение новых, перспективных разработок промышленными предприятиями, которые помогут организациям ускорить и

упростить обслуживание своих бизнес-процессов, ведут к появлению новых уязвимостей системы и новым информационным рискам;

- во-вторых, влияние информационных рисков на экономические деятельность предприятия может выражаться как в конкретных цифрах (например простои оборудования), так и нести и косвенный вред (потеря конфиденциальной информации), которые, в результате, могут вести в падению экономической эффективности предприятия.

- в-третьих, отсутствует методический подход к управлению информационными рисками на предприятиях, дающий менеджерам различных уровней конкретный инструмент по выявлению и борьбе с информационными рисками на предприятии;

3 МЕТОДИЧЕСКИЙ ПОДХОД К УПРАВЛЕНИЮ ИНФОРМАЦИОННЫМИ РИСКАМИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

Промышленные предприятия с каждым годом вкладывают средства в развитие и модернизацию своих производственных мощностей, развитие и модернизацию информационных технологий как ключевых факторов развития производства. Развитие информационной среды предприятия, внедрение новых модулей КИС предприятия, модернизация каналов передач данных ведет к появлению уязвимостей и создаёт благоприятную среду для появления новых факторов информационных рисков.

В целях минимизации влияния существующих информационных рисков на промышленных предприятиях, предлагается использовать методический подход, который реализуется внедрением *системы управления информационными рисками (СУИР)*.

Под СУИР понимается единый комплекс правовых норм, экономических и организационных мероприятий, технических, программных средств, а также информационных ресурсов и специалистов предприятия, обеспечивающий противодействие информационным рискам и компенсацию ущерба от них.

3.1 МЕТОДИКА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Для применения СУИР на необходима реализация методики управления информационными рисками, которая включает в себя следующие положения:

- анализ информационных рисков является основным этапом управления информационными рисками;
- принятие решения по управлению информационными рисками;
- комплексное согласованное использование методов и средств управления информационными рисками;

В контексте использования СУИР предлагается использовать следующий порядок управления информационными рисками на предприятии (рисунок 7).

Рисунок 7 – Порядок управления информационными рисками в СУИР

Анализ информационных рисков является основным этапом управления и состоит из двух последовательных действий:

- идентификация информационных рисков;
- оценка информационных рисков

Первым этапом анализа информационных рисков является их идентификация. На этом этапе проводится поиск всех возможных информационных рисков для ИСП и создание их перечня. В процессе идентификации предлагается использовать информационную модель предприятия и классификацию информационных рисков. Они позволяют определить место каждого конкретного риска, его природу, понять причину его появления. В результате проведения идентификации рисков получится классификационная таблица, в которой каждый риск будет описан по различным критериям. Классификация должна показывать последствия реализации рисков для информационных систем, по результатам воздействия на информацию можно судить об опасности того или иного риска для предприятия, а также выбирать определенное направление защиты [38].

Классификация рисков по различным критериям представлена на рисунке 3. Ниже, в таблицах 4-8, составлены классификационные таблицы информационных рисков для основных видов деятельности предприятия ООО «Виз-Сталь».

Таблица 4 – Классификационная таблица информационных рисков для Производства

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
АСУТП	1. Механические повреждения устройств	Сбои и отказы технический средств	Технические	РНД	Внутренний
	2. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНД	Внутренний
	3. Ошибки при вводе информации через ПК	Ошибки специалистов	Технические, организационные	РНД, РНЦ	Внутренний
	4. Ошибки при эксплуатации программных средств	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД, РНЦ, РНК	Внутренний
	5. Ошибки при работе с носителями информации	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД, РНЦ	Внутренний
	6. Неправильные действия со средствами защиты информации	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД, РНЦ	Внутренний
	7. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНК	Внутренний, внешний
	8. Отказ системы (ввод, вывод, чтение, запись информации)	Сбои и отказы технических средств, сбои и отказы программных средств	Технические	РНД	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	9. Хищение информации, шпионаж	Нарушение авторских прав, шпионские программы, несанкционированный доступ	Организационные, технические	РНК	Внешний, внутренний
	10. Умышленное внесение изменений в режимы работа устройств	Вредоносное ПО шпионские программы, несанкционированный доступ	Организационные, технические	РНЦ	Внутренний
	11. Блокировка систем защиты	Вредоносное ПО шпионские программы, несанкционированный доступ, ошибки специалистов	Технические	РНД, РНЦ	Внешний, внутренний
	12. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний
MRP	1. Механические повреждения устройств	Сбои и отказы технический средств	Технические	РНД	Внутренний
	2. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНД	Внутренний
	3. Ошибки при вводе информации	Ошибки специалистов	Технические, организационные	РНК, РНЦ	Внутренний
	4. Ошибки при	Ошибки специалистов,	Технические,	РНК,	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	эксплуатации программных средств	сбои и отказы программных средств	организационные	РНЦ	
	5. Ошибки в настройках системы	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНК, РНЦ	Внутренний
	6. Неправильные действия со средствами защиты информации	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНК, РНЦ	Внутренний
	7. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНК	Внутренний, Внешний
	8. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний
	9. Отказ системы (ввод, вывод, чтение, запись информации)	Сбои и отказы технических средств, сбои и отказы программных средств	Технические	РНД, РНЦ	Внутренний
	10. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технических средств	Технические	РНД	Внутренний

Таблица 5 – Классификационная таблица информационных рисков для службы сервиса и ремонтов

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	1. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНД	Внутренний
	2. Ошибки при вводе информации	Ошибки специалистов	Технические, организационные	РНЦ	Внутренний
	3. Ошибки при эксплуатации программных средств	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внутренний
	4. Ошибки в настройках системы	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНЦ, РНК	Внутренний
	5. Неправильные действия со средствами защиты информации	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внутренний
	6. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНК	Внутренний
	7. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний, внешний
	8. Механические	Сбои и отказы технический	Технические	РНД	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	повреждения основных элементов системы	средств, Несанкционированный доступ			
Доступ в Internet	9. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНД	Внутренний
	10. Недоступность ресурсов	Сбои и отказы технических средств, Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний, внешний
	11. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы технических средств, Сбои и отказы сетевого оборудования	Технические	РНД	Внешний, внутренний
	12. Хищение информации, шпионаж	Нарушение авторских прав, шпионские программы, несанкционированный доступ	Организационные, технические	РНК	Внутренний, внешний
	13. Умышленное внесение изменений в режимы работа устройств	Вредоносное ПО шпионские программы, несанкционированный доступ	Организационные, технические	РНК, РНД, РНЦ	Внутренний, Внешний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
Система планирования ремонтов	14. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технических средств	Технические	РНД	Внутренний
	1. Ошибки при вводе информации	Ошибки специалистов	Технические, организационные	РНЦ, РНД	Внутренний
	2. Ошибки при эксплуатации 3. Программных средств	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внутренний
	4. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНК	Внутренний
	5. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний, внешний
	6. Механические повреждения основных элементов системы	Сбои и отказы технический средств, Несанкционированный доступ	Технические, организационные	РНД	Внутренний
	7. Отказ системы (ввод, вывод, чтение, запись информации)	Сбои и отказы технических средств, сбои и отказы программных средств	Технические		Внутренний

Таблица 6 – Классификационная таблица информационных рисков для отделов Логистики/закупки/поставки

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
CRM/SRM	8. Пожары	Стихийные бедствия, пожары	Природные, технические	РНД	Внешний, внутренний
	9. Землетрясения	Стихийные бедствия		РНД	Внешний
	10. Наводнения	Стихийные бедствия		РНД	Внешний
	11. Обрушение зданий	Аварии	Технические	РНД	Внешний
	12. Механические повреждения устройств	Сбои и отказы технический средств	Технические, организационные	РНД	Внутренний
	13. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНЦ	Внутренний
	14. Ошибки при вводе информации	Ошибки специалистов	Технические, организационные	РНД	Внутренний
	15. Ошибки при эксплуатации программных средств	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНЦ, РНК	Внутренний
	16. Ошибки в настройках системы	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внутренний
	17. Неправильные действия со средствами защиты информации	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНК	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	18. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНД	Внутренний, внешний
	19. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний
	20. Механические повреждения 21. Основных элементов системы	Сбои и отказы технический средств, Несанкционированный доступ	Технические	РНЦ	Внутренний
Доступ в Internet	1. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технических средств, Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний
	2. Недоступность ресурсов	Нарушение авторских прав, шпионские программы, несанкционированный доступ	Организационные, технические	РНК	Внутренний, внешний
	3. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования	Сбои и отказы технический средств, Несанкционированный доступ	Организационные, технические	РНД	Внешний, внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	4. Хищение информации, шпионаж	Нарушение авторских прав, шпионские программы, несанкционированный доступ	Организационные, технические	РНК	Внутренний, внешний
	5. Умышленное внесение изменений в режимы работа устройств	Вредоносное ПО шпионские программы, несанкционированный доступ	Организационные, технические	РНД	Внутренний, Внешний

Таблица 7 – Классификационная таблица информационных рисков для экономического отдела/бухгалтерии

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
FRM	1. Механические повреждения устройств	Сбои и отказы технический средств	Технические	РНД	Внутренний
	2. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНЦ	Внутренний
	3. Ошибки при вводе информации	Ошибки специалистов	Технические, организационные	РНД	Внутренний
	4. Ошибки при	Ошибки специалистов,	Технические,	РНЦ,	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	эксплуатации программных средств	сбои и отказы программных средств	организационные	РНК	
	5. Ошибки в настройках системы	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внутренний
	6. Неправильные действия со средствами защиты информации	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНК	Внутренний
	7. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНД	Внутренний, внешний
	8. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний
	9. Отказ системы (ввод, вывод, чтение, запись информации)	Сбои и отказы технических средств, сбои и отказы программных средств	Технические	РНД	Внутренний
Доступ в Internet,	1. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНД	Внутренний
	2. Недоступность ресурсов	Ошибки специалистов	Технические, организационные	РНД	Внутренний, внешний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	3. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внешний, внутренний
	4. Хищение информации, шпионаж	Нарушение авторских прав, шпионские программы, несанкционированный доступ	Организационные, технические	РНД	Внутренний, внешний
	5. Умышленное внесение изменений в режимы работы устройств	Вредоносное ПО шпионские программы, несанкционированный доступ	Организационные, технические	РНЦ	Внутренний, Внешний

Таблица 8 – Классификационная таблица информационных рисков для руководства

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
HRM	1. Механические повреждения устройств	Сбои и отказы технический средств	Технические	РНД	Внутренний
	2. Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технический средств	Технические	РНЦ	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
	3. Ошибки при вводе информации	Ошибки специалистов	Технические, организационные	РНД	Внутренний
	4. Ошибки при эксплуатации программных средств	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНЦ, РНК	Внутренний
	5. Ошибки в настройках системы	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внутренний
	6. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНК	Внутренний
	7. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний, внешний
	8. Отказ системы (ввод, вывод, чтение, запись информации)	Сбои и отказы технических средств, сбои и отказы программных средств	Технические	РНД	Внутренний
	9. Утечка персональных данных	Шпионские программы, Несанкционированный доступ, Ошибки специалистов	Технические, организационные	РНД	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
BI	1. Механические повреждения устройств	Сбои и отказы технический средств	Технические	РНЦ	Внутренний
	2. Ошибки при вводе информации	Ошибки специалистов	Технические, организационные	РНЦ	Внутренний
	3. Ошибки при эксплуатации программных средств	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНЦ, РНД	Внутренний
	4. Ошибки в настройках системы	Ошибки специалистов, сбои и отказы программных средств	Технические, организационные	РНД	Внутренний
	5. Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов, Шпионские программы, Несанкционированный доступ	Организационные, технические	РНД	Внутренний
	6. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний
	7. Отказ системы (ввод, вывод, чтение, запись информации)	Сбои и отказы технических средств, сбои и отказы программных средств	Технические	РНД	Внутренний, внешний
Доступ в Internet	1. Недоступность ресурсов	Сбои и отказы технических средств, Сбои и отказы сетевого	Технические, организационные	РНЦ	Внутренний

Источники появления риска	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
		оборудования, Ошибки специалистов			
	2. Нарушение работоспособности каналов передач данных, поломки сетевого оборудования)	Сбои и отказы технических средств, Сбои и отказы сетевого оборудования,		РНД	Внутренний
	3. Хищение информации, шпионаж	Нарушение авторских прав, шпионские программы, несанкционированный доступ	Организационные, технические	РНК, РНЦ	Внутренний, внешний
	4. Умышленное внесение изменений в режимы работа устройств	Вредоносное ПО шпионские программы, несанкционированный доступ	Организационные, технические	РНК, РНЦ	Внутренний, Внешний

Приведенные таблицы классификации следует составлять для каждого направления деятельности предприятия. Они может включать большее или меньшее число информационных рисков, в зависимости от изменений, вносимых ИСП предприятия. Большая детализация информационных рисков возможна, если ввести разделение рисков в группах на подгруппы.

Таким образом, данный подход позволяет создавать гибкую классификацию информационных рисков, обеспечивая требуемую полноту и удобство практического использования. Формализованное табличное представление результатов позволяет выполнять автоматизированную обработку полученных результатов и получать необходимые сведения для дальнейшего управления информационными рисками.

Следующим этапом анализа является оценка информационных рисков. Предлагается использовать карты рисков, как основного инструмента оценки.

Для составления *карты рисков* необходимо определить ранг каждого информационного риска в списке.

Ранжирование — один из самых важных этапов работы при составлении карты рисков предприятия, после их выявления и описания.

Рангом в данном случает будет являться уровень влияния конкретного риска на деятельность предприятия при его наступлении.

Для определения ранга каждого информационного риска можно воспользоваться двумя методами:

- проведение экспертной оценку методом попарного сравнения;
- проведение анкетирования среди ведущих специалистов отделов.

Для определения ранга каждого риска предлагается проводить *анкетирование среди ведущих специалистов каждого отдела*.

В результате проведения анкетирования, можно составить карту информационного риска для основных направлений деятельности, где вертикальной осью будет являться вероятность появления информационного

риска (от 1 до 5, где 1 – вероятность крайне мала (0-20%, 5 – высокая вероятность (80-100%), а горизонтальной осью будет сила влияния данного информационного риска на деятельность предприятия (от 1 до 5, где 1 – минимальное влияние, 5 – максимальное влияние). Цветовое оформление карты рисков представлено на рисунке 8.

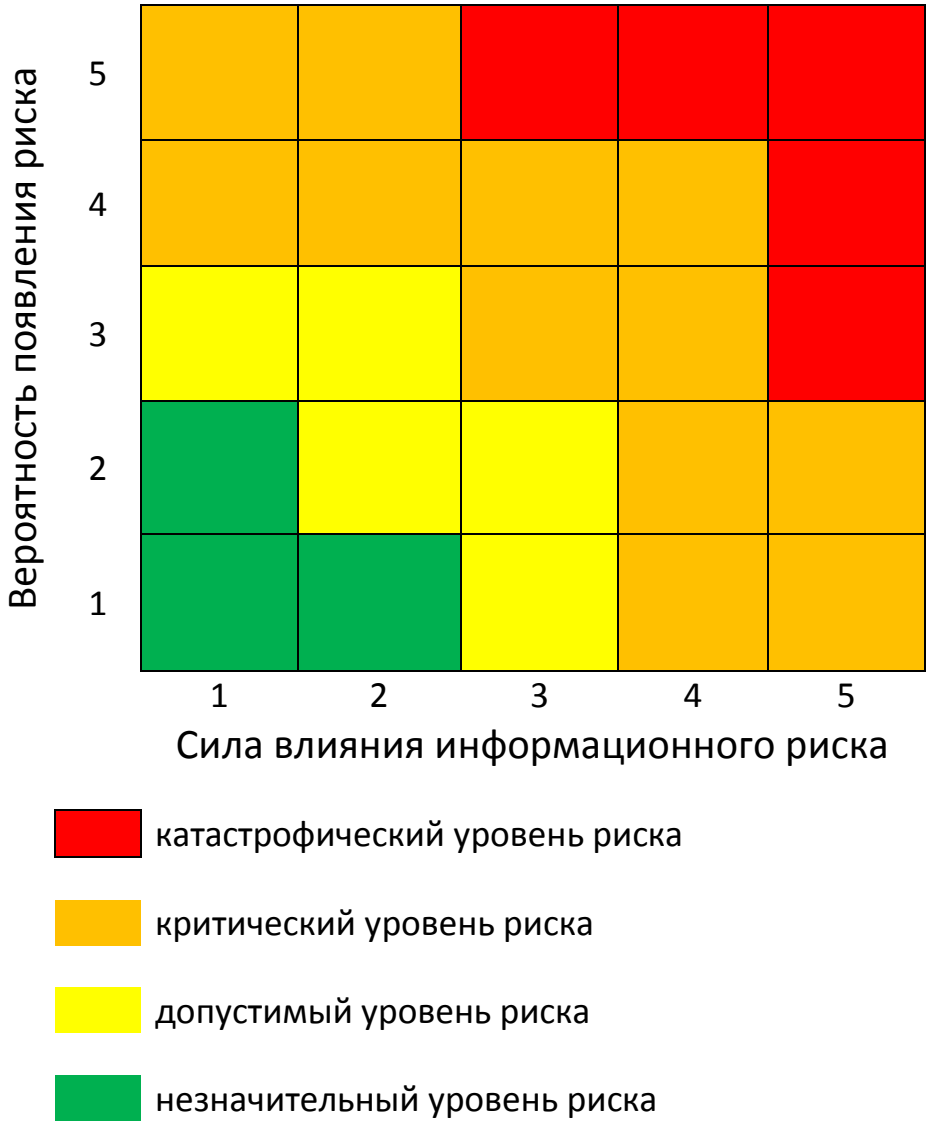

Рисунок 9 – Графическое отображение карты информационных рисков

Для лиц, принимающих решение по минимизации влияний рисков на деятельность предприятия, необходимо будет сначала применять инструменты минимизации рисков на те информационные риски, которые попадают в зону катастрофических, затем критических и допустимых рисков.

В зону *катастрофических рисков* должны попадать информационные риски, влияние которых на деятельность предприятия может оказать непоправимый ущерб. К таким рискам можно отнести стихийные бедствия, риски остановки непрерывного производства, отказ информационной системы.

К *критическим рискам* можно отнести информационные риски, влияние которых на деятельность предприятия наносит большой ущерб, но деятельность производства при их наступлении не будет остановлена. К таким рискам могут относится аварии в системах электропитания, водоснабжения, отопления, механические повреждения устройств, которые поддерживают основные функции направления деятельности.

К *допустимому уровню риска* могут быть отнесены те информационные риски, влияние которых на деятельность предприятия оказывают незначительное влияние. Частота появления таких рисков может быть высокой, но ущерб от них может не приносить ощутимого вреда для предприятия. К таким рискам могут отнситься ошибки ввода информации, неправильные действия со средствами защиты и др.

К *незначительным рискам* относятся те информационные риски, которые оказывают минимальные или вообще не оказывают вреда деятельности организации. Риски, попадающие в зону «незначительный риск» должны устраняться в последнюю очередь.

При составлении карты исков для отдельных направлений деятельности предприятия стоит учесть, что одни и те же информационные риски могут оказывать различный ущерб, в зависимости от источника появления этих рисков. Так, наступление информационного риска «отказ системы ввода вывода» в одном из узлов АСУТП может остановить линию производства и предприятие вынуждено будет прекратить выпуск продукции на этой линии, поэтому данный вид риска является катастрофическим для производственной деятельности. В то же время для отдела, занимающегося распределением потребностей производства и использующих модуль MRP,

«отказ системы ввода-вывода информации» может быть рядовой проблемой информационной системы и означать лишь проблемы с устройствами ввода-вывода на одним из компьютеров в отделе.

Пример карты рисков для, в зависимости от источника возникновения приведен на рисунке 10.

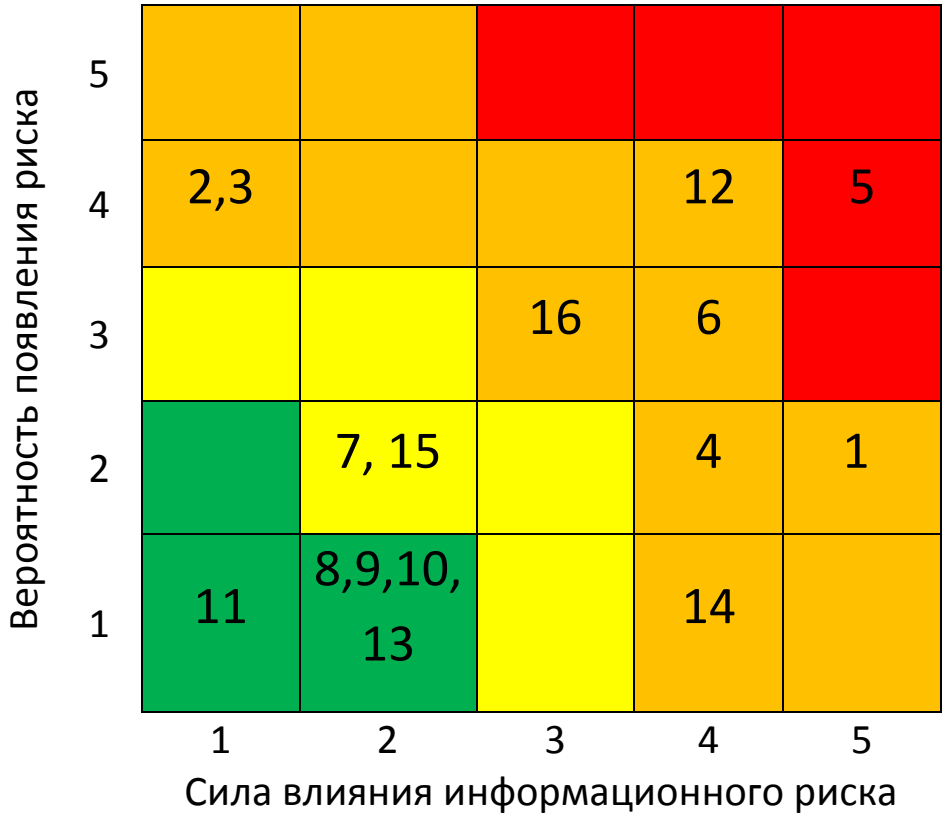

Рисунок 10 – Карта информационных рисков для АСУТП

Из карты информационных рисков для АСУТП видно, что в зону «катастрофического уровня риска» попадает риск механических повреждений устройств. В зону критического уровня риска попадают такие информационные риски: отказ системы (ввод, вывод, чтение, запись информации), нарушение работоспособности каналов передач данных, умышленное изменение в режимы работы устройств. При принятии решений по управлению рисками в первую очередь необходимо устранить минимизировать влияние именно этих типов рисков, так как именно они, по

мнению ведущих специалистов, оказывают наибольшее влияние на деятельность производства при использовании АСУТП.

Карту рисков так же необходимо обновлять с определенной периодичностью. На период обновления может влиять появление новых модулей информационных систем, которые начали использовать в деятельности предприятия, обновление версий программного обеспечения, ротация кадров в отделах и др.

В результате использование карты рисков как механизма по управлению информационными рисками на предприятии позволит создать удобный визуальный инструмент для определения влияния каждого информационного риска и определить первоочерёдность действия по минимизации влияния этих рисков.

Проведение экспертной оценки методом попарного сравнения применяется при групповом экспертном сравнивании, когда ранжирование не имеет смысла или затруднено из-за большой размерности множества объектов [32]. Результаты парного сравнения представляются в виде матрицы парных сравнений. Если экспертные оценки сравнительной предпочтительности при парном сравнении расположенных в произвольной последовательности альтернатив заданы в виде трех функций:

$$P_{i,j} = 2, \text{ если } A_i > A_j ;$$

$$P_{i,j} = 0, \text{ если } A_i < A_j ;$$

$$P_{i,j} = 1, \text{ если } A_i = A_j ,$$

то матрица парных сравнений четырех (n=4) альтернатив $A_{i,j}$ (i =1,..,n; j=1,..,n) будет иметь вид, представленный в таблице 9.

Таблица 9 – пример составления матрицы попарных сравнений альтернатив с оценками

i j	A(i=1)	A(i=2)	A(i=3)	A(i=4)
A(j=1)	1	2	0	0
A(j=2)	0	1	0	2
A(j=3)	2	2	1	2
A(j=4)	2	0	0	1

предпочтительности.

Диагональные элементы матрицы парных сравнений в соответствие с условиями всегда равны 1. Если в процедуре парных сравнений участвуют несколько экспертов, то каждый из них составляет свою матрицу.

Попарное сравнение необходимо проводить по 2 критериям – сила влияния и вероятность появления данного информационного риска.

Результат проведения попарного сравнения для отдела экономического отдела бухгалтерии, где источником риска выступает «Доступ в Internet» отображен в таблице 10 и 11.

Таблица 10 – Результаты проведения экспертной оценки для экономического отдела (сила влияния)

№ п/п	Факторы	Эксперты					Сумма	Вес	Место
		1	2	3	4	5			
1	Аварии в системе электропитания, водоснабжения, отопления	9	9	9	9	7	43	7,17	1
2	Недоступность ресурсов	5	5	5	3	5	23	3,83	4
3	Нарушение работоспособности каналов передач данных, поломки сетевого оборудования	5	5	5	9	5	29	4,83	3
4	Хищение информации, шпионаж	7	7	7	7	9	37	6,17	2
5	Умышленное внесение изменений в режимы	5	5	3	5	3	21	3,50	5

№ п/п	Факторы	Эксперты					Сумма	Вес	Место
		1	2	3	4	5			
	работа устройств								

Таблица 11 - Результаты проведения экспертной оценки для экономического отдела (вероятность появления)

№ п/п	Факторы	Эксперты					Сумма	Вес	Место
		1	2	3	4	5			
1	Аварии в системе электропитания, водоснабжения, отопления	5	5	7	5	5	27	5,40	3
2	Недоступность ресурсов	9	7	9	9	7	41	8,20	1
3	Нарушение работоспособности каналов передач данных, поломки сетевого оборудования	7	9	5	7	9	37	7,40	2
4	Хищение информации, шпионаж	5	3	3	3	3	17	3,40	4
5	Умышленное внесение изменений в режимы работа устройств	1	1	1	1	1	5	1,00	5

При перемножении значений «Место» в соответствующих строках получим таблицу очередностей применения мер по минимизации информационных рисков.

№ п/п	Факторы	Результирующее Значение	Очередность
1	Аварии в системе электропитания, водоснабжения, отопления	3	1
2	Недоступность ресурсов	4	2
3	Нарушение работоспособности каналов передач данных, поломки сетевого оборудования	6	3
4	Хищение информации, шпионаж	8	4
5	Умышленное внесение изменений в режимы работа устройств	25	5

Таблица 12 – Таблица очередности применения мер

В первую очередь меры по управлению рисками должны быть применены к тем информационным рискам, у которых очередность ниже. В экономическом отделе самыми влиятельными из рисков являются «Аварии в системе электропитания, водоснабжения, отопления», на втором месте стоят «недоступность ресурсов». Именно на эти минимизацию влияния этих информационных рисков и должны быть направлены в первую очередь методы управления информационными рисками.

Метод попарного сравнения целесообразно применять при достаточно небольшом количестве сравниваемых элементов (до 5). При большем количестве сравниваемых факторов задача становится более сложной для экспертов т.к. возрастает вероятность допустить ошибки.

Принятие решения по управлению информационными рисками является следующим этапом методического подхода к управлению.

Суть принятия решения по управлению состоит в применении системы управления информационными рисками вместе с резервными ресурсами, где в качестве резервов подразумеваются аппаратные, программные, административные, информационные и финансовые ресурсы предприятия [40].

В основу системы управления информационными рисками входит принятие решения по управлению, которая включает следующие разновидности:

- *принятие риска*, которое означает, что в отношении конкретного информационного риска не применяются никакие механизмы, инструменты предотвращения риска, не осуществляется устранение факторов, способствующих их возникновению [41];
- *предотвращение информационных рисков*, т.е. воздействие на источники рисков с целью снижения вероятности наступления рискового события;
- *минимизация ущерба* от реализации риска, которая предполагает снижение величины ущерба от информационного риска при

помощи заблаговременного внедрения и применения специальных механизмов, суть которых состоит в придании предприятию устойчивости к воздействию информационных рисков.

В общем случае процесс принятие решения по управления информационными рисками может быть представлен схематически (рисунок 10).

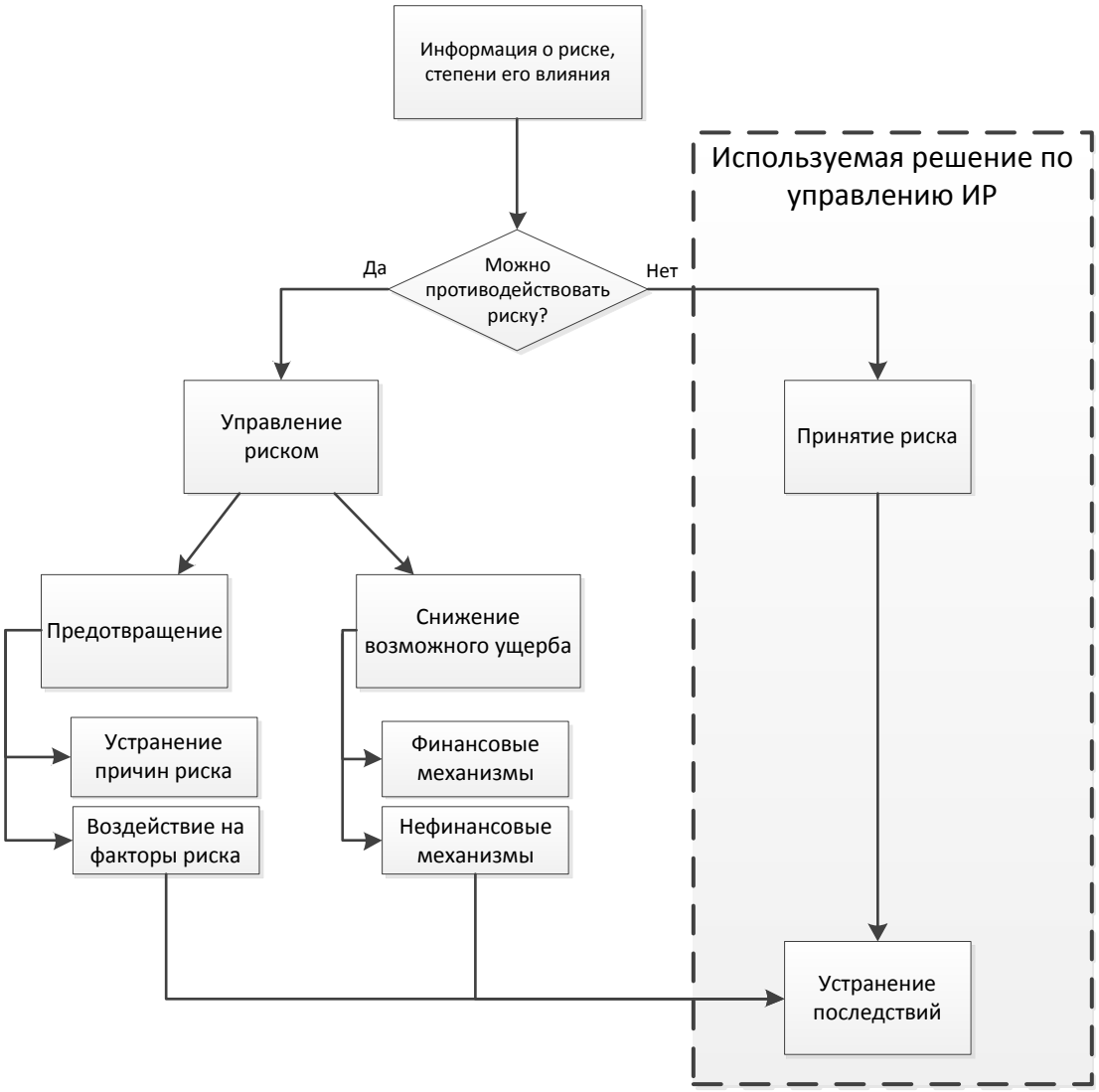

Рисунок 10 – Принятие решения по управлению информационными рисками

Таким образом, выбор решения по управлению, предполагает автономное использование такого этапа как принятие риска, и использование в комплексе таких этапов как предотвращение и снижение ущерба от информационных рисков. Реализация данной стратегии не представляется

возможным без правовых и организационных мер, которые являются приоритетными, так как именно они обеспечивают комплексное правовое использование всех остальных механизмов по управлению.

Финансовыми механизмами, позволяющими снизить ущерб от информационных рисков, являются создание резервов денежных средств и страхование информационных рисков [42]. Резервы денежных средств создаются предприятием самостоятельно или за счет паевого участия нескольких предприятий. Резерв может создаваться и за счет заемных денежных средств. Такие механизмы, как правило, используются для покрытия лишь части возможного ущерба, так как изъятие значительных сумм из оборота предприятия экономически не оправдано. Денежные резервы целесообразно использовать для решения первоочередных задач устранения последствий информационных рисков [43]. Наиболее приемлемым финансовым механизмом сокращения ущерба от информационных рисков является страхование. Отрасль страхования информационных рисков, особенно в нашей стране, пока еще находится в стадии становления. Основными сдерживающими факторами развития страхования информационных рисков являются недостаточная правовая база такого страхования, сложность определения факта наступления страхового случая по отдельным рискам, а также трудности определения размеров страховых платежей [44]. Эти трудности объясняют отсутствие общепризнанных методик проведения расчетов страхования.

К нефинансовым механизмам относятся создание резервных запасов материальных средства, включая резервное оборудование, резервирование информации создание средств оперативного обнаружения рисковых событий и локализации их воздействия на ИСП, создание организационных структур (возможно нештатных) для оценки и устранения последствий

информационных рисков, разработка планов действий и инструкций в условиях наступления рисковых событий [45].

3.2 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ МЕТОДИКИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

После идентификации информационных рисков на промышленном предприятии, проведения анализа по уровню их влияния и необходимо определиться с инструментами по их управлению.

Для эффективного управления информационными рисками необходимо недостаточно применять какой-то один метод управления. Только при комплексном использовании различных методов и средств различного типа можно добиться положительного результата в рамках единой ИСП.

Совокупность всех средств и методов управления информационными рисками можно объединить в единое понятие – механизм управления информационными рисками.

На рисунке 11 представлена классификация механизмов управления рисками. Такая классификация позволяет стандартизовать все механизмы для удобства их применения на практике.

Рисунок 11 – Механизмы управления информационными рисками.

Все средства и методы управления информационными рисками тесно взаимосвязаны между собой. Средства управления всегда применяются с использованием определенного метода управления информационными рисками, в рамках определенной технологии. Методы управления обладают большей самостоятельностью по отношению к средствам управления, и могут дополнять и усиливать технологии, основанные на применении средств управления [46]. Методы управления могут применяться самостоятельно, не опираясь на использование специальных средств управления информационными рисками.

Методы управления информационными рисками. К методам управления можно отнести, прежде всего, нормативно-правовые методы, экономические и, в значительной мере, организационные методы управления информационными рисками. Рассмотрим средства и методы управления информационными рисками подробней.

Нормативно-правовые методы управления информационными рисками образуют правовую основу построения и применения систем управления информационными рисками. На уровне предприятия использование таких методов заключается в необходимости выбора решения по управлению информационными рисками и построения СУИР в соответствии с информационным правом государства и всеми нормативными документами, в части касающейся предприятия. К нормативно-правовым документам относится, в первую очередь, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 №149-ФЗ [47]. В нем закреплены основные понятия информационного права, такие как: информация, информационные технологии, обладатель информации, конфиденциальность информации и др. Сюда же относятся действующие законы: «Об участии в международном информационном обмене» от 04.07.1996 №85-ФЗ [48]; «О государственной тайне» от 21.07.1993 №5485-1 [49]; «О коммерческой тайне» от 29.07.2004 № 98-ФЗ [50]; «О связи» от 16.02.1995 №15-ФЗ [51], «О средствах массовой информации» от 27.12.1991, «О персональных данных» от 27.07.06 №152 – ФЗ и другие. В них установлены взаимоотношения субъектов права при работе с разными видами информации в информационных системах.

К нормативно-правовым методам управления информационными рисками так же относятся российские и международные стандарты в области информационной безопасности, которые позволяют решать ряд следующих задач:

- согласование характеристик блоков ИСП для совместного бесконфликтного использования;

- оценка эффективности функционирования системы;

- взаимозаменяемость средств информатизации и информационных технологий;

При разработке системного подхода к управлению информационными рисками на предприятии все механизмы необходимо проверять на противоречивость основным законам и стандартам.

Организационные методы управления информационными рисками могут быть разделены на следующие группы:

- методы применения средств управления;
- методы непосредственного управления информационными рисками;
- методы общего менеджмента.

Реализация *методов применения средств управления* происходит с помощью создания методик, инструкций, различных графиков и схем, описания функциональных обязанностей для персонала, которые позволяют применять средства управления на практике.

Управление отдельными информационными рисками может осуществляться без применения специальных средств. Такие методы используются, если организационные методы эффективнее методов с использованием специальных средств или когда организационные методы используются в дополнение к другим механизмам в качестве примеров организационных методов управления информационными рисками, имеющих самостоятельное значение, могут служить следующие организационные методы: организация хранения носителей информации в специальных хранилищах, совместное выполнение и контроль особо ответственных операций, допуск в помещения с использованием систем контроля доступа.

Пользователи должны иметь доступ к рабочей информации в соответствии со своим уровнем компетенции согласно занимаемой должности. Перечень информационных ресурсов, к которым допущен пользователь, определяется его непосредственным начальником. При этом непосредственный начальник руководствуется инструкцией, утвержденной советом по управлению информационным рискам предприятия.

В инструкции должны быть указаны функциональные обязанности персонала по идентификации и применению методов управления информационными рисками. К таким методам должны относиться:

- обеспечение доступа на рабочие местах;
- ведение журналов;
- действия в случае обнаружения информационных рисков;

К методам общего менеджмента отнесены методы управления, которые выполняются на любом предприятии, при управлении любой системой: планирование работ, создание документации, сбор, обработка и передача управляющей информации, контроль, аудит

Экономические методы управления информационными рисками используются для обеспечения экономической эффективности применения системы управления информационными рисками. К экономическим методам управления могут быть отнесены следующие методы:

- оценки ущербов от информационных рисков;
- оптимизации общих расходов на управление информационными рисками;
- страхования информационных рисков;
- создания резервов для минимизации ущербов.

Средства управления информационными рисками в соответствии с особенностями решаемых задач могут быть разделены на три группы средств:

- средства сбора и первичной обработки информации;
- средства обеспечения качества информации в информационной системе;
- средства обеспечения безопасности информации в информационной системе.

На первом этапе использования информации в ИСП применяются *средства сбора и первичной обработки информации*. Для обеспечения

необходимого качества информации это процесс является определяющим. В соответствии с расположением источника информации, относительно информационной среды предприятия, ее условно можно разделить на внешнюю и внутреннюю. Процесс поиска информации производится с использованием следующих источников информации:

- компьютерные системы;
- телекоммуникационные системы;
- информационно-поисковые компьютерные системы;
- технические средства учета, измерений и контроля;
- средства массовой информации;
- внешние источники аналитической информации;
- специалисты, эксперты предприятия.

Внутренними источниками информации являются компьютерные системы предприятия, которые предоставляют информацию о состоянии объектов предприятия.

Телекоммуникационные системы, наряду с компьютерными системами, выполняют важную роль по получению информации от партнеров по бизнесу, клиентов предприятия, государственных и других организаций.

Важными источниками внутренней первичной информации являются технические средства учета, измерений и контроля, которые функционируют в рамках бизнес-процессов предприятия. Они обеспечивают автоматический и автоматизированный ввод данных о контролируемых процессах.

Важным источником внешней информации являются информационные ресурсы, доступ к которым возможен с помощью сети Интернет. Наиболее ценная информация в сети аккумулируется и предоставляется в пользование крупными организациями. К таким системам относят поисковые системы в глобальной сети: Google, Yahoo, Yandex и др.

Первичная информация должна быть проверена, прежде всего, на отсутствие ошибок, противоречий и дезинформации. Проверяется также актуальность информации, то есть степень ее полезности и своевременности.

Средства обеспечения качества информации применяются после сбора, ввода и первичной обработки информации. Задача этих методов обеспечить качество и безопасность информации внутри информационной системы. Ее качество на этом этапе определяется, прежде всего, ее достоверностью, актуальностью, доступностью, полнотой и формой представления.

Требования к основным характеристикам информации формируются, в основном, на этапах разработки и создания информационной системы, а так же на этапах разработки и внедрения алгоритмов и программных средств. На этапе эксплуатации необходимо контролировать соответствие требований по актуальности, полноте и форме представления информации реальным показателям внедряемых новых алгоритмов обработки информации.

Причинами получения недостоверной информации внутри информационной системы являются программные и аппаратные сбои, а также ошибки пользователей и обслуживающего персонала.

Основным направлением борьбы с утратой достоверности информации является использование развитой аппаратно-программной системы контроля доступа к информационной среде предприятия.

Одной из наиболее сложных проблем остается проблема ошибок персонала информационной системы, неумышленные ошибочные действия персонала остаются основной причиной снижения качества информации.

Современные технологии оказывают двойственное воздействие на процессы взаимодействия человека и информационных систем. С одной стороны, взаимодействие человека с техническими системами становится более комфортным. С другой - постоянно возрастают объемы информации и интенсивность информационных процессов, возрастают масштабы негативных последствий ошибок человека.

Для снижения количества ошибок персонала информационных систем предлагается обеспечить следующее:

- комфортное оборудование рабочих мест;
- дружественный интерфейс человека с техническими системами;
- оптимальный режим труда и отдыха;
- обучение пользователей и персонала;

Средства обеспечения безопасности информации направлены на минимизацию информационных рисков, связанных с нарушением 3 основных аспектов информационной безопасности информационной системы предприятия [53]. На рисунке 12 приведены 3 основные составляющие безопасности информации

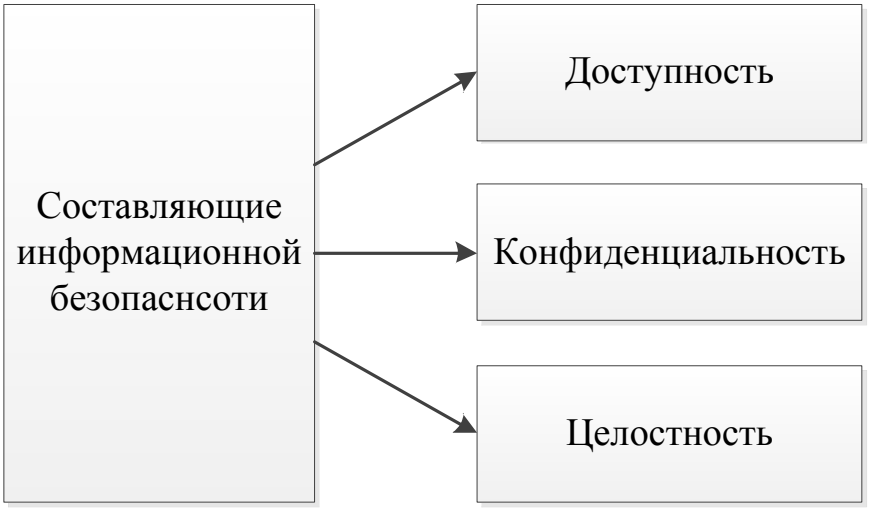

Рисунок 12 – Составляющие информационной безопасности

Риск нарушения доступности информации может зависеть как от неисправности оборудования и сбоев в программном обеспечении в компании, так и от успешно реализованных сетевых атак на информационную систему от внешних источников.

Данный тип риска напрямую зависит от надежности аппаратных и программных компонентов информационной системы, а так же от уровня компетенций персонала, управляющего их работой. Нарушение доступности так же возникают из-за несоблюдения требований различных стандартов как

на этапе проектирования так и на этапах производства или эксплуатации системы.

Под целостностью понимается актуальность и непротиворечивость информации, уровень ее защиты от разрушения и несанкционированного изменения и удаления.

Риск нарушения целостности обеспечивается вероятностями отказа оборудования и программного обеспечения, степенью продуманности алгоритмов и надежностью средств доступа пользователей системы, имеющих право на редактирование информации, вероятностью наличия в системе недокументированных возможностей, несовершенством организационной структуры ИС, а так же несоблюдением требований стандартов на этапе проектирования, производства и эксплуатации системы.

Под конфиденциальностью понимается уровень защиты информации от несанкционированного доступа.

Риск нарушения конфиденциальности так же зависит от уровня алгоритмов аутентификации пользователей, вероятностью наличия недокументированных ситуаций при работе с ИС, несовершенством организационной структуры, несоблюдением стандартов и человеческим фактором.

Применяемые механизмы обеспечения безопасности информации целесообразно распределить по видам в зависимости от физической сущности рисковых событий, особенностей информационных ресурсов, объектов и субъектов, с которыми связаны риски, а также от специфики применяемых средств и методов.

Предлагается использовать следующую классификацию механизмов обеспечения информационной безопасности:

- средства охраны и управления доступом;
- средства обеспечения информационной безопасности при работе с немашинными носителями информации и конфиденциальными производственными образцами, материалами и технологиями;

- средства разграничения доступа к компьютерной информации;
- средства защиты от электромагнитных излучений и наводок;
- специальные средства защиты от инсайдеров.

Создание организационной структуры. В основе использования СУИР на промышленных предприятиях лежит создание организационной структуры, основной целью которой является координация управления деятельности по управлению информационными рисками на предприятии. Анализ решаемых задач и принципов управления информационными рисками показывает, что целесообразнее всего объединять в единую систему все элементы предприятия, участвующие в управлении информационными рисками.

Создание организационно-правовой структуры СУИР возможно при взаимодействии определенных методов, принципов и средств.

В основу организационно-правовой структуры положены нормативно-правовые и организационные методы [37]:

a) Нормативно-правовые методы управления информационными рисками образуют правовую основу построения и применения систем управления информационными рисками. К нормативно-правовым методам управления информационными рисками относятся российские и международные стандарты в области информационной безопасности, которые позволяют решать ряд следующих задач: во-первых, согласование характеристик блоков ИСП для совместного бесконфликтного использования; во-вторых, оценка эффективности функционирования системы; в-третьих, взаимозаменяемость средств информатизации и информационных технологий. На уровне предприятия использование таких методов заключается в необходимости выбора политики управления информационными рисками и построения СУИР в соответствии с информационным правом государства и всеми нормативными документами, в части касающейся предприятия.
b) Организационные методы могут быть разделены на следующие группы:

- методы применения средств управления (создание методик, инструкций, различных графиков и схем, описания функциональных обязанностей для персонала, которые позволяют применять средства управления на практике);

- методы непосредственного управления информационными рисками (организация хранения носителей информации в специальных хранилищах, совместное выполнение и контроль особо ответственных операций, допуск в помещения с использованием систем контроля доступа);

- методы общего менеджмента (планирование работ, создание документации, сбор, обработка и передача управляющей информации, контроль, аудит.).

Применение вышеперечисленных методов при реализации организационно-правой структуры СУИР основывается на следующих принципах:

1. Принцип централизации, заключающийся в передаче/ делегировании

прав и ответственности за ряд ключевых решений на нижние уровни управления организацией. Учитывая вес информационных рисков, руководители предприятий уже не могут полагаться на готовые решения службы безопасности, информационного, аналитического отделов и некоторых других служб и отделов. Для интеграции усилий различных подразделений предприятия, направленных на эффективное управление информационными рисками необходимо непосредственное участие первых лиц предприятий в выработке политики управления информационными рисками, руководители предприятий должны использовать имеющиеся в их распоряжении механизмы автоматизированного контроля деятельности руководителей отделов и служб, возглавлять работу по анализу эффективности СУИР, участвовать в обсуждении и принятии решений по совершенствование системы. Без жесткой централизации невозможна

эффективная реализация единой политики управления информационными рисками. Роль централизации управления возрастает на предприятиях, которые имеют удаленные филиалы, дочерние компании и тому подобные удаленные подразделениям практическая реализация централизованного управления на таких предприятиях требует решения целого ряда сложных технических и организационных проблем.

2. Иерархический принцип, который заключается в распределении функций управления между соподчиненными частями системы, т.е. обобщённые

управляющие сигналы подсистем высшего уровня поступают для

управления подчинёнными подсистемами, и наоборот, —

конкретные осведомительные и задающие сигналы низших уровней иерархи

и используютсядля формирования управляющих сигналов вышестоящих.

Иерархический принцип управления позволяет построить рациональную систему, в которой исключены потоки информации не соответствующие уровню компетентности органа управления.

Организационно-правовая структура по управлению информационными рисками представляет собой коллегиальный орган управления на которую возложена функция ведения политики предприятия по минимизации и управлению информационными рисками в организации – Совет по управлению информационными рисками (рисунок 8).

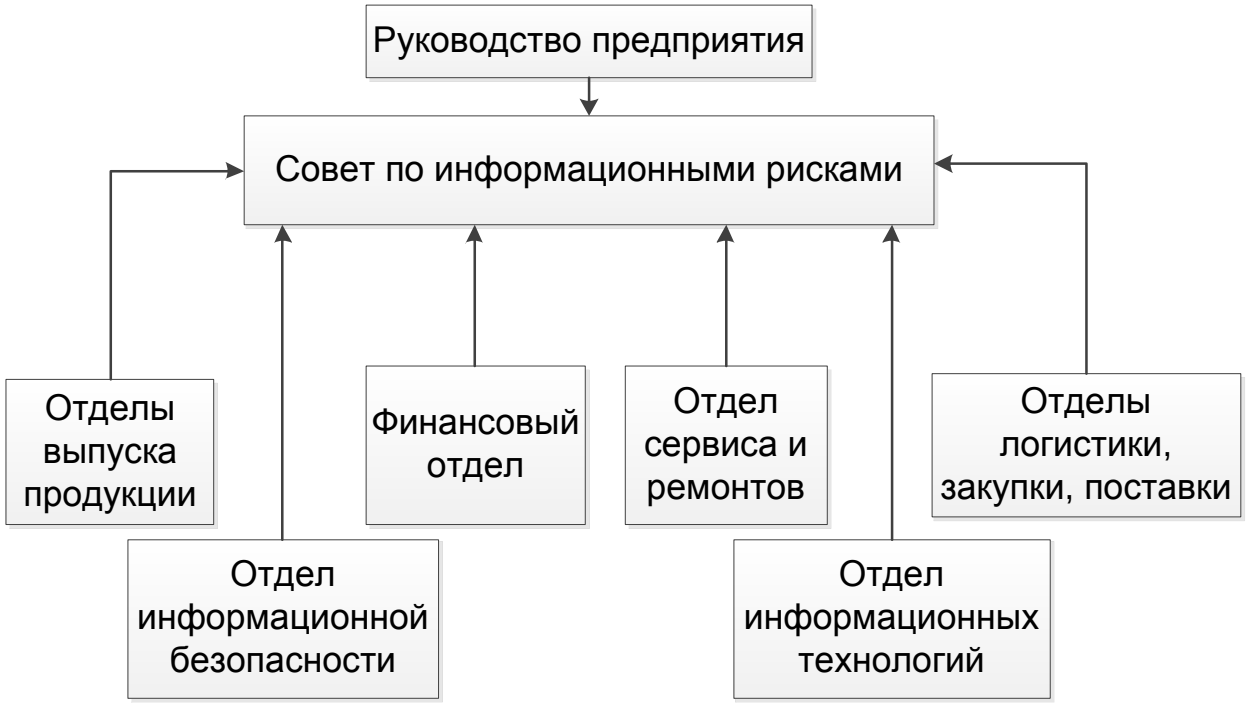

Рисунок 8– Пример схемы совета по информационным рискам (на примере ООО «ВИЗ-Сталь»)

Совет собирается для подготовки к принятию решений по стратегическим вопросам управления информационными рисками, обсуждения текущих важнейших проблем информационной политики. К компетенции совета может быть отнесено решение следующих задач:

- подготовка программа управления информационными рисками предприятия;

- оценка степени соответствия реального состояния информационной безопасности;

- внесение и обсуждение предложений по совершенствованию программы и системы управления информационными рисками;

- обсуждение и выработка предложений по ликвидации последствий крупных инцидентов информационной сфере предприятия.

Основными направления деятельности совета будет создание руководящих и стратегических документов предприятия по управлению информационными рисками. Основой для них станет нормативно-правовые акты, которые позволят создавать безопасные с точки зрения доступности,

конфиденциальности и целостности данные систем на предприятии, эффективного использования этих систем.

Возглавляет систему управления информационными рисками руководитель предприятия. Непосредственное руководство может осуществляться одним из заместителей руководителя. Совет является нештатным совещательным органом при руководстве предприятия. В его состав входят руководитель и заместители руководителя предприятия, руководители отделов информационных технологий и информационной безопасности, основных бизнес-процессов, а также ведущие специалисты предприятия.

Отдел информационных технологий осуществляет технического эксплуатации компьютерных систем, систем связи и оргтехники предприятия. Отдел обеспечивает качество и безопасность данных с момента их ввода в ИСП до получения информации на выходе технических средств. При этом безопасность информации обеспечивается отделом информационных технологий совместно с отделом информационной безопасности. В состав отдела входят специалисты по эксплуатации программных и технических средств.

Отдел информационной безопасности обеспечивает безопасность информации предприятия. Отдел организует и координирует действия сотрудников всех отделов информационного направления и всех менеджеров предприятия по вопросам обеспечения безопасности в соответствии нормативно-правовыми актами Российской Федерации, международными стандартами в области информационной безопасности, а так же нормативными документами самого предприятия. Наиболее тесное сотрудничество отдел осуществляет с отделом информационных технологий и службой охраны.

Для эффективной работы совета необходимо:

- четкое определение функциональных обязанностей сотрудников привлекаемых к работе в составе таких органов;

- заранее разработанные схемы управления и взаимодействия специалистов;

- подготовка специалистов к работе в составе не штатного объединения;

- всестороннее обеспечение работы нештатных органов.

Таким образом, предлагаемая организационная структура совета по управлению информационными рисками на промышленных предприятиях позволит обеспечить выполнение организационно-правовых, экономических и организационных методов управления информационными рисками на предприятии.

ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ

Для управления информационными рисками на предприятии ООО «Виз-Сталь» в работе предложено использовать комплексный подход к управлению информационными рисками, на основе системы менеджмента качества (СМК), используемого на предприятии. Основной целью данного подхода - минимизации влияния существующих информационных рисков на деятельность ООО «Виз-Сталь», достигается путем практического применения следующих положений,

- в разработке организационно-правовой структуры по управлению информационными рисками, представляющей собой коллегиальный орган управления (Совет по управлению информационными рисками) на который возложена функция ведения политики предприятия по минимизации и управлению информационными рисками в организации;

- в применении основных способов анализа информационных рисков, а именно:

  - индексной классификации информационных рисков,
  - карты рисков;

- в выработке стратегии управленческой деятельности при возникновении угрозы информационного риска;

- в комплексном применении механизмов управления информационными рисками на предприятии

Таким образом, применение разработанной концепции системы управления рисками в деятельности предприятий позволит, во-первых, вовремя обнаруживать информационную угрозу; во-вторых, своевременно воздействовать на факторы и причины информационных рисков и минимизировать ущерб от их наступления.

ЗАКЛЮЧЕНИЕ

Для разработки методического подхода была изучена сущность информационных рисков, определен источник их появления, разработана классификация информационных рисков по различным критериям, изучены методы анализа и управления рисками.

С целью изучения роли информационных рисков в деятельности промышленных предприятий был проведен анализ статистических данных по использованию информационных технологий, выявлены тенденции роста расходов предприятий на модернизацию информационного комплекса.

Для анализа эффективности управления информационными рисками было проведено анкетирование среди руководителей, менеджеров различных отделов, IT-специалистов, который показал, что не смотря на присутствие информационных рисков в деятельности предприятий, отсутствует методика по управления ими.

С целью изучения воздействия информационных рисков на деятельность промышленных предприятий, проанализировано предприятие ООО «ВИЗ-Сталь». Установлено негативное влияние информационных рисков на деятельность предприятия, которое выражается во времени простоя оборудования информационных систем в различных отделах, вызванного наступлением информационных рисков.

Для целей минимизации влияния существующих информационных рисков на деятельность промышленных предприятий, предложен методический подход к внедрению системы управления информационными рисками (СУИР).

Для обеспечения результативности использования СУИР на промышленных предприятиях, необходима методика управления информационными рисками, которая включает в себя анализ информационных рисков, принятие решения по управлению, комплексное использование механизмов управления. Для проведения анализа, как

ключевого этапа методики, предложено использование классификационных таблиц, составленных на основе авторской классификации информационных рисков, а так же составление карт рисков, как удобного графического инструмента для определения влияния каждого риска.

Для обеспечения реализации методики управления информационными рисками определены материальные и нематериальные инструменты управления, а так же, для координации действий по управлению рисками предложен вариант организационной структуры.

Таким образом, в работе разработана методика, которая позволяет идентифицировать информационные риски, установить степень их влияния на деятельность промышленных предприятий и снизить вероятность их наступления.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Cnews аналитика http://www.cnews.ru/ [Электронный ресурс]
2. Искусство управления http://анализ-риска.рф [Электронный ресурс]
3. Искусство управления информационной безопасностью http://iso27000.ru/ [Электронный ресурс]
4. Мескон М., Альберт М., Хедоури Ф. Основы менеджмента
5. Найт Ф. Понятие риска и неопределенности // Thesis: теория и история экономических и социальных институтов и систем. 1994. № 5.
6. Луман Н. Понятие риска // Thesis: теория и история экономических и социальных институтов и систем. 1994. № 5.
7. Долматов А.С. Математические методы риск-менеджмента: учеб. пособие. – М.: Экзамен, 2007. – 319 с.
8. Менеджмент качества http://www.kpms.ru/Automatization [Электронный ресурс]
9. Управление рисками на предприятии. http://www.risk24.ru/ [Электронный ресурс]
10. Исаев Г.Н. Информационные технологии: учебное пособие М: Омега-Л, 2012, 464 с.
11. Активы организации как ключевые факторы риска http://анализ-риска.рф [Электронный ресурс]
12. Берлимер Б. Риски в современном бизнесе. – М.: Аланс, 1994. – 200 с.
13. Мазов Н.А., Ревнивых А.В., Федотов А.М. Классификация рисков информационной безопасности: Вестник НГУ. Серия: Информационные технологии, 2011. Том 9, выпуск 2, С.80-89.
14. Виды и классификация рисков. http://www.risk24.ru/ [Электронный ресурс]

15. Классификация и проблемы оценки рисков промышленного предприятия Интернет-журнал «Науковедение» ISSN 2223-5167. http://naukovedenie.ru/ [Электронный ресурс]

16. Варфоломеев А.А. Управление информационными рисками. Учебное пособие М.: РУДН, 2008. – 158 с.

17. Экономический анализ http://economics.studio [Электронный ресурс]

18. Управление, управление рисками на предприятии. http://www.risk24.ru/ [Электронный ресурс]

19. Метод экспертных оценок. http://center-yf.ru/ [Электронный ресурс].

20. Круи М., Галай Д., Марк Р. Основы риск-менеджмента. – М.: Юнити, 2011. – 400 с.

21. Хохлов Н.В. Управление риском. М.: Юнити – Дана, 1999. 239 с.

22. О.И. Дегтярева. Управление рисками в международном бизнесе

23. Методы компенсации рисков http://www.risk24.ru/ [Электронный ресурс]

24. Владимиров В.А., Воробьев Ю.Л., Малинецкий Г.Г. Управление риском. Риск, устойчивое развитие, синергетика. М.: Наука, 2000

25. А. Вепринцев. Управление рисками при автоматизации [Электронный журнал Управляем предприятием № 3 (26)]

26. Бастриков М.В., Пономарев О.П. Информационные технологии управления

27. Атапина Н.В. Сравнительный анализ методов оценки рисков и подходов к организации риск-менеджмента / Н.В. Атапина, В.Н. Кононов // Молодой учёный. Ежемесячный научный журнал. - 2013 - №5.

28. Лапуста М. Риски в предпринимательской деятельности / М. Лапуста // – М.: Дело и Сервис, 2009

29. Результаты IT-расходов [Электронный ресурс]: электронный журнал об информационных технологиях C-News. URL:

http://www.cnews.ru/news/top/2016-01-18_mirovye_itrashody (дата обращения: 17.04.2017)

30. Статистика по затратам промышленных предприятий на развитие информационных технологий [Электронный ресурс]: данные Росстата. URL: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/enterprise/industrial/ (дата обращения: 21.04.2017)

31. Статистика по затратам промышленных предприятий на развитие информационных технологий [Электронный ресурс]: данные Росстата. URL: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/enterprise/industrial/ (дата обращения: 21.04.2017)

32. Экспертный журнал по информационной безопаснсоти Безопасник [Электронный ресурс]. URL: http://bezopasnik.org (дата обращения: 22.04.2017)

33. Вдовенко Л.А. Информационная система предприятия. Учебное пособие. – М.: Инфра, 2015, 304 с.

34. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. − М.: АйТи-Пресс, 2004. − 384 с.

35. Дэниел О'Лири. ERP-системы Современное планирование и управление ресурсами предприятия. – М.: Вершина, 2004. – 272 с.

36. Официальный сайт ООО «Виз-Сталь» [Электронный ресурс]. URL: http://viz-steel.nlmk.com/ru/ (дата обращения: 22.04.2017)

37. Виз-Сталь [электронный ресурс]: Википедия. Свободная энциклопедия. URL: https://ru.wikipedia.org (дата обращения: 20.04.2017)

38. Правовые и организационные методы защиты [Электронный ресурс]: электронный журнал об информационных технологиях C-News. URL: http://studopedya.ru/1-49144.html (дата обращения: 05.05.2017)

39. Словарь терминов антикризисного управления [Электронный ресурс]: Академический словарь Академик URL: http://dic.academic.ru/dic.nsf/anticris/73782 (дата обращения: 10.05.2017)

40. Завгородний В.И. Системное управление информационными рисками. Выбор механизмов защиты от информационных рисков [Текст] /В.И. Завгородний //Проблемы управления. - 2009. - №1 - С.53-58.

41. Методы управления экономическими рисками [Электронный ресурс]: электронный журнал Информатика для экономистов URL: http://studme.org/53395/informatika/metody_sredstva_zaschity_informatsii_kompyuternyh_sistemah (дата обращения: 26.04.2017)

42. Результаты IT-расходов [Электронный ресурс]: электронный журнал об информационных технологиях C-News. URL: http://www.cnews.ru/news/top/2016-01-18_mirovye_itrashody (дата обращения: 17.04.2017)

43. Статистика по затратам промышленных предприятий на развитие информационных технологий [Электронный ресурс]: данные Росстата. URL: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/enterprise/industrial/ (дата обращения: 21.04.2017)

44. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. − М.: АйТи-Пресс, 2004. − 384 с.

45. Экспертный журнал по информационной безопасности Безопасник [Электронный ресурс]. URL: http://bezopasnik.org (дата обращения: 22.04.2017)

46. Беспалов П.В. Информационная политика: учебник / П.В. Беспалов, В.Б. Вепринцев, В.В.; под общей ред. В.А. Попова [Текст]. -М.: Издательство РАГС, 2003. - 460 с.

47. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.06 №149-ФЗ [Текст] // Собрание законодательства РФ, 13.10.1997

48. Закон Российской Федерации "О государственной тайне" от 21.07.93 № 5481-1 с изменениями и дополнениями, внесенными 6.10.97 № 131-ФЗ, Собрание законодательства РФ, 13.10.1997, N 41, стр. 8220-8235.

49. Закон Российской Федерации "О государственной тайне" от 21.07.93 № 5481-1 с изменениями и дополнениями, внесенными 6.10.97 № 131-ФЗ [Текст] // Собрание законодательства РФ, 13.10.1997, N 41, стр. 8220-8235.

50. Закон Российской Федерации "О коммерческой тайне" от 12.03.94 № 36-ФЗ

51. Закон Российской Федерации «О связи» от 16.02.1995 №15-ФЗ.

52. Закон Российской Федерации «Об авторском праве и смежных правах» от 09.07.1993 № 5351-1

53. Кузнецов Н.А. Информационная безопасность систем организационного управления. Теоретические основы. М.: Наука, 2006.-Т.1-495 с.

ПРИЛОЖЕНИЕ 1 – АНКЕТА ДЛЯ ИССЛЕДОВАНИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

Анкетирование проводится с целью сбора данных по использованию системы управления информационных рисков на промышленных предприятиях. На основании собранных сведений производится анализ по уровню управления информационными рисками на предприятии.

Информационный риск - это опасность возникновения убытков или ущерба в результате применения информационных технологий на предприятии. IT-риски связаны аппаратной частью (компьютеры, серверы, датчики и тд.), программным обеспечением, каналами передач данных, а так же персоналом, который непосредственно работает с информационными технологиями на предприятии.

IT-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи.

1. Организация
   _____
2. Занимаемая должность в организации?
   _____
3. Штат сотрудников предприятия (отдела)?
   _____

Управление рисками

1. Существует ли на предприятии система управления рисками?
   А. да, существует
   Б. нет, не существует
   В. а что это??

2. Какой стандарт по управления рисками применяется у вас на предприятии?
   А. никакой стандарт не применяется
   Б. применяется, но не знаю какой
   В. FERMA
   Г. ISO 31000 – 2009 (ГОСТ Р ИСО/МЭК 31010 – 2011)
   Д. COSO II
   Е. Базель II

Ж. другой (напишите название, если знаете)

_____

3. Определен ли подход к оценке рисков в организации?
   А. да, определен
   Б. нет
   В. не знаю

4. Имеются ли в Вашей организации документы, регламентирующие политику управления рисками?
   А. да, имеются (если знаете название, то напишите)

   _____

   Б. нет таких документов
   В. не знаю

5. Разработан ли в организации план обработки рисков, в котором идентифицированы соответствующие действия персонала ответственность при управлении рисками?
   А. да, разработан
   Б. нет, не разработан
   В. не знаю
6. Установлены ли возможные варианты обработки рисков?
   А. да, разработаны
   Б. нет, не разработаны
   В. не знаю

7. Проводится ли регулярный анализ результативности управления рисками в организации?
   А. да, проводится
   Б. нет, не проводится
   В. не знаю

8. Проводится ли в Вашей организации анализ инцидентов в области управления рисками с последующим привлечением виновных к дисциплинарной ответственности?
   А. да, проводится анализ и наказываются виновные
   Б. да, проводится анализ, но виновные не наказываются
   В. нет, анализ не проводится

Информационные риски

1. Знакомы ли Вы с понятием «Информационные риски»?
   А. да, знакомы
   Б. нет, не знакомы

2. Оцените вероятность каждого из информационных рисков у Вас на предприятии (от 0 до 5, где 0 – нет рисков, 5 – вероятнее всего проявится)

а). ошибки специалистов при работе с IT — 0 1 2 3 4 5

б). сбои и отказы технических средств — 0 1 2 3 4 5

в). сбои и отказы сетевого оборудования — 0 1 2 3 4 5

г). сбои и отказы программных средств — 0 1 2 3 4 5

д). вредоносное ПО — 0 1 2 3 4 5

е). шпионские программы — 0 1 2 3 4 5

ж). несанкционированный доступ — 0 1 2 3 4 5

з). нарушение авторских прав — 0 1 2 3 4 5

и). распространение ложной информации — 0 1 2 3 4 5

к). аварии — 0 1 2 3 4 5

3. Применяется ли какой-то стандарт в области управления информационными рисками у вас на предприятии?
   А. да, применяется (если знаете название, то напишите)
   _____
   Б. нет, не применяется
   В. не знаю

4. Идентифицированы ли информационные риски (риски информационной безопасности) в организации?
   А. да, идентифицированы
   Б. нет, не идентифицированы
   В. не знаю

5. Анализируются и оцениваются ли информационные риски?
   А. анализируются и оцениваются
   Б. только анализируются
   В. не оцениваются и не анализируются

6. Проводится ли в Вашей организации обучение персонала порядку действия и обработке в случаях выявления информационных рисков?
   А. да, обучение проводится
   Б. нет, не проводится
   В. не знаю

7. Учитываются ли вопросы управления информационными рисками при стратегическом и оперативном планировании на Вашем предприятии?
   А. да, учитываются
   Б. нет, не учитываются

8. Производится ли проверка всех внедряемых в информационную систему Вашей организации компонентов на взаимную совместимость с существующими?
   А. да, проводится;
   Б. проводится, но не со всеми;
   В. нет, не проводится

Информационная безопасность

1. Вырабатываются ли на основе анализа инцидентов в области информационной безопасности последующие рекомендации, методики анализа и минимизации рисков?
   А. да, вырабатываются

Б. нет, не вырабатываются

2. Проводится ли в Вашей организации анализ инцидентов в области информационной безопасности?
   А. да, проводится
   Б. нет, не проводится
   В. не знаю

3. Проводится ли регулярное обучение, повышение квалификации и проверка уровня подготовки персонала Вашей организации в области информационной безопасности?
   А. да, обучение проводится
   Б. нет, обучение не проводится

4. Включены ли в должностные инструкции сотрудников Вашей организации права и обязанности, касающиеся информационной безопасности, такие как порядок обработки и обращения с информацией ограниченного доступа, в том числе информацией конфиденциального характера?
   А. да, включены
   Б. нет, не включены

5. Имеется ли в Вашей организации подразделение по защите информационных ресурсов или лица, отвечающие за обеспечение информационной безопасности?
   А. да
   Б. нет
   В. не знаю

6. Прописаны ли функциональные обязанности должностных лиц, обеспечивающих безопасность информации в Вашей организации?
   А. да, прописаны
   Б. нет, не прописаны

7. Предусмотрена ли ответственность за нарушение политики информационной безопасности сотрудниками Вашей организации?
   А. да, предусмотрена
   Б. нет, не предусмотрена

ПРИЛОЖЕНИЕ 2 – ПРИМЕР АНКЕТЫ ДЛЯ ЭКСПЕРТОВ ПРЕДПРИЯТИЯ (ИСТОЧНИКОМ РИСКОВ ЯВЛЯЕТСЯ АСУТП)

Анкетирование проводится с целью установления силы влияния каждого информационного риска на деятельность предприятия. Анкета состоит из 2-х вопросов: в перовом, необходимо оценить вероятность появления каждого из информационных рисков, во втором – силу влияния информационного риска.

1. Оцените вероятность появления каждого из информационных рисков у Вас на предприятии, которые находятся в таблице 1(от 1 до 5, где 1 – нет рисков, 5 – вероятнее всего проявится)

Таблица 1 – Оценка вероятности появления информационных рисков

Информационный риск	Вероятность возниконовения информационного риска
1. Механические повреждения устройств	1 2 3 4 5
2. Аварии в системе электропитания, водоснабжения, отопления	1 2 3 4 5
3. Ошибки при вводе информации через ПК	1 2 3 4 5
4. Ошибки при эксплуатации программных средств	1 2 3 4 5
5. Ошибки при работе с носителями информации	1 2 3 4 5
6. Неправильные действия со средствами защиты информации	1 2 3 4 5
7. Непреднамеренное разглашение конфиденциальной информации	1 2 3 4 5
8. Отказ системы (ввод, вывод, чтение, запись информации)	1 2 3 4 5
9. Хищение информации, шпионаж	1 2 3 4 5
10. Умышленное внесение изменений в режимы работа устройств	1 2 3 4 5
11. Блокировка систем защиты	1 2 3 4 5

2. Оцените силу влияния каждого из информационных рисков на деятельность Вашего предприятия, которые находятся в таблице 2 (от 1 до 5, где 1 – нет рисков, 5 – вероятнее всего проявится)

Таблица 2 – Оценка силы влияния информационных рисков

Информационный риск	Сила влияния информационного риска
1. Обрушение зданий	1 2 3 4 5
2. Механические повреждения устройств	1 2 3 4 5
3. Аварии в системе электропитания, водоснабжения, отопления	1 2 3 4 5
4. Ошибки при вводе информации через ПК	1 2 3 4 5
5. Ошибки при эксплуатации программных средств	1 2 3 4 5
6. Ошибки при работе с носителями информации	1 2 3 4 5
7. Неправильные действия со средствами защиты информации	1 2 3 4 5
8. Непреднамеренное разглашение конфиденциальной информации	1 2 3 4 5
9. Отказ системы (ввод, вывод, чтение, запись информации)	1 2 3 4 5
10. Хищение информации, шпионаж	1 2 3 4 5
11. Умышленное внесение изменений в режимы работа устройств	1 2 3 4 5
12. Блокировка систем защиты	1 2 3 4 5