Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, управления и природопользования
кафедра финансов

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И.С. Ферова
подпись

«_17_» __06___ 2020 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ(НА ПРИМЕРЕ ООО «ТРАНСНЕФТЬ-ВОСТОК»)

Научный руководитель _____ канд. экон. наук, доцент Е.А. Шнюкова
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ К.О.Ничипуренко
подпись, дата инициалы, фамилия

Рецензент _____ нач. отдела сырья и соб-го МТО АО «РУСАЛ Менеджмент»
подпись, дата должность М.С. Толмачёв
инициалы, фамилия

Красноярск 2020

РЕФЕРАТ

Выпускная квалификационная работа по теме «Анализ и оценка информационной составляющей экономической безопасности предприятия на примере ООО «Транснефть-Восток»)» и содержит 88 страниц текстового документа, 6 иллюстраций, 10 таблиц, 5 формул, 4 приложения, 55 использованных источника.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТЬ АКТИВОВ, МЕТОДЫ ОЦЕНКИ РИСКОВ.

Предмет исследования – методические подходы к оценке информационных рисков.

Объектом исследования является Общество с ограниченной ответственностью «Транснефть-Восток».

Цель анализ информационной безопасности и разработка рекомендации по снижению информационных рисков.

В соответствии с поставленной целью были изучены теоретические и методические основы оценки рисков информационной составляющей экономической безопасности предприятия; проанализировано состояние информационной безопасности предприятия на сегодняшний день, осуществлена оценка методических подходов, используемых на предприятии для обеспечения информационной защищенности, проведён анализ критериев, используемых для оценки рисков информационной безопасности, дана оценка уровня рисков для активов предприятия.

Под результатами исследования понимается предложение рекомендаций по созданию методики, позволяющей определять защищенность системы информационной безопасности и производить расчет рисков информационной безопасности. Эта методика направлена на систематизацию данных и определение необходимых направлений защиты.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современных рыночных условиях экономической безопасности хозяйствующего субъекта уделяется все больше внимания и в научной литературе, и в практической предпринимательской деятельности. Разного рода риски, которые существуют в России и за рубежом, оказывают дестабилизирующее воздействие на экономику, которое отражается на функционировании предприятия.

Особое внимание уделяется информационной безопасности, как одной из составляющих экономической безопасности предприятия. На сегодняшний день у хозяйствующих субъектов возникает стремление единоличного обладания информационными ресурсами и технологиями, применения их для удовлетворения своих потребностей и противодействия интересам конкурентов. При этом информация и информационные технологии начинают выступать в качестве объектов угроз, порождая проблему информационной безопасности. В связи с этим тема исследования сущности и содержания информационной безопасности особенно актуальна в современных условиях.

Целью дипломной работы является анализ информационной безопасности предприятия и разработка рекомендации по снижению информационных рисков.

Объект исследования данной работы – Общество с ограниченной ответственностью «Транснефть-Восток».

Предметом исследования являются методические подходы к оценке информационных рисков

Для достижения поставленной цели необходимо решить следующие задачи:

– изучить понятие, принципы и задачи экономической безопасности предприятия;

– рассмотреть основные элементы экономической безопасности предприятия;

– изучить характеристику и сущность информационной составляющей экономической безопасности;

– провести анализ критериев, используемых для оценки рисков информационной безопасности;

– провести сравнительный анализ методических подходов и инструментария для оценки информационных рисков;

– привести обоснование выбора методов оценки рисков информационной безопасности;

– дать краткую характеристику ООО «Траснефть-Восток» и его основных направлений информационной безопасности;

– провести оценку методических подходов, используемых на предприятии для обеспечения информационной защищенности;

– разработать методику оценки информационных рисков для ООО «Траснефть-Восток».

Научная новизна представленного исследования состоит в разработке средств и методов обеспечения информационной безопасности предприятия путем выявления и оценки угроз конфиденциальности информации предприятия, проведения планирования и расчета информационных рисков.

Практическая значимость работы заключается в ее результатах, позволяющих повысить уровень защиты информации на предприятии за счет применения предложенных методов при формировании системы информационной безопасности, способствующей снижению информационных рисков.

В качестве методологических основ проведения исследований в сфере информационной составляющей экономической безопасности выступают современные теории, научные труды ученых по вопросам повышения информационной и экономической безопасности предприятия, а также законодательные и нормативные акты по вопросам экономической

безопасности. Теоретико-методологическим основам экономической безопасности посвящены работы А.В. Бабаш, В.В. Гафнер, Н.И. Глухова, Ю.Ю. Громова, Д.А. Мельникова, В.Ф. Шаньгина, В.И. Ярочкина и др.

В работе были использованы методы анализа, сравнения, обобщения, наблюдения. Применение данных методов позволило выявить оценить систему и методы информационной безопасности предприятия и разработать методику оценки информационных рисков.

Дипломная работа включает в себя введение, три главы, заключение, список источников и приложения.

В первой главе дается общее понятие экономической безопасности предприятия, приводятся ее основные принципы и задачи, рассматриваются основные элементы экономической безопасности предприятия, исследуется характеристика и сущность информационной составляющей экономической безопасности.

Во второй главе проводится анализ критериев, применяемых для оценки рисков информационной безопасности, проводится сравнительный анализ методических подходов и инструментария для оценки информационных рисков, приводится обоснование выбора методов оценки рисков информационной безопасности.

В третьей главе приводится краткая характеристика ООО «Траснефть-Восток», рассматриваются основные направления его информационной безопасности, проводится оценка методических подходов, используемых на предприятии для обеспечения информационной защищенности, разрабатывается методика оценки информационных рисков предприятия.

1 Основы экономической безопасности и её информационная составляющая

1.1 Понятие, принципы и задачи экономической безопасности предприятия

Понятие «экономическая безопасность» тесно связано с введением другого термина «национальная безопасность». Отсюда и возникает актуальность понятия «экономическая безопасность» - на современном этапе она является одной из важнейших составляющих системы национальной безопасности страны в целом.

В Российской Федерации определение понятия «безопасность» официально было закреплено еще в Законе РФ «О безопасности». В данном документе безопасность - это «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Под жизненно важными интересами в Законе определены «совокупность потребностей, удовлетворение которых надежно обеспечивать существование и возможности прогрессивного развития личности, общества, государства» [9].

В новейшем официальном документе, освящающем вопросы безопасности, «Стратегии национальной безопасности Российской Федерации до 2020 года» приводится следующее определение национальной безопасности как «состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качества и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства»[7]. Согласно этой стратегии, объектами экономической безопасности Российской Федерации являются «личность, общество, государство и основные элементы экономической системы, включая систему институциональных отношений при государственном регулировании экономической деятельности».

На современном этапе развития общества экономическая безопасность осуществляется на следующих уровнях:

1) на государственном уровне – как такое состояние экономики, при котором, не смотря на наличие неблагоприятных внешних и внутренних факторов, государством гарантируется полная защищенность национального хозяйства от внешних и внутренних угроз и при этом обеспечивается поступательное развитие общества, его экономическая и социально-политическая стабильность.

2) на уровне предприятия – как такое состояние хозяйственного субъекта, при котором он, эффективно используя свои корпоративные ресурсы, добивается защиты от всех внешних и внутренних опасностей и угроз, а также обеспечивает достижение целей бизнеса в условиях конкуренции и хозяйственного риска.

Следует отметить, что большое внимание уделяется таким видам безопасности как экологическая, сырьевая, финансовая, информационная и многим другим. В связи с этим, исследуем понятие экономической безопасности более подробно.

Например, Л.И. Абалкин рассматривает экономическую безопасность как «совокупность условий и факторов, обеспечивающих независимость национальной экономики, ее стабильность и устойчивость, способность к постоянному обновлению и самосовершенствованию» [3].

А. Архипов, А. Городецкий и Б. Михайлов считают, что экономическая безопасность – «это способность экономики обеспечивать эффективное удовлетворение общественных потребностей на национальном и международном уровнях». Иными словами, экономическая безопасность – это совокупность внутренних и внешних условий, которые благоприятствуют эффективному динамичному росту национальной экономики, ее способности удовлетворять потребности общества, государства, индивида, обеспечивать конкурентоспособность на внешних рынках, гарантирующую от различного рода угроз и потерь [4].

Экономическая безопасность в широком смысле слова, – отмечал академик РАН ректор МГУ им. М.В. Ломоносова В. Садовничий, – «это система условий и факторов, в которой страна и общество функционируют и развиваются по своим внутренним законам, делегируя управлению право стимулировать положительные сдвиги и тенденции, а также корректировать негативные отклонения, ограждая при этом страну от угроз внешней среды»[25].

Несмотря на разнообразие формулировок, и научных трактовок, мнения многих авторов имеют одну часто встречающуюся общую точку, и заключается она в том, что важной характеристикой экономической безопасности является ее должное обеспечение, иначе невозможно будет решать актуальные проблемы экономики как внутри государства, так и за его пределами, а также реализовывать национально-государственные интересы.

Имея в виду все вышесказанное, экономическая безопасность на государственном уровне несет в себя важнейшую роль, однако не стоит забывать об обеспечении безопасности на уровне субъектов экономики. Ведь, эффективность стабильного функционирования предприятия, к тому же его

существование в целом, напрямую зависит от системы работы экономической безопасности в условиях нестабильной среды, повторяющихся экономических кризисах и усилении конкуренции.

Изначально, до существенных изменений, а именно спада производства по стране, главной функцией экономической безопасности являлась сохранность коммерческой тайны. Сейчас понятие экономической безопасности имеет более широкое значение и несет в себе больший функционал.

В эпоху современной информационной экономики необходимым элементом предприятия является обеспечение экономической безопасности с помощью управления, а это требует построение собственной системы безопасности. Целями функционирования такой системы является выявление и дальнейшее предотвращение угроз и правильно подобранный механизм для достижения стратегических и тактических целей деятельности [18]. Поставленная цель реализуется путем решения множества сложных задач, таких как: своевременное выявление угроз и прогнозирование потенциальных опасностей и угроз, поиск приёмов и средств для их предотвращения, ослабления или уничтожение последствий их воздействия, анализ сил и средств, необходимых для обеспечения безопасности. Данной позиции придерживаются множество ученых.

В.К. Сенчаговым было сформулировано более обобщенное понятие при рассмотрении термина экономической безопасности предприятия, он определяет его как «состояние объекта в системе его связей с точки зрения способности к выживанию и развитию в условиях внешних и внутренних угроз, а также действиях непредсказуемых или непрогнозируемых»[8].

«Под экономической безопасностью предприятия следует понимать состояние эффективного использования его ресурсов и существующих рыночных возможностей, позволяющее предотвращать внутренние и внешние угрозы и обеспечивающее его длительное выживание и устойчивое развитие на

рынке в соответствии с избранной миссией» - считают Должиков П.Н., Величко Н.М., Должикова А.П [24].

Анализируя несколько определений, нетрудно сделать вывод о том, что все данные понятия объединили в себе ориентированность на стабильное положение и угрозы внешнего и внутреннего характера.

Постоянное соблюдения экономической безопасности – это необходимость, которая объясняется задачей, стоящей перед субъектом хозяйствования – сделать так, чтобы функционирование было стабильным, а главной целью деятельности стало достижение поставленной цели. Эффективность работы по предотвращению возможных угроз и устранению ущерба руководством и специалистами от негативных воздействий на те или иные составляющие экономической безопасности определяет уровень экономической безопасности.

Источниками негативных воздействий могут являться:

-заранее спланированные или спонтанные и незапланированные действия отдельных должностных лиц и хозяйствующих субъектов

-влияние объективных экономических и социальных обстоятельств (состояние финансовой конъюнктуры, научные открытия и технологические разработки и т. п.).

Факторы негативного воздействия на экономическую безопасность делятся на объективные и субъективные. Объективным фактором считаются негативные воздействия, которое наступает без участия и независимо от воли предприятия или работников. Субъективный фактор — это следствие непродуктивной работы предприятия в целом или его работников, прежде всего руководителей.

Основная цель экономической безопасности предприятия - обеспечить устойчивость и результативность работы в настоящее время и дальнейшее развитие предприятия на рынке в целом. Для этого необходимо определить корректный и наиболее успешный набор методов и подходов к ее обеспечению.

Система экономической безопасности предприятия строится на следующих принципах:

Первый – комплексность. Предполагается создание единой концепции экономической безопасности предприятия. Безопасность финансовых и информационных ресурсов, а также защита персональных данных – все это сферы деятельности предприятия, которые необходимо защищать от всех возможных угроз и атак. Поэтому только четко сформулированная концепция поможет обеспечить защиту всех данных и сохранить устойчивое функционирование.

Второй – приоритетность мер предупреждения. Только своевременное выявление всевозможных угроз, грамотный анализ ситуации и моментальная реакция на проблему, обеспечит максимальную защиту от негативного воздействия.

Третий принцип – непрерывность. Основывается на беспрерывном анализе ситуации и обеспечении своевременной помощи при различных угрозах.

Следующий принцип – законность. Каждое действие или бездействие преследуется законом. На предприятии должны быть разработаны системы безопасности на основе действующего федерального законодательства и различных нормативных актов, ориентированных на безопасность.

Пятый принцип – экономности. Все затраты, которое несет предприятие должны быть экономически выгодны и обоснованы.

Шестым принципом является взаимодействие. Все действия лиц, отделов, подразделений и служб внутри организации должны быть скоординированы со службами внешних организаций, таких как правоохранительные органы, служба безопасности на разных уровнях и другие органы власти.

Еще один принцип – компетентность. Каждый сотрудник должен быть подготовлен к определенному виду деятельности, проинструктирован надлежащим образом и нести ответственность за все свои действия. Каждое лицо должно быть профессионалом своего дела, понимать суть проблемы,

уметь адекватно оценивать происходящее и моментально принимать необходимые решения.

Восьмой – плановость. Деятельность по обеспечению экономической безопасности предприятия организуется на основе единого замысла, отраженного в конкретных планах предприятия по отдельным направлениям обеспечения его безопасности.

Вернемся к принципу комплексности и отметим тот факт, что он требует особого внимания. Для обеспечения непрерывного и эффективного функционирования предприятия необходимо иметь в виду, что именно задачи отражают требования, которые для этого необходимы. Однако следует отметить, что специфика задач у каждого предприятия своя, потому что зависит от отрасли деятельности. Следовательно, будут рассмотрены только несколько основных задач экономической безопасности предприятия:

-обеспечение сохранности информационных ресурсов, защита законных прав сотрудников, соблюдение политики конфиденциальности;
-защита особо ценной информации, а также сведений, к которым имеет доступ только ограниченный круг лиц. Своевременное предотвращение угрозы внешней атаки;
-с постоянной периодичностью должен производиться сбор, анализ и оценка данных, которые характеризуют внутреннее состояние предприятие;
-анализ конкурентной среды с целью собственного развития или же наоборот, предотвращение контактов с ненадежными партнерами или посредниками;
-принятие правильных управленческих решений с помощью поиска новой актуальной информации по вопросам стратегии и тактики для дальнейшего развития предприятия;
-обеспечение физической безопасности сотрудников, в частности руководства, ведущих специалистов и других сотрудников;

-правильная работа со средствами массовой информации для положительного мнения о предприятии, которое в дальнейшем может способствовать реализации планов экономической деятельности;

-возмещение морального и материального ущерба, который нанесен предприятию в результате неправомерного действия других организаций или лиц, являющихся её сотрудниками;

-борьба со шпионажем как внутренним, так и внешним, организованными преступными группировками или отдельными лицами[8].

Данный выше список задач экономической безопасности не является исчерпывающим. Каждое предприятие, в зависимости от своей специфики, направления деятельности и многих других факторов корректирует и детализирует список задач под себя.

1.2 Основные элементы экономической безопасности предприятия

Для представленного перечня задач необходимо разрабатывать индивидуальную систему экономической безопасности на предприятии. Система в свою очередь состоит из соответствующих элементов, которая подробно представлена на рисунке 1.

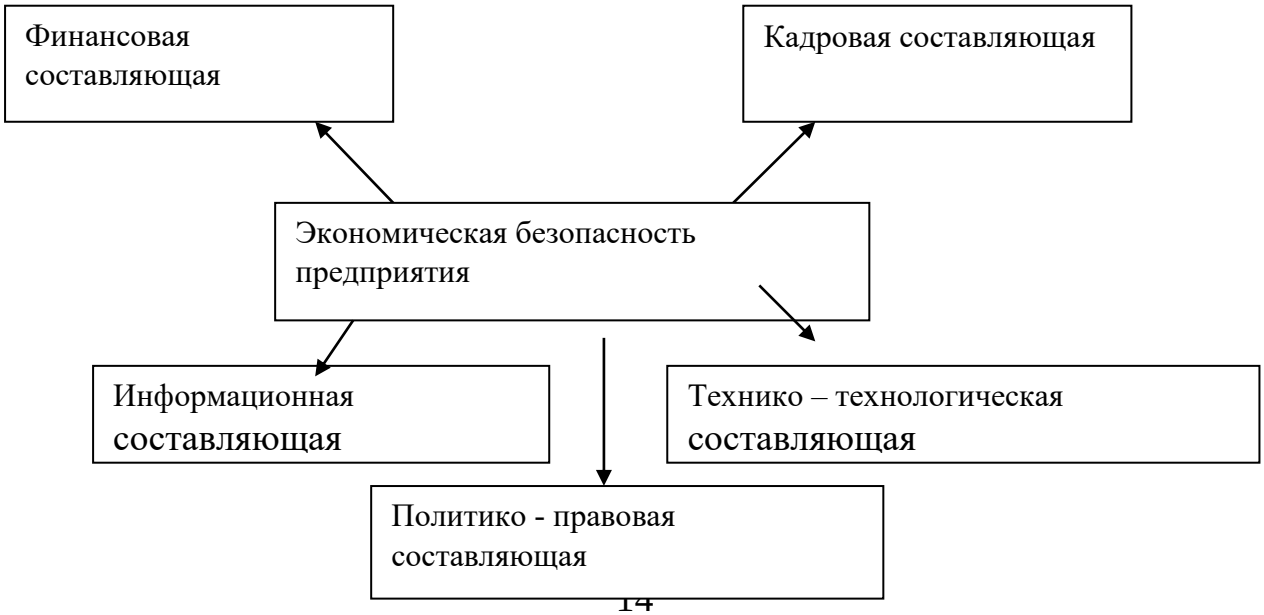

Рисунок 1 – Элементы системы экономической безопасности предприятия

Процесс обеспечения финансовой безопасности представляет собой финансово-экономическою состоятельность предприятия, устойчивости к банкротству, определяется параметрами платежеспособности и другими «денежными» характеристиками.

Финансовая безопасность трактуется как защищенность деятельности предприятия от опасных воздействий внешней среды, а также как способность моментально среагировать и уничтожить потенциальные угрозы или подстроиться к сложившимся условиям, которые не оказывают отрицательное влияние на деятельность предприятия. Однако, в виду наличия важных характеристик финансовой безопасности, данная категория является сложным понятием, которое требует подробного изучения.

Финансовая часть экономической безопасности присутствует практически во всех функционально важных сферы деятельности предприятия. Оценивая финансовую сторону безопасности, много положений пересекается с разными видами деятельности. Положения оценки затрагивают область стратегического управления предприятием. Если разработаны и приняты к исполнению функциональные стратегии (инновационная, ресурсная, инвестиционная, маркетинговая), то их цели обязательно должны соотноситься с формулировкой стратегических интересов предприятия, а характеризующие показатели должны корреспондировать количественной оценке стратегических интересов предприятия [21].

Комплекс последовательных, взаимосвязанных этапов деятельности строит систему оценки и анализа финансовой составляющей экономической безопасности. Последующее систематизирование их с методиками поможет выявить и даже уменьшить влияние хозяйственного риска до нормированного уровня с минимальными затратами ресурсов.

Существующие на данный момент методические подходы к стабилизации финансовой безопасности фирмы находятся на этапе разработки, как в теоретическом, так и в организационно–правовом аспекте. Непосредственно, сам механизм управления финансовой безопасностью – это выполнение работ по сохранению максимального уровня платежеспособности и ликвидности оборотных средств предприятия и его рост качества планирования и реализации финансово–хозяйственной деятельности. Однако, на данный момент термин «финансовая безопасность» является лишь одним из элементов экономической безопасности и не является самостоятельным объектом управления [12].

Кадровая безопасность еще один важный элемент экономической безопасности предприятия в целом. Понятие «кадровая безопасность» предприятия является производным от понятия безопасности вообще. Несмотря на то, что единого определения безопасности не существует, можно выделить несколько подходов к его анализу.

Так, Митрофанова Е.А. считает, что: «Кадровая безопасность - это такое положение организации, при котором воздействие на нее и индивидов внутри нее со стороны природной, экономической и социальной среды, а также внутренней среды самого человека не способны причинить вреда»[13].

Существует ряд факторов, от которых зависит кадровая безопасность предприятия:

1. Найм – это комплекс мер безопасности при приеме на работу и прогнозирования благонадежности. Этот фактор включает в себя поиск кандидатов на ту или иную должность, документальное и юридическое обеспечение приема на работу, испытательный срок, сама процедура отбора персонала и даже адаптация.

2. Лояльность-это положительное отношение работника к руководству, политике организации и коллективу, в котором он трудится. Профессиональные менеджеры по управлению персоналом отмечают, что

основой является стремление сотрудников фирмы приносить ей пользу и избегать тех действий, которые могут навредить.

3. Контроль-проверка действий персонала по определенной системе с последующим анализом и принятием оперативных и стратегических решений. Этот комплекс уже непосредственно нацелен на ликвидацию возможностей причинения ущерба и отрабатывается, как правило, службой безопасности или другими подразделениями, но в меньшей степени службой персонала.

Кадровая безопасность предприятия - это сложное понятие, которое наукой трактуется и используется по-разному. Как базовое понятие безопасности его содержание можно раскрыть через различные научные подходы отраслевой направленности.

При работе каждое предприятие использует самостоятельно выбранный набор технологий материального или интеллектуального производства. То насколько корректно и уместно будет подобран этот набор и будет определять эффективное функционирование предприятия, а, следовательно, и экономическую безопасность.

По мнению Евдокимова Ф. И.: «обеспечение технико-технологической безопасности предприятия заключается в соответствии уровня применяемых на предприятии технологий лучшим образцам мировой науки, учитывая оптимизацию расходов»[26].

Работа с технико-технологической составляющей экономической безопасности влечет необходимость реализовать несколько последовательных этапов, представленных на рисунке 2.

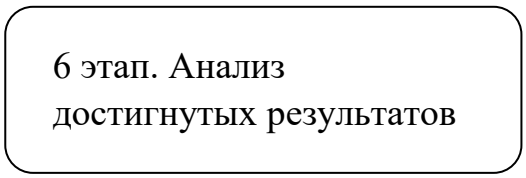

Рисунок 2 - Процесс обеспечения технико-технологической составляющей экономической безопасности

Первый этап заключается в анализе рынка технологий по производству продукции, аналогичной профилю предприятия (изучение особенностей технологических процессов предприятий, которые производят аналогичную продукцию, анализ научно-технической информации в отношении новых разработок в конкретной области).

Второй этап предусматривает проведение анализа конкретных технологических процессов и выявление внутренних резервов с целью оптимизации используемых технологий. Третий этап состоит из выполнения таких работ:

а) изучение товарных рынков по аналогичной продукции производимой предприятием;

б) оценка дальнейших направлений развития рынков сбыта продукции предприятия;

в) прогноз необходимых технологических процессов для производства конкурентоспособных товаров.

На четвертом этапе разрабатывается стратегия развития предприятия (производителя продукции), включая:

1) поиск товаров из существующего ассортимента предприятия, которые в дальнейшем принесут большую прибыль;

2) изучение новых технологий для производства перспективных товарных единиц;

3) оптимизация бюджета технологического развитию предприятия путем правильного расчета расходов на технологическое развитие. Два возможных

варианта: внедрение собственных технологий или приобретение патентов и подходящего оборудования на рынке;

4) составление общего плана технологического развития предприятия (с конкретизацией выбора: альтернативного вектора технологического развития; сроков и объемов финансирования; ответственных исполнителей);

5) разработка плана собственных финансовых ресурсов согласно бюджету технологического развития предприятия.

Пятый этап строится на оперативной реализации планов по технологическому развитию предприятия, при этом процесс его производственно-хозяйственной деятельности не останавливается.

Шестой этап заключительный. При его реализации проводится анализ и оценка результатов фактического выполнения мероприятий по обеспечению технико-технологическому развитию. При этом, возможно использование специальной карты расчетов показателей эффективности мероприятий.

Таким образом, технико-технологическая безопасность предприятия представляет собой анализ того, как соответствуют применяемые на предприятии технологии лучшим мировым аналогам по оптимизации расходов.

Особое значение для безопасной работы организации представляет информационный ресурс. Он помогает оценить внутреннюю и внешнюю экономическую среду, угрозы развития, рост, падение и результаты хозяйственной деятельности предприятия в целом. Информация помогает высчитать резервы увеличения эффективности деятельности предприятий, снизить затраты на производство, оптимизировать загрузку мощностей и запасы материальных ценностей, и, что наиболее важно – повысить качество и управляемость процессов хозяйствующего субъекта.

Информацию в процессе воспроизводства экономической безопасности можно рассматривать с двух сторон. С одной стороны, эффективная работа с информационными ресурсами является одной из характеристик экономической безопасности хозяйствующего субъекта. С другой стороны: информация - это

необходимое условие оценки уровня экономической безопасности и контроля процессов ее воспроизводства.

Информационная безопасность имеет два типа угроз:

1) непреднамеренные – выражаются ошибками в управлении;

2) преднамеренные – незаконное получение информации другими лицами.

Ущерб от этих рисков может быть различным:

– ущерб деловой репутации организации;

– ущерб, связанный с разглашением персональных данных отдельных лиц;

–финансовый ущерб от разглашения защищаемой (конфиденциальной) информации;

– ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

–потери от невозможности выполнения взятых на себя обязательств перед третьей стороной;

– моральный и материальный ущерб от дезорганизации в работе всего предприятия.

Не маловажным является выявление источников вышеперечисленных угроз, то есть источников угроз. Они подразделяются на внешние и внутренние.

К внешним относят:

– криминальные структуры;

– конкуренты;

– потенциальные преступники и хакеры;

– технический потенциал поставщиков услуг;

– представители силовых структур;

– представители надзорных организаций.

К внутренним относят:

– основной персонал (пользователи, разработчики, программисты);

– представители службы защиты информации;

– вспомогательный персонал;

– технический персонал.

Таким образом, нужно вовремя и правильно оценивать негативные последствия ущерба нанесенного информационной безопасности, при этом выполнять ряд важных стратегических обязанностей по информационному обеспечению деятельности.

Политико-правовая составляющей экономической безопасности предприятия – это всестороннее и эффективное правовое обеспечение деятельности предприятия, с четким соблюдением всех правовых нормативов и аспектов действующего законодательства.

Для решения всех поставленных задач, которые ставятся перед специалистами экономической безопасности, необходимо создавать целостную систему, подход к которой должен быть отражен в концепции по обеспечению экономической безопасности на предприятии. В свою очередь, концепция должна содержать основные принципы, направления и этапы реализации мер безопасности.

Имея в виду отечественный и зарубежный опыт, необходимо понимать, что для качественной и эффективной борьбы с угрозами должна быть налажена система процесса противодействия, в котором должны принимать участие профессионалы всех структур организации для обеспечения всестороннего подхода к борьбе.

1.3 Характеристика и сущность информационной составляющей экономической безопасности

В современном мире информация играет важную роль и является одним из основных ресурсов для общества, поэму логично, что в основе экономической системы стоят информационные ресурсы. Деятельность любого предприятия основывается на бухгалтерском учете, управлением финансами и кадрами, а также на операционной деятельности, существенную роль в них занимают информационные технологии, которые, в свою очередь, решают

различные задачи оптимальным способом. На внедрение таких технологий требуется достаточное количество времени, поэтому деятельность предприятия зависит от скорости внедрения в работу информационных систем.

Для анализа и оценки внедрения таких систем в работу необходима правильная организация процесса обеспечения информационной составляющей экономической безопасности предприятия.

Цель информационной безопасности — выявление угроз безопасности информации, определение всех последствий и анализ причинного ущерба, принятие необходимых мер защиты с оценкой эффективности. Так как анализ информационной инфраструктуры далеко не всегда оправдан с экономической точки зрения, то целесообразно выявить сразу источники потенциального ущерба.

Угрозы сохранности, целостности и конфиденциальности информационных ресурсов ограниченного доступа практически реализуются через риск образования канала несанкционированного получения (добывания) кем-то ценной информации и документов. Этот канал представляет собой совокупность незащищенных или слабо защищенных направлений возможной утраты информационных ресурсов ограниченного доступа, которые злоумышленник использует для получения необходимых сведений. Функционирование канала несанкционированного доступа к информации обязательно влечет за собой утрату информации, исчезновение носителя информации.

Обеспечение информационной безопасности должно начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления).

Исходя из вышеизложенного, в наиболее общем виде информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой.

К объектам информационной безопасности в организации относят:

1) информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;

2) средства и системы информатизации – средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления в организациях, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации [22].

Говоря о защите информации, вводят следующую классификацию тайн по шести категориям:

- государственная тайна;
- коммерческая тайна;
- банковская тайна;
-профессиональная тайна;
-служебная тайна;
-персональные данные.

GartnerGroup выделяет 4 уровня зрелости организации с точки зрения обеспечения информационной безопасности:

-0-й уровень: - информационной безопасностью (ИБ) в организации никто не занимается, руководство не осознает важности данной проблемы; - финансирование отсутствует; - информационная безопасность реализуется штатными средствами операционных систем, систем управления базами данных (СУБД) и приложений (парольная защита, разграничение доступа к ресурсам и сервисам);

- 1-й уровень: - информационная безопасность рассматривается как чисто «техническая» проблема, отсутствует единая программа развития системы обеспечения информационной безопасности (СОИБ) организации; - финансирование ведется в рамках общего бюджета; - информационная безопасность реализуется средствами 0-го уровня плюс средства резервного копирования, антивирусные средства, межсетевые экраны, т.е. традиционные средства защиты;

-2-й уровень: - информационная безопасность рассматривается как комплекс организационных и технических мероприятий, существует понимание важности данного вопроса для производственных процессов, есть утвержденная руководством программа развития системы охраны и безопасности организации; - финансирование ведется в рамках отдельного бюджета; - информационная безопасность реализуется средствами 1-го уровня плюс средства усиленной аутентификации, средства анализа почтовых сообщений и web-контента, системы обнаружения вторжений, средства анализа защищенности, средства однократной аутентификации и организационные меры;

- 3-й уровень: - информационная безопасность является частью корпоративной культуры, назначен старший администратор по вопросам обеспечения информационной безопасности; - финансирование ведется в рамках отдельного бюджета; - информационная безопасность реализуется средствами 2-го уровня плюс системы управления информационной безопасности, группа реагирования на инциденты нарушения информационной безопасности и соглашения об уровне сервиса.

На каждом предприятии (в организации) соответствующие службы выполняют функции, в совокупности, характеризующие процесс обеспечения информационной составляющей в рамках усиления экономической безопасности. К основным относятся такие функции:

1. Сбор всех видов информации, имеющей отношение к деятельности предприятия или другого субъекта хозяйствования (информация по всем видам

рынков, по политическим событиям и тенденциям макроэкономического развития мировой и национальной экономики; научно-техническая информация; новые законодательные и нормативные документы, регулирующие деятельность предприятий и организаций).

2. Анализ получаемой информации с обязательным соблюдением общепринятых принципов (систематизации, непрерывности поступления, всестороннего характера аналитических процессов) и методов (локальных, по специфическим и общекорпоративным проблемам) организации работ.

3. Прогнозирование тенденций развития научно-технологических, экономических и политических процессов на предприятии, в стране и в мире относительно конкретной сферы бизнеса (деятельности), а также показателей, которых необходимо достичь (например, финансовые прогнозы, прогнозы объектов производства и технологического развития данного предприятия или данной организации).

4. Оценка уровня экономической безопасности предприятия по всем составляющим и в целом, разработка рекомендаций по повышению его уровня на данном субъекте хозяйствования.

5. Другие виды деятельности по обеспечению информационной составляющей экономической безопасности предприятия (связь с общественностью, формирование благоприятного имиджа фирмы, зашита конфиденциальной информации).

При всей своей многозадачности, информационная безопасность предприятия должна решать круг узких задач, таких как:

-выявление, оценка и предотвращение угроз информационным ресурсам и системам

-сохранение коммерческой, служебной и личной тайны

-защита прав физических и юридических лиц на интеллектуальную собственность

Делая вывод из вышесказанного, определяем основную задачу, стоящую перед предприятием по осуществлению информационной безопасности.

Предприятие должно обладать информационными ресурсами, проверять и защищать их для того, чтобы обеспечить экономическую безопасность в целом.

Оценка уровня экономической безопасности организации по всем функциональным составляющим на основе статистических методов обработки информации сильно затруднена из-за того, что большинство аспектов данной проблемы крайне сложно поддается математической формализации, а некоторые из них не поддаются вовсе. Тем не менее, важность данной проблемы для эффективного функционирования организации очень велика, поэтому необходимо оценивать уровень ее экономической безопасности на основе определения критериев экономической безопасности организации.

В последующих главах будут проанализированы вопросы оценки уровня работы информационных систем в рамках обеспечения экономической безопасности, а также риски нанесения ущерба предприятию в целом.

2 Методические подходы к оценке информационных рисков на предприятии

2.1 Анализ критериев, используемых для оценки рисков информационной безопасности

Все российские предприниматели на современном этапе осознают важность управления рисками, которые связаны с их деятельностью. Эксперты, специализирующиеся на риск менеджменте, оценив дальнейшее развитие данного направления деятельности и его тенденции, а также серьезные угрозы в будущем, пришли к выводу о том, что в ближайшей время самыми значимыми будут являться –операционные и репутационные риски. На следующем месте по значимости –политические риски, опасности стратегического партнерства, риски вследствие изменений климата и информационные угрозы нового поколения[11].

К тому же на современном этапе развития отмечается опасность экономической нестабильности, рост организованной преступности, угрозу

терроризма и ужесточение конкуренции. Более половины руководителей считают, что в их организациях действует надежная защита от всех потенциальных угроз. Именно поэтому важным является то, что комплексной системе управления рисками организации придается существенное значение [11].

Следует отметить, что информационный риск занимает лидирующие позиции в структуре рисков предприятия [28]. Именно поэтому вопросам управления этими рисками стоит уделять больше внимание. Как один из вариантов систему защиты активов предприятия можно представить в виде пирамиды, верхнюю часть которой занимает информационная защищенность, поскольку информационные риски взаимосвязаны со всеми остальными рисками и сопровождают создание, передачу, хранение и использование информации (рисунок 3).

Рисунок 3 – Система защиты активов хозяйствующего субъекта

Все информационные риски подразделяются на три типа:

– риски, связанные с утратой либо утечкой информации предприятия, которая может быть использована конкурентами и сотрудниками организации в целях, способных нанести ущерб бизнесу;

– риски, связанные с техническими сбоями в работе каналов передачи информации, способные повлечь убытки;

– риски, обусловленные форс-мажорными обстоятельствами [12].

Общепризнанно, что риском является событие, способное в случае реализации оказывать значительное положительное либо негативное воздействие на достижение компанией своих краткосрочных и долгосрочных целей. Риски, имеющие положительное влияние, носят название возможностей, в то время как риски, способные оказать негативное воздействие, называются угрозами.

В узком смысле риск представляет собой поддающуюся измерению вероятность возникновения убытка либо упущения выгоды, а вероятность риска – это степень возможности реализации определенного события в определенных условиях. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого экономической системе или хозяйственному субъекту в случае реализации угрозы информационной безопасности. Угрозы информационной безопасности представляют собой совокупность условий и факторов, способные повлечь нарушение конфиденциальности, целостности и доступности информации.

Уязвимость – это слабость в системе защиты, которая делает возможным реализацию угрозы. Под опасностью информационной безопасности понимается вероятность реализации угрозы. При разработке критериев по оценки рисков информационной безопасности предприятию следует учитывать следующие моменты:

– стратегическую ценность обработки бизнес-информации;

–критичность информационных активов, подвергшихся воздействию;

– действующие законодательно-нормативные требования и обязательства по договорам;

–значение для бизнеса конфиденциальности, доступности и целостности;

– ожидания и реакция причастных сторон, а также возможные негативные последствия для нематериальных активов и репутации организации [13].

Оценка рисков в качестве направления информационной безопасности выступает существенным инструментом в создании защиты. В процессе оценки рисков выявляются риски для организации и определяется комплекс мер безопасности, необходимых для снижения риска.

В классическом представлении под риском понимается вероятность реализации угрозы информационной безопасности. В ходе оценки рисков осуществляется моделирование картины возникновения неблагоприятных условий путем учета всех возможных факторов, которые определяют данный риск. При анализе рисков с математической точки зрения эти факторы считаются входными параметрами. Однако, следует учитывать большое количество источников информации и степень неопределенности самой информации. Наибольший интерес в ходе оценки рисков представляют формулы и данные для расчета величины риска.

Далее будут рассмотрены разные методы расчета рисков. Риск информационной безопасности в классическом варианте представляет собой функцию трех переменных:

– вероятность существования угрозы;

– вероятность существования уязвимости;

– степень потенциального воздействия.

Когда любая из указанных переменных стремится к нулю, то полный риск также приближается к нулю. В соответствии с ISO/IEC 27001 (международный стандарт по информационной безопасности, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией), выбранный метод должен гарантировать сравнимые и воспроизводимые результаты оценки рисков. При этом в данном стандарте не указывается конкретная формула расчета [1].

NIST 800-30 содержит следующую классическую формулу расчета риска (1):

$$R = P(t) * S, \quad (1)$$

где R – значение риска;

P(t) – вероятность возникновения угрозы информационной безопасности;

S – степень воздействия угрозы на актив(цена актива в качественной шкале и количественной).

В результате рассчитывается значение риска, выражаемое в относительных единицах, которое возможно ранжировать по уровню значимости для процесса управления рисками информационной безопасности [13].

В соответствии с ГОСТ Р ИСО/МЭК ТО 13335-3-2007 оценка риска осуществляется по следующей формуле (2):

$$R = P(t) * P(v) * \mathrm{C}, \quad (2)$$

где *P(t)* – вероятность возникновения угрозы информационной безопасности;

P(v) – вероятность присутствия уязвимости;

C – ценность актива.

В качестве варианта значений вероятностей P(t) и P(v) используется качественная шкала с тремя уровнями (высоком, средним, низким). Оценка ценности актива *C* производится с применением числовых значений в интервале от 0 до 8. Присвоение им конкретных значений производится в организации, которая проводит оценку рисков информационной безопасности [14].

В соответствии cBS 7799-2:2005, уровень риска рассчитывается с учетом ряда показателей, таких как ценность ресурса, уровень угрозы и степень

уязвимости. С ростом значений данных параметров увеличивается и риск. Формула оценки риска представлена в следующем виде (3):

$$R = \mathrm{C} * L(t) * L(v), \quad (3)$$

где *C* – ценность актива;

L(t) – уровень угрозы;

L(v) – степень уязвимости.

На практике для вычисления рисков информационной безопасности используют таблицы позиционировании для значений степени угроз, вероятности использования уязвимости и величины стоимости активов. Величина риска может принимать значения в диапазоне от 0 до 8, в итоге по каждому из активов формируется список угроз с разными значениями риска. Поэтому для точности и удобства используется шкала ранжирования рисков: высокий (6–8), средний (3–5) и низкий (0–2) (Приложение А). Это позволяет выявить наиболее критичные риски [15].

Согласно стандарту РС БР ИББС-2.2-200, оценка степени вероятности реализации угрозы информационной безопасности осуществляется по качественно-количественной шкале, в соответствии с которой нереализуемой угрозе присваивается значение 0%, средней – от 21% до 50% и т. д. Степень тяжести последствий для различных типов информации оценивается с применением качественно-количественной шкалы, в которой минимальное значение составляет 0,5% от величины капитала предприятия, высокое – от1,5% до 3% от величины капитала [5].

Для проведения качественной оценки рисков информационной безопасности применяется таблица соответствия уровня тяжести последствий и возможности реализации угроз. Формулу количественной оценки можно представить в следующем виде (4):

$$R = P(v) * S, \quad (4)$$

где$P(v)$ – вероятность присутствия уязвимости;

S – ценность актива.

Анализ всех вышеперечисленных методов оценки рисков позволяет отметить, что определение риска осуществляется с применением уровня угроз и величины ценности актива.

В заключение следует отметить, что анализ информационных рисков имеет важное значение в структуре экономической безопасности предприятия. В зависимости от сферы применения, объекта и целей управления рисками, на предприятии могут использоваться разные подходы. Выбор либо разработка определенного подхода к оценке рисков осуществляется с учетом основных критериев, включающих критерии оценки риска, критерии влияния, критерии принятия риска.

2.2 Сравнительный анализ методических подходов и инструментария для оценки информационных рисков

Существует большое многообразие методов и подходов, которые используются для оценки информационных рисков. Выделяют четыре основных подхода к решению задач по изучаемой проблеме. Далее будет рассмотрен подробно каждый из этих подходов.

К особенностям первого подхода относится оценка информационных рисков от возникновения предполагаемых угроз с учетом причиняемого при этом ущерба. В ходе оценки проводится анализ всех возможных угроз, возможности их появления и последствия таких угроз в виде причиненного ущерба конкретной организации. По итогам такого анализа принимается решение о необходимости разработки мероприятий. При этом могут оставаться угрозы, в отношении которых не вынесено решения об использовании защитных мероприятий, вследствие чего возможен определенный ущерб в

случае их реализации, что и определяет риск. В стандарте ГОСТ Р ИСО/МЭК 15408 такой тип риска называется «остаточным риском».

В ходе реализации такого подхода рекомендуется изучение всех аспектов нарушения информационной безопасности, включающей конфиденциальность, целостность и доступность, с учетом степени наносимого ущерба. Высокая трудоемкость применения данного метода может уменьшаться путем применения подходов, содержащихся в техническом отчете ISO/IEC 13335. Эти варианты предполагают проведение анализа уровня риска для всех систем, связанных с обеспечением безопасности информации с целью определения системы с высоким уровнем риска. Далее осуществляется изучение выделенных систем с применением детального анализа информационного риска [10]. Применение такого подхода позволит направить процесс управления информационной безопасностью на области, отличающиеся наивысшим уровнем риска и требующие наибольшего внимания, таким образом может быть разработана программа мер, характеризующаяся наименьшими затратами времени и средств.

Второй подход предусматривает проведение оценки влияния отклонений в организациях от утвержденного образца, закрепленного в нормативных документах. Предполагается, что в ходе разработки и выбора нормативного документа были учтены все либо основные угрозы и их воздействие [8, с. 76].

Следовательно, в соответствии с данным подходом оценка риска представляет собой оценку уровня отклонений от установленных требований информационной безопасности с учетом степени их важности и влияния на деятельность предприятия. Этот подход менее трудоемкий в сравнении с первым подходом, однако, его использование возможно лишь в случае наличия нормативного документа, содержащего все требования, которые позволяют сформировать защиту от всех известных угроз [6,].

Третий подход ориентируется на оценку рисков информационной безопасности предприятия в условиях реальной деятельности в изменяемой среде, что позволяет выявить тенденцию к ухудшению общего состояния

информационной безопасности. Этот подход базируется на проведении непрерывного мониторинга предприятия, автоматизированной системы обработки информации, оценки состояния ее параметров, уровня стабильности и т. д. Любое отклонение от состояния, запланированного на этапе разработки, способно привести предприятие к кризисному положению и требует незамедлительного принятия мер [5]. В плане применения данный подход больше ориентирован на проведение оценки действующих систем и предназначен для деятельности подразделений или лиц, ответственных за управление и качество их функционирования.

В основе четвертого подхода к оценке рисков лежат принципы, предполагающие известность всех источников опасности еще на этапе разработки информационной системы. Предполагается, что работоспособность всех заложенных средств защиты система является полностью защищенной, а незащищенность выступает следствием некачественной работой защитных средств [12].

Этот подход в плане оценки информационных рисков близок к первому и второму подходам. Главное отличие подхода заключается в ориентации на имеющуюся статистику появления угроз. Подход применим при условии возможности выявления всего перечня угроз, определения точных значений вероятности их появления, интервала воздействия, а также при условии существования уверенности в гарантии необходимого уровня информационной безопасности в случае защиты от выбранного перечня угроз [13].

На сегодняшний день существуют качественные и количественные методы оценки информационных рисков предприятия. Качественные методы предполагают большое количество табличных методов оценки информационных рисков компании. Такие методы отражены в рекомендациях международных стандартов информационной безопасности, прежде всего, в ISO 17799, принимаемого отдельными методами оценки рисков за образец «нулевого риска», в котором риск показывает степень отклонения от образца.

Основной целью качественных методик является определение самих рисков, а также выявлении причин и факторов, способных оказать влияние на их уровень. Выделяют следующие виды качественных методик анализа рисков:

– метод экспертных оценок;

– метод рейтинговых оценок;

– контрольные списки источников рисков.

В процессе применения метода экспертных оценок осуществляется оценка действий, в основе которой лежит мнение группы экспертов, позволяющее сформировать экспертное заключение. Среди достоинств данного подхода выделяют возможность привлечения для проведения анализа квалифицированных специалистов. Недостаток метода заключается в субъективности сформированных мнений и подходов и возможных трудностей с поиском независимых экспертов. В качестве источников информации используются опросные листы, результаты проведения анализа слабых и сильных сторон предприятия, исследования в сфере маркетинга и др.

Базой метода рейтинговых оценок является система рангов или оценок, предполагающая присвоение баллов в диапазоне от 5 до 100. Критерии балльной оценки определяются специалистом, осуществляющим анализ. По результатам исследования составляется таблица с данными рейтингов рисков.

Метод контрольных списков представляет собой методику проведения аналитических исследований событий прошлых периодов и факторов появления вследствие таких событий рисков и убытков. Этот метод может применяться только на этапе идентификации. При этом предусматривается корректировка исследуемого списка в связи с появлением новой статистической информации. Недостатком данного метода является неполный учет изучаемой информации вследствие большого объема исследуемых данных. В ходе оценки рисков используются стандарты ИСО «Методы оценки риска». Выделяют следующие этапы оценки рисков:

– идентификация риска;

– анализ последствий;

– качественная, смешанная или количественная оценка вероятностных характеристик риска;

– оценка эффективности существующих средств управления;

– количественная оценка уровня риска;

– сравнительная оценка риска.

В основе количественных способов оценки информационных рисков лежит использование статистических данных. Данный подход к оценке рисков отличается большой объективностью, однако он ограничен в применении, поскольку определение возможного ущерба от большинства информационных рисков является довольно сложным, возможна лишь их приблизительная оценка [16]. Характеристика наиболее используемых методов анализа рисков приведена в таблице 1.

Таблица 1– Характеристика наиболее используемых методов анализа рисков

Метод	Характеристика метода
Вероятностный анализ	Построение и расчеты по методике производятся в соответствии с принципами теории вероятностей, в то время как при использовании выборочных методов это осуществляется путем расчетов по выборкам. Вероятность получения потерь рассчитывается на основе статистических данных предыдущего периода с определением зоны рисков, достаточности финансовых ресурсов, показателя рисков
Экспертный анализ рисков	Метод используется при отсутствии или недостаточности исходной информации и предполагает привлечение экспертов для проведения оценки рисков. Выбранная группа экспертов проводит оценку проекта и его отдельных процессов по степени рисков
Метод аналогов	Использование базы данных реализованных аналогичных проектов для переноса их показателей результативности на планируемый проект. Этот метод применяется, когда внутренняя и внешняя среда проекта сходна с основными параметрами аналога.
Анализ показателей предельного уровня	Вычисление степени устойчивости проекта относительно возможных изменений условий его реализации
Анализ чувствительности проекта	Метод позволяет провести оценку изменения результирующих показателей реализации проекта с различными значениями заданных переменных, которые необходимы для расчета
Анализ сценариев развития проекта	Метод предусматривает разработку нескольких вариантов развития проекта и проведение их сравнительной оценки. определяются пессимистический вариант возможного изменения данных, оптимистический и наиболее вероятный вариант.
Метод построения	Предусматривает пошаговое развитие процесса выполнения

деревьев решений проекта	проекта с оценкой рисков, затрат, ущерба и выгод
Имитационные методы	Основан на пошаговом определении значения результирующего показателя путем проведения многократных опытов с моделью. К основным преимуществам относятся прозрачность расчетов, простота и возможность оценки результатов анализа проекта всеми участниками процесса планирования. Серьезным недостатком являются существенные затраты на расчеты, обусловленные большим объемом выходной информации

Количественный способ позволяет установить уровень риска, провести оценку возможного ущерба при возникновении угроз, величину фактических затрат и объемов непредвиденных затрат, которые могут понадобиться, а также воздействие последствий информационных рисков на деятельность компании. Однако необходимо отметить, что статистические методы оценки информационных рисков не нашли широкого применения в практике международного сообщества.

Проведение полного анализа рисков информационной защищенности организации предусмотрено с применением инструментальных средств, основанных на структурных методах системного анализа и проектирования. Неотъемлемым условием таких продуктов выступает база данных, в которой отражена вся информация о событиях в сфере информационной безопасности. Она позволяет проводить оценку рисков и уязвимостей, рассчитывать эффективность различных вариантов применяемых контрмер в конкретных ситуациях.

Методика, положенная в основу инструментальных средств анализа рисков, обуславливает их ценность. В качестве примеров методик, предполагающих проведение полного анализа рисков, можно привести программные продукты, наиболее известными среди которых являются CRAMM (Великобритания), Risk Watch (США), КОНДОР и ГРИФ (Россия). Данные методики предусматривают проведение сравнительного анализа с применением 15 наиболее существенных критериев:

– поддерживаемые стандарты;

– способы оценки информационных рисков;

– используемые технологии оценки рисков;

– наличие статистики по инцидентам в области информационной безопасности;

– наличие базы данных по угрозам, уязвимостям, контрмерам в области информационной безопасности;

– оценка надежности персонала;

– организационный и программно-технический уровни оценки рисков;

– оценка эффективности внедрения контрмер;

– содержание методики анализа рисков;

– особенности отчетной документации;

– системные требования;

– наличие специальной подготовки и высокой квалификации аудитора в области информационной безопасности;

– стоимость;

– возможность адаптации продукта под конкретные потребности организации (гибкость методики).

Сравнение указанных методик оценки рисков позволило выделить их особенности и достоинства (приложение Б). Далее охарактеризованы и недостатки перечисленных методик:

1. Risk Watch:

– применение методики требует наличия специальной подготовки и достаточно высокой квалификации специалистов в сфере информационной безопасности. В какой-то степени, это может быть достоинством методики, способствующим повышению уровня доверия к результатам анализа информационных рисков;

– в методике не учтены организационные факторы обеспечения информационной безопасности.

– не проводится оценка надежности сотрудников, имеющих доступ к конфиденциальной информации;

– существует ряд ограничений по использованию способов оценки рисков, заключающийся в применении только количественных способов;

– предполагает применение упрощенного подхода к описанию информационной системы и к оценке рисков;

–высокая стоимость [10].

2. CRAMM

– отсутствие гибкости методики: трудности адаптации метода под конкретные потребности организации в связи с невозможностью внесения дополнений в базу знаний;

– высокая трудоемкость процесса, предполагающая длительный период непрерывной работы аудиторов;

– обязательное наличие специальной подготовки и высокой квалификации аудиторов в сфере информационной безопасности, что также может быть отнесено и к достоинствам, поскольку применение методики квалифицированными означает достоверность и обоснованность полученных результатов анализа;

– генерирование большого объема бумажной документации, не всегда необходимой на практике;

– упор сделан на технические и программно-аппаратные вопросы обеспечения информационной безопасности, практически не учтены организационные направления защиты информации;

– отсутствует оценка надежности персонала, допущенного к конфиденциальной информации;

– нет базы данных по инцидентам в области информационной безопасности;

– сложность русификации данного продукта для отечественных пользователей;

– высокая стоимость [4].

3. ГРИФ и КОНДОР:

–ограниченная база данных по уязвимостям и угрозам информационной безопасности;

– нет базы данных по инцидентам в сфере информационной безопасности;

– обязательным условием является наличие значительных по сравнению с другими продуктами ресурсов персонального компьютера: высокие требования к оперативной памяти и свободному дисковому пространству;

– отсутствует перечень бизнес-процессов и связанной с ним ценной информации, активов и т.д. Аналитик вынужден вручную вносит в базу данные по отдельным бизнес-процессам компании и иным видам ценной информации, не включенным в список;

– учет организационного направления в сфере обеспечения информационной безопасности производится согласно международному стандарту ИСО 17799, при этом не осуществляется оценка надежности персонала в ходе анализе рисков информационной безопасности компании;

– вычисление предполагаемого ущерба при возникновении угроз безопасности ведется при помощи метода экспертных оценок. Однако могут возникать трудности в решении поставленных задач в связи с отсутствием четкой методики оценки [14].

Таким образом, на основании проведенного анализа средств оценки информационных рисков компании можно выделить следующие основные моменты:

– методики позволяют проводить аудит информационных систем на соответствие требованиям международным стандартам;

– при помощи данных инструментов возможна оценка уровня текущего состояния информационной безопасности экономического субъекта;

– методики предполагают использование имеющихся баз данных по угрозам и уязвимостям;

– применение указанных методов позволяет провести оценку реальных и потенциальных потерь в случае реализации угроз;

– на основе полученных при помощи данных методов результатов оценки рисков можно управлять информационными рисками, разрабатывать политику информационной безопасности компании [16].

К недостаткам всех методов можно отнести то, что, несмотря на комплексный подход всех методик к оценке рисков, в них хорошо проработан алгоритм проведения программно-технического анализа рисков и достаточно слабо учтены организационные направления обеспечения информационной безопасности. Отсутствует оценка надежности сотрудников предприятия как основного источника угроз. Кроме этого, отсутствие четкой методики оценки возможного ущерба в некоторых методиках является существенным недостатком, а подходы отдельных методик к оценке величины ущерба не всегда возможны к применению в российских условиях.

В заключение можно сделать вывод о том, что анализ методических подходов и инструментов, используемых для оценки информационных рисков, подтверждает необходимость комплексной системы защиты информации. Сравнительный анализ нескольких наиболее популярных методик оценки информационных рисков позволяет сделать вывод о невозможности использования какой-либо единой методики, которая явилась бы универсальной для большинства отечественных предприятий. Каждый отдельный случай предполагает адаптацию общей методики оценки информационных рисков под потребности предприятия, исходя из специфики его деятельности. Для дальнейшего анализа была выбрана многофакторная модель оценки информационных рисков безопасности предприятия, рассмотренная в следующем параграфе.

2.3 Обоснование выбора методов оценки рисков информационной безопасности

Оценка рисков предусматривает идентификацию рисков, определение параметров для их описания и оценок по выбранным параметрам. Выбор

подхода к оценке рисков определяется уровнем требований, которые предъявляются на предприятии к информационной безопасности. Цель проведения анализа рисков заключается в оценке угроз и уязвимостей, а также уровня предполагаемого ущерба с учетом степени защиты информационной системы предприятия. Анализ рисков является отправной точкой создания системы информационной безопасности и предполагает реализацию мероприятий по исследованию информационной безопасности, заключающейся в установлении угроз и ресурсов, нуждающихся в защите [11]. К стратегиям управления разными группами информационных рисков относятся:

– уклонение от риска;

– изменение характера риска;

– уменьшение степени риска;

– принятие риска [9].

Взаимосвязь между элементами системы информационной безопасности говорит о том, что модель состоит из большого количества взаимодействующих субъектов и объектов это влияет на количество факторов, влияющих на оценку риска. Поэтому представляется целесообразным использовать многофакторную модель оценки информационных рисков безопасности предприятия.

Анализ риска заключается в моделировании картины наступления этих самых неблагоприятных условий посредством учета всех возможных факторов, определяющих риск как таковой. С математической точки зрения, при анализе рисков такие факторы можно считать входными параметрами.

Перечислим эти параметры:

– активы, являющиеся ключевыми компонентами инфраструктуры системы, вовлеченные в бизнес-процесс и имеющие определенную ценность;

– угрозы, реализация которых возможна посредством эксплуатации уязвимости;

– уязвимости – слабость в средствах защиты, вызванная ошибками или несовершенством в процедурах, проекте, реализации, которая может быть использована для проникновения в систему;

– ущерб, который оценивается с учетом затрат на восстановление системы в исходное состояния после возможного инцидента ИБ.

Первым этапом при проведении многофакторного анализа рисков является идентификация и классификация анализируемых входных параметров. Далее следует провести градацию каждого параметра по уровням значимости: высокий, средний, низкий. На заключительном этапе моделирования вероятного риска происходит привязка выявленных угроз и уязвимостей к конкретным компонентам ИТ-инфраструктуры.

Учитывая различные методические подходы к оценке информационных рисков, необходимо отметить, что обычно рассматривается процесс оценки и управления информационными рисками, состоящий из нескольких этапов. В специализированной литературе обобщенная модель процесса оценки и управления информационными рисками выглядит следующим образом (рисунок 4).

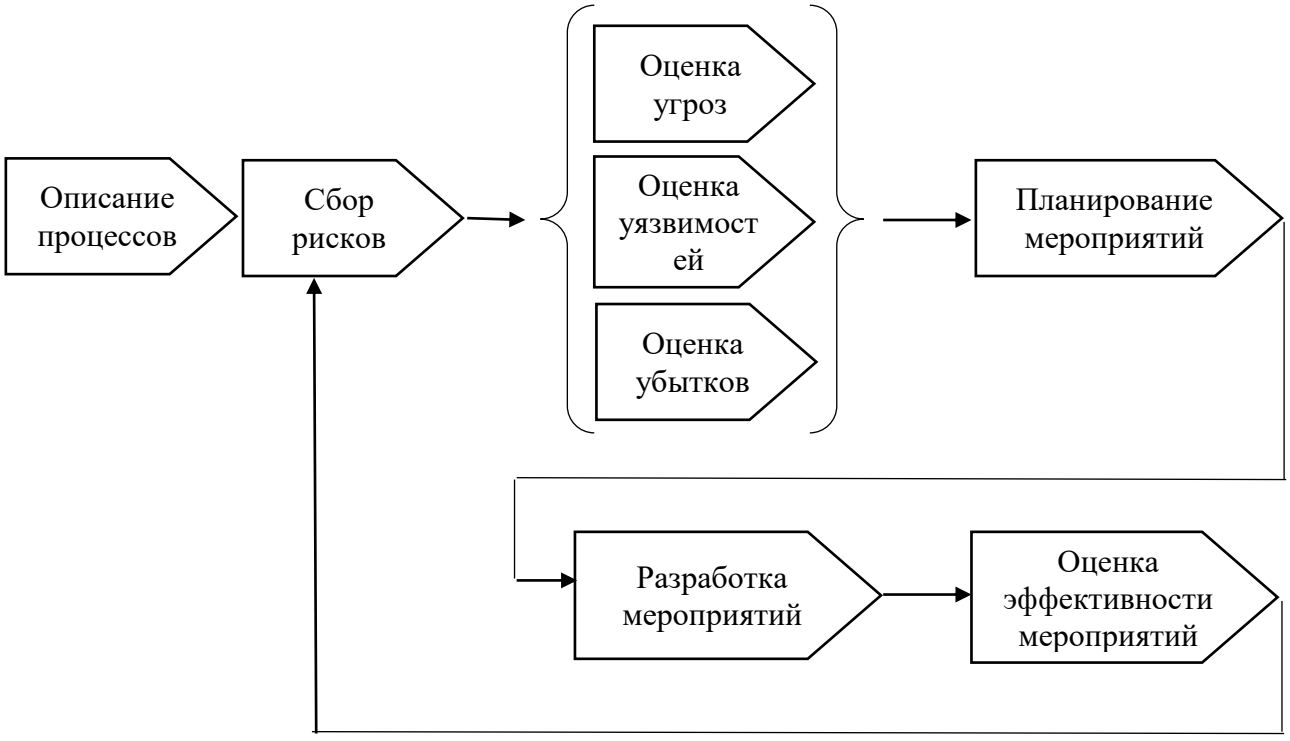

Рисунок 4 – Обобщенная модель процесса оценки и управления информационными рисками [8]

Прежде всего, необходимо определить, что является ценным активом компании с точки зрения информационной безопасности. Стандарт ISO 17799, подробно описывающий процедуры системы управления ИБ, выделяет следующие виды активов:

– информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.);

– программное обеспечение;

– материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.);

– сервисы (сервисы телекоммуникаций, системы обеспечения жизнедеятельности и др.);

– сотрудники компании, их квалификация и опыт;

– нематериальные ресурсы (репутация и имидж компании).

Следует определить, нарушение информационной безопасности, каких активов может нанести ущерб компании. В этом случае актив будет считаться ценным, и его необходимо будет учитывать при анализе информационных рисков. Инвентаризация заключается в составлении перечня ценных активов компании. Как правило, данный процесс выполняют лица, которые имеют утвержденные руководством компании обязанности по управлению созданием, разработкой, поддержанием, использованием и защитой активов.

В процессе категорирования активов необходимо оценить критичность активов для бизнес-процессов компании или, другими словами, определить, какой ущерб понесет компания в случае нарушения информационной безопасности активов. Оценка критичности активов выполняется по трем параметрам: конфиденциальности, целостности и доступности. Т.е. следует оценить ущерб, который понесет компания при нарушении конфиденциальности, целостности или доступности активов. Оценку критичности активов можно выполнять в денежных единицах и в уровнях [31].

Анализ угроз должен рассматриваться в тесной связи с уязвимостями исследуемой системы. Задачей данного этапа управления рисками является составление перечня возможных уязвимостей системы и категорирование этих уязвимостей с учетом их силы. Согласно общемировой практике, градацию уязвимостей можно разбить по уровням: критический, высокий, средний, низкий. Эти уровни более подробно представлены далее:

– критический уровень опасности. К этому уровню опасности относятся уязвимости, которые позволяют осуществить удаленную компрометацию системы без дополнительного воздействия целевого пользователя и активно эксплуатируются в настоящее время. Данный уровень опасности подразумевает, что эксплойт находится в публичном доступе;

– высокая степень опасности. К этому уровню опасности относятся уязвимости, которые позволяют осуществить удаленную компрометацию системы. Как правило, для подобных уязвимостей не существует эксплойта в публичном доступе;

– средняя степень опасности. К этому уровню опасности относятся уязвимости, которые позволяют провести удаленный отказ в обслуживании, неавторизованный доступ к данным или выполнение произвольного кода при непосредственном взаимодействии с пользователем;

– низкий уровень опасности. К этому уровню относятся все уязвимости, эксплуатируемые локально, а также уязвимости, эксплуатация которых затруднена или которые имеют минимальное воздействие

Деятельность крупных предприятий подвержена большому количеству рисков. В связи с этим для оценки рисков в них целесообразно применять полный вариант анализа рисков, предполагающий использование матрицы с предопределенными значениями. Здесь мера риска определяется исходя из предложенной указанным выше вариантом таблицы (таблица 2) на основе шкалы от 0 до 8.

Таблица 2 – Матрица оценки рисков

Показатель	Уровень угрозы	Низкая			Средняя			Высокая		
	Уровень уязвимости	н	с	в	н	с	в	н	с	в
Ценность активов	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Ценность актива определяется с точки зрения стоимости его замены, приобретения или восстановления, если это физический или программный актив, либо, если это информационный актив, его оценка определяется из опросов отдельных представителей владельцев информации. Все оценки приводятся к единой числовой шкале от 0 до 8. Далее проводится идентификация каждого вида угроз для каждой группы активов, с которыми связан данный вид угроз, чтобы провести последующую оценку. Уровень угрозы определяется как вероятность ее возникновения, а уровень уязвимости как простота использования угрозы, чтобы вызвать неблагоприятные последствия. Оценка проводится по качественной шкале от высокий до низкий. На основании полученных оценок по таблице 2 определяется мера риска:

– низкий риск: 0-2;

– средний риск: 3-5;

– высокий риск: 6-8.

Для формулирования дополнительных требований необходимо:

– определить ценность активов;

– к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

– оценить вероятности угроз;

– определить уязвимости активов [15].

В заключение следует отметить, что управление рисками предполагает несколько этапов, включая идентификацию, анализ рисков, определение необходимых мер и принятие решений, направленных на максимизацию

положительных и минимизацию отрицательных последствий рисков. Это позволит применять оптимальные по своей эффективности и стоимости средства защиты информации, соответствующие целями задачам компании. Для оценки информационных рисков предприятия, рассмотренного в следующей главе, будет использоваться полный вариант анализа рисков.

3 Анализ информационной безопасности и рекомендации по снижению рисков информационной составляющей экономической безопасности для ООО «Транснефть-Восток»

3.1 Краткая характеристика ООО «Траснефть-Восток» и его основные направления информационной безопасности

Полное название организации – Общество с ограниченной ответственностью «Траснефть-Восток». Сокращенное название – ООО «Траснефть-Восток». Компания зарегистрирована Межрайонной инспекция ФНС России № 15 по Иркутской области24 января 2006 г. Организация располагается по адресу: 665734, Иркутская область, город Братск, жилой район Энергетик, Олимпийская улица, 14.

Общество с ограниченной ответственностью «Транснефть–Восток»является одним из самых молодых предприятий в структуре ПАО «Транснефть». Выступая инвестором строительства нефтепроводной системы «Восточная Сибирь– Тихий Океан» и осуществляя ее эксплуатацию, компания, созданная в августе 2009 года, способствует развитию территории Дальнего Востока.

ООО «Транснефть–Восток» выступает гарантом социальной стабильности в местах осуществления своей деятельности. Предприятие проводит целевое обучение местных жителей, в дальнейшем обеспечивая 100% трудоустройство успешно окончивших образовательные курсы. Предприятие способствует занятости большого количества подрядных организаций, а также выполняет обязательства перед региональными и местными бюджетами своевременно и в полном объеме.

Основным видом деятельности ООО «Транснефть–Восток» является «Транспортирование по трубопроводам нефти». Помимо основного вида деятельности, зарегистрировано и дополнительные виды деятельности:

– добыча декоративного и строительного камня, известняка, гипса, мела и сланцев;

– разработка гравийных и песчаных карьеров, добыча глины и каолина;

– ремонт машин и оборудования;

– строительство жилых и нежилых зданий;

– строительство инженерных коммуникаций для водоснабжения и водоотведения, газоснабжения;

–строительство междугородних линий электропередачи и связи;

– деятельность сухопутного пассажирского транспорта: внутригородские и пригородные перевозки пассажиров;

– деятельность автобусного транспорта по регулярным внутригородским и пригородным пассажирским перевозкам;

– хранение и складирование нефти и продуктов ее переработки;

– деятельность в области инженерных изысканий, инженерно-технического проектирования, управления проектами строительства, выполнения строительного контроля и авторского надзора, предоставление технических консультаций в этих областях;

– деятельность по обеспечению общественного порядка и безопасности[18]

Организационная структура ООО «Транснефть – Восток»представлена аппаратом управления и четырьмя филиалами (рисунок 5).Общество занимает одно из центральных мест в производственной деятельности ПАО «Транснефть», обеспечивает бесперебойную работу важного участка стратегической нефтепроводной системы «Восточная Сибирь – Тихий океан», ее международной составляющей – нефтепровода «Сковородино-Мохэ». Запуск ВСТО дал мощный импульс в развитии месторождений сибирского региона.

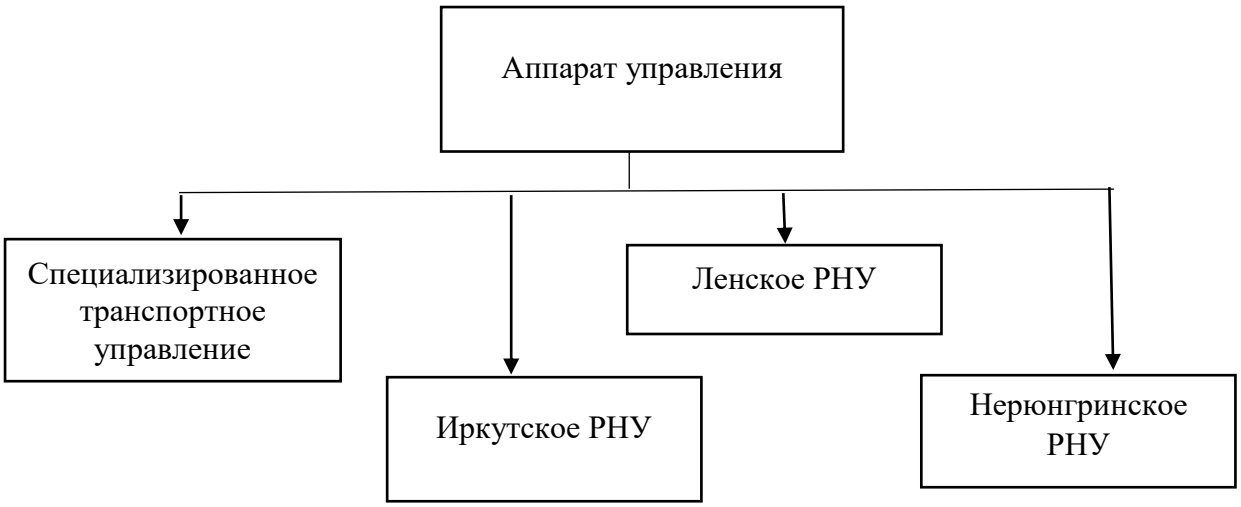

Рисунок 5 – Организационная структура ООО «Транснефть – Восток»

Коллектив предприятия в трех регионах страны насчитывает 6 тысяч человек и продолжает расти.

Ниже в таблице 3 представлены экономические показатели деятельности организации.

Таблица 3 – Экономические показатели деятельности ООО «Транснефть – Восток» за 2017-2019 гг.

Название показателя	2017	2018	2019	2018 к 2017		2019 к 2018	
				тыс. руб.	%	тыс. руб.	%
Выручка, млн. руб.	93795,00	106396,00	90117,00	12601,00	13,43	-16279,00	-15,30
Себестоимость продаж, млн. руб.	64508,00	74052,00	72940,00	9544,00	14,80	-1112,00	-1,50
Прибыль от продаж, млн. руб.	29287,00	32344,00	17177,00	3057,00	10,44	-15167,00	-46,89
Прочие доходы, млн. руб.	31757,00	18006,00	2400,00	-13751,00	-43,30	-15606,00	-86,67
Прочие расходы, млн. руб.	26104,00	15405,00	3862,00	-10699,00	-40,99	-11543,00	-74,93
Прибыль до налогообложения, млн. руб.	17077,00	15861,00	1377,00	-1216,00	-7,12	-14484,00	-91,32

Окончание таблицы 3

Налог на прибыль, млн. руб.	2376,00	2593,00	533,00	217,00	9,13	-2060,00	-79,44
Чистая прибыль, млн. руб.	13208,00	11209,00	2526,00	-1999,00	-15,13	-8683,00	-77,46

В 2018 году финансовые показатели Компании заметно выросли в результате увеличения выручки от транспортировки нефти и нефтепродуктов, а также в связи с приобретением в сентябре 2018 года контроля в Группе ПАО «НМТП». В связи с приобретением контроля была проведена переоценка до справедливой стоимости уже имевшейся у Группы косвенной доли в ПАО «НМТП»на дату приобретения контроля. В 2019 году отмечается значительное ухудшение практически всех показателей деятельности компании по сравнению с 2018 годом. Наблюдается снижение выручки от продаж на 15,3%, однако себестоимость снизилась лишь на 1,5%, явившееся следствием колебаний цен на нефть. В 2019 году более чем на 80 % уменьшились прочие доходы компании вследствие ухудшения показателей деятельности подконтрольных ООО «Транснефть – Восток» предприятий, что также негативно отразилось на финансовых результатах компании. Существенное падение отмечается по показателям прибыли до налогообложения и чистой прибыли. В целом, можно отметить, что результаты деятельности компании в 2019 году существенно ухудшились, о чем свидетельствуют данные бухгалтерской отчетности.

Основными направлениями организации в сфере обеспечения информационной безопасности являются следующие:

– установление особенностей хранения и передачи информации, определение основных видов угроз и предполагаемых каналов утечки информации предприятия;

– создание концепции и выбор принципов формирования системы защиты информации, разработку структуры системы защиты хранения, обработки и передачи информации;

– подготовка критериев оценки защиты информации;

– разработка либо выбор из уже имеющихся средств программного обеспечения защиты информации;

– создание системы физических мероприятий охраны устройств и носителей информации, предполагающей охрану территории предприятия, на которой размещены автоматизированные информационные системы с применением технических средств и специального персонала, пропускной режим, соблюдение противопожарных требований;

– использование программно-технических средств для защиты от несанкционированного доступа к информации.

В заключение следует отметить, что ООО «Транснефть-Восток» одним их предприятий, входящих в структуру ПАО «Транснефть».

В своей деятельности предприятие придерживается основных направлений обеспечения информационной безопасности, среди которых использование физических мероприятий и программно-технических средств, для защиты конфиденциальной информации, формирование целостной системы защиты информации.

3.2 Оценка основных организационных мер и программно-аппаратных средств информационной безопасности, используемых на предприятии для обеспечения информационной защищенности

Все ИТ-ресурсы ООО «Транснефть – Восток» можно разделить на три группы:

1)информация, относящаяся к коммерческой тайне;

2) конфиденциальная информация;

3) строго конфиденциальная информация.

Сведения, входящие в составе этих групп, указаны в таблице 4.

Таблица 4 – Перечень сведений ООО «Транснефть – Восток», носящих конфиденциальный характер

Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, №№ статей
1. Информация о структуре производства предприятия, производственных мощностях, типах оборудования и их размещении, сведения о запасах материальных ресурсов	строго конфиденциально	Указ президента РФ №188
2. Сведения о планируемых инвестициях, закупках, продажах	коммерческая тайна	Указ президента РФ №188
3. Сведения о банковских счетах организации и осуществляемых операциях	строго конфиденциально	Федеральный закон №98-ФЗ ст.11
4. Сведения о состоянии компьютерного и программного обеспечения	конфиденциально	Федеральный закон №98-ФЗ ст.11
5. Сведения о применяемых и разрабатываемых технологиях и их специфике	конфиденциально	Федеральный закон №98-ФЗ ст.11

На сегодняшний день насчитывают около 30 разных видов конфиденциальной информации, что требует особого внимания к обеспечению их информационной безопасности. Важным условием является подписание пользователями информационных средств организации соответствующих обязательств по отношению к конфиденциальной информации (соглашение о неразглашении). Как правило, служащие обычно подписывают такие обязательства в качестве основных условий при приеме на работу. Следует отметить, что договор о соблюдении неразглашении информации необходимо пересматривать в случае изменения условий приема на работу и так же в случаях увольнения служащего и при окончании срока действия договора.

Попадание секретной информации к конкурентам может повлечь различные негативные последствиям для организации, а именно деятельности и престижу компании, ущерб материальным активам, потере важных клиентов.
Информация об оценке активов ООО «Транснефть – Восток» представлена в приложении В.

После проведения оценки информационных активов организации следует провести их ранжирование для дальнейшего выявления актуальных и неактуальных угроз, и формирования технических мер для защиты. Итоги ранжирования активов ООО «Транснефть – Восток» представлены в таблице 5.

Таблица 5 – Результаты ранжирования активов ООО «Транснефть – Восток»

Наименование актива	Ценность актива (ранг)
Сведения делового характера	4
Информация по торгово-экономической деятельности	4
Информация о предоставляемых услугах	5
Информация по вопросу обеспечения информационной безопасности	5
Сведения по организационно-управленческой деятельности предприятия	2
Продукция компании	3
Оборудование	3

Активы, которые имеют наибольшую ценность:

-информация об оказанных услугах;

-сведения по вопросу обеспечения безопасности;

-сведения чисто делового характера;

-сведения по торгово-экономическим вопросам;

-продукция предприятия;

-оборудование;

-информация по организационно-управленческой деятельности.

Высшим руководством организации ПАО «Транснефть» в лице генерального директора было разработано положение об информационной политике безопасности для структурных подразделений компании. Политика безопасности выступает результатом совместной деятельности технического персонала, понимающего все аспекты политики компании и ее реализации, а также генерального директора, обладающего полномочиями влияния на политику.

Один из пунктов этого положения гласит, что с целью обеспечения информационной безопасности на должном уровне ежегодно должна

проводиться внутренняя аудиторская проверка, соответствующая правовым и законодательным документам по аудиторской деятельности РФ. В ходе проверки используется детальный анализ риска, предполагающий оценку уязвимости активов.

Уязвимость информации – возможность возникновения состояний, содержащих условия для реализации угрозы безопасности данным предприятия. Наличие уязвимости само по себе не наносит ущерба, это возможно лишь при наличии соответствующих угроз. Уязвимость информации не требует применения защитных мер в случае отсутствии таких угроз. Однако уязвимости следует зафиксировать и в дальнейшем проверить на случаи изменения ситуации.

Данные виды оценок предусматривают проведение идентификации уязвимости в окружающей среде, предприятиях, персонале, процедурах, администрации, менеджменте, программном обеспечении, аппаратных средствах и аппаратуре связи, которые могут использоваться в качестве источников угроз для причинения ущерба активу и деловому функционированию предприятия, которые проводятся с их применением. Следует отметить, что неправильно используемые, а также некорректно работающие защитные меры могут сами выступать источником возникновения уязвимости. Результат оценки уязвимости активов ООО «Транснефть – Восток» проводилась следующим образом: выбирался вид деятельности в организации, связанный с информационной составляющей – активом деятельности и по выбранным критериям определения стоимости, давалась оценка от средней до очень высокой. Процедура проводилась собранной специально группой специалистов, оценка информационных активов предприятия представлена в приложении В.

Положение об информационной безопасности было сформировано генеральным директором ПАО «Транснефть». Согласно этому положению задачи по обеспечению информационной безопасности возложены на системного администратора. Проверка предполагает внутренний аудит, по

окончании которого составляется заключение в письменной виде и передается генеральному директору, который принимает окончательное решение по внедрению и совершенствованию конкретного защитного модуля.

Информационная система ООО «Транснефть – Восток» представляет собой комплекс рабочих станций и серверов, которые объединены в единую локальную сеть. Обработка и хранение информации осуществляются на рабочих станциях и на файловом сервере.

Локальная вычислительная сеть создана с учетом единых концептуальных положений, в основе которого лежит использование общих принципов построения сетевого оборудования. При выборе компонентов сети компания руководствуется следующими требованиями:

–компьютерная техника должна отличаться хорошим быстродействием для обеспечения работы всех служб и приложений в реальном времени без существенных задержек в работе;

–жесткий диск компьютера должен отличаться максимальной надежностью для обеспечения безопасности и целостности хранимой информации;

– установка сетевых принтеров должна учитывать местоположение пользователя, который активно им пользуется;

–коммутаторы, являющиеся центральными устройствами такой сети, должны располагаться в легкодоступных местах для возможности подключения кабеля и слежения за индикациями.

В утвержденном положении об информационной безопасности генеральным директором ПАО «Транснефть» установлено, что по итогам внутреннего аудита, возложенного на системного администратора, будет представлено заключение в письменном виде о суммарной оценке риска с детальным анализом риска для выбора в дальнейшем комплекса мероприятий по защите информации.

На заключительных стадиях анализа рисков осуществляют суммарную оценку рисков. Оценка рисков представляет собой оценку соотношения

влияния негативных факторов на деятельность предприятия в случае реализации нежелательного инцидента и степени выявленной угрозы и уязвимых мест. Фактически риски выступают мерой незащищенности системы безопасности и связанного с ними предприятия. Величина рисков обусловлена рядом факторов:

–уровень ценность актива;

–выявленные угрозы и вероятность их реализации;

–возможность реализации угрозы в наиболее уязвимом месте с дальнейшим нежелательным воздействием;

–наличие существующего либо планируемого средства защиты, направленного на снижение степени уязвимости, устранение угрозы и нивелирования нежелательного воздействия.

Следует отметить, что выбор методики оценки риска осуществляется полностью по усмотрению лица, которое проводит этот анализ. В данном случае это системный администратор группа специалистов, которая собирается по усмотрению руководящего лица. В качестве определяющего фактора выбора выступает удобство для организации и доверие к методу. В данном случае применяется метод с использованием матрицы в виде таблицы с заранее установленными значениями.

Суть этого подхода заключается в установлении наиболее критичного актива в организации с точки зрения рисков информационной безопасности по «штрафному баллу». Оценка риска осуществляется экспертной комиссией, собранной заранее и утвержденной руководителем отдела экономической безопасности. Проводится она на основе анализа ценности актива, вероятности реализации угрозы и использования уязвимости, рассчитанной в предыдущем пункте. Для оценки применяются таблицы, в которых заранее определены «штрафные баллы» для каждой комбинации ценности актива, степени угрозы и уязвимости. После оценки актива всеми установленными уязвимостями и угрозами рассчитываем сумма штрафных баллов. Окончательная сумма

является итоговой мерой риска, на основании которой осуществляется ранжирование рисков на предприятии.

Оценка проводится следующим образом: идентифицируются соответствующие ряды матриц в зависимости от ценности активов, а соответствующая колонка– по уровню угроз и уязвимостей. К примеру, если ценность актива равняется 4, то угроза характеризуется как «высокая», а степень уязвимости– как «низкий», при этом мера риска будет равна 5. Если существует уязвимость без соответствующих угроз информационной безопасности, то считают, что в настоящий момент риски отсутствуют.

Показатель риска в используемой таблице варьируется в шкалах от 0 до 8 с определениями степени рисков:

− 1 − риски почти отсутствуют, в теории возможно наступление события, но на практике это случается редко, а величина потенциального ущерба сравнительно невелика;

− 2 − риски достаточно малы, события подобного рода случаются редко, негативные последствия невелики;

− 8 − риски достаточно велики, событие вероятнее всего наступит, и последствия будут тяжелыми и т.д.

В таблице 6 представлена применяемая для оценки шкала.

Таблица 6 – Оценки рисков ООО «Транснефть – Восток»

	Уровень угрозы	Низкая			Средняя			Высокая		
	Уровень уязвимости	н	с	в	н	с	в	н	с	в
Ценность активов	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Результаты проведения оценки рисков ООО «Транснефть – Восток» представлены в таблице 7.

Таблица 7 – Результаты оценки рисков ООО «Транснефть – Восток»

Риск (в штрафных баллах)	Актив	Ранг риска
6	Информация о предоставляемых услугах	1
22	Информация по вопросам обеспечения безопасности предприятия	2
27	Сведения делового характера	3
46	Информация по торгово-экономическим вопросам	4
47	Оборудование	5
60	Информация по организационно-управленческой деятельности предприятия	6
61	Продукция организации	7

Исходя из анализа рисков в ООО «Транснефть – Восток»,определены следующие виды угроз информационной безопасности, для которых в дальнейшем будет разрабатываться система защиты:

1) угрозы нарушения конфиденциальности информации. Конфиденциальность – это характеристика информации, предполагающая запрет на получение информации неавторизованному пользователю, то есть пользователю, не обладающему привилегиями на получение такой информации. Хранение и просмотр ценной информации доступен только людям, которым она предназначена по их служебным обязанностям и полномочиям.

Конфиденциальность используется для защиты передаваемой информации от пассивных атак, то есть для защиты потоков информации от возможностей их аналитических исследований. Это делает невозможным для нарушителей обнаружение источников информации и их содержимого. Основным способом обеспечения конфиденциальности является шифрование информации с применением ключей пользователей. При этом содержание информации доступно только владельцу ключа, содержащего зашифрованные данные. Обеспечение данной характеристики является одной из наиболее важных задач, поскольку в случае нарушения целостности и доступности данных вследствие порчи или воровства ее можно восстановить из архива, а в

случае нарушения конфиденциальности информация становится общедоступной и повлечь огромные убытки;

2) угрозы нарушения целостности данных. Целостностью является характеристика информации, предполагающая невозможность модифицирования информации неавторизованным пользователем. Поддержание целостности ценных секретных данных обозначает защиту от неправомочных модификаций. Существует большое количество видов информации, обладающих ценностью только тогда, когда есть гарантия правильности информации.

Основными задачами мероприятий по обеспечению целостности информации являются возможности выявления случаев модификации, факта отсутствия повреждений информации, разрушений или изменений иным способом. С искажением информации связан полный контроль над информационными потоками между звеньями системы и возможности получения сообщений от других пользователей. Для сохранения целостности информации используются разные виды цифровых подписей либо однонаправленную функцию хеширования;

3) угрозы нарушения доступности. Доступностью называются свойства ресурсов системы, заключающиеся в том, что пользователи либо процессы, у которых есть соответствующие полномочия, могут пользоваться ресурсами в соответствии с правилами, установленными политикой безопасности. Обеспечение доступности информации и информационной системы и готовности к их применению в случае необходимости. В данном случае необходимы гарантии доступности данных и поддержания их в состоянии, пригодном для использования;

4) угрозы нарушения наблюдаемости данных. Наблюдаемость предполагает свойства информационных систем, позволяющие фиксирование деятельности пользователей и процессов, применение пассивного объекта, а также однозначное трактование идентификаторов, которые причастны к определенному событию пользователя или процесса для нарушения политики

безопасности либо сокрытия фактов ответственности за конкретное событие, которое имело место;

5) угрозы нарушение аутентичности информации. Аутентичность информации обеспечивается с помощью процедур аутентификации. Под аутентификацией понимают процедуры проверки соответствия предъявляемых идентификаторов объектов на предмет отнесения их к таким объектам. Угроза нарушения аутентичности состоит в выдаче себя при проведении некоторых действий за других пользователей и возможности использовать чужие права и привилегии.

В заключение можно сделать вывод о том, что в ООО «Транснефть-Восток» при оценке рисков используется подход, предполагающий применение матриц, оформленных в виде таблицы с заранее установленными значениями. Этот подход предусматривает определение наиболее критичного актива предприятия в плане оценки рисков информационной безопасности по «штрафному баллу». На основании анализа, проведенного с использованием такого подхода, был выявлен ряд угроз информационной безопасности предприятия, включающий угрозы нарушения конфиденциальности информации, аутентичности информации, нарушения наблюдаемости данных, нарушения целостности данных.

3.3 Разработка мероприятий по снижению информационных рисков для ООО «Транснефть-Восток»

Защита информации – важное условие функционирования предприятия, поэтому, чтобы выявить уязвимость системы, требуется комплексный подход. Для того чтобы задачу выявления уязвимости упростить, требуется разработать такую базу данных, которая будет рассчитывать защищенность системы и ее составляющих. Формирование базы данных невозможно без правильно подобранной методики расчётов рисков информационной безопасности. Созданная методика позволит сделать построение базы проще, с помощью чёткой систематизации данных и выделения необходимых аспектов защиты.

Суть методики заключается в определении показателя риска информационной безопасности в количественном выражении, для дальнейшего принятия мер по защите информации. Возможная методика расчёта рисков будет делиться на пять стадий:

1)стадия первая – интервью**.** Здесь эксперты проводят интервью с каждым сотрудником, для выяснения информации об используемых в работе активов. Технологии, связанные с использованием информации, являются одним из важных компонентов общей системы, в которые компания инвестирует значительную часть средств и которым важна защита от внешних и внутренних угроз. Стоит обратить внимание на то, что при определении используемых активов, в состав каждого входят аппаратные и программные средства, которые тоже должны подвергаться надёжной защите;

2) стадия вторая–проверка на соответствие требованиям законодательства в области информационной безопасности**.** Каждое предприятие при использовании информационных систем, должна соблюдать федеральные законы в этой отрасли. Обратное может повлечь за собой непоправимые последствия. Для анализа на соответствие требований законодательства в области информационной безопасности необходимо провести всесторонний анализ состояния системы защиты, для того чтобы определить выполняются ли

требования законодательства. Выполняемым требованиям, присваивается значение «1», тем требованиям, которые были не выполнены – значение «0». Все значения с «1», суммируются, остальные отбрасываются и не учитываются. В конце анализа нужно определить уровень риска несоответствия требований по информационной безопасности, который определяется по таблице 8;

Таблица 8 – Уровень риска несоответствия требованиям законодательства

Сумма выполненных требований, баллов	Риск несоответствия законодательству (R_n)
40-51	0,01
27-39	0,25
Менее 26	0,5
Не выполняются	0,9

3) стадия три – разработка модели угроз. Для максимальной точности определения риска информационной безопасности необходимо разработать частную модель угроз информационной безопасности предприятия. Эксперт, а чаще всего группа экспертов осуществляют разработку модели угроз, с помощью расчёта вероятности возникновения неблагоприятного события. После проделанной оценки угроз, на каждый актив или группу активов создаётся список обнаруженных угроз, а также определяется вероятность наступления угроз;

4) стадия четыре – самая трудоёмкая – это количественная оценка рисков информационной безопасности. В процессе оценки рисков главной является процедура количественного оценивания рисков. Поэтапный алгоритм показан на рисунке 6.

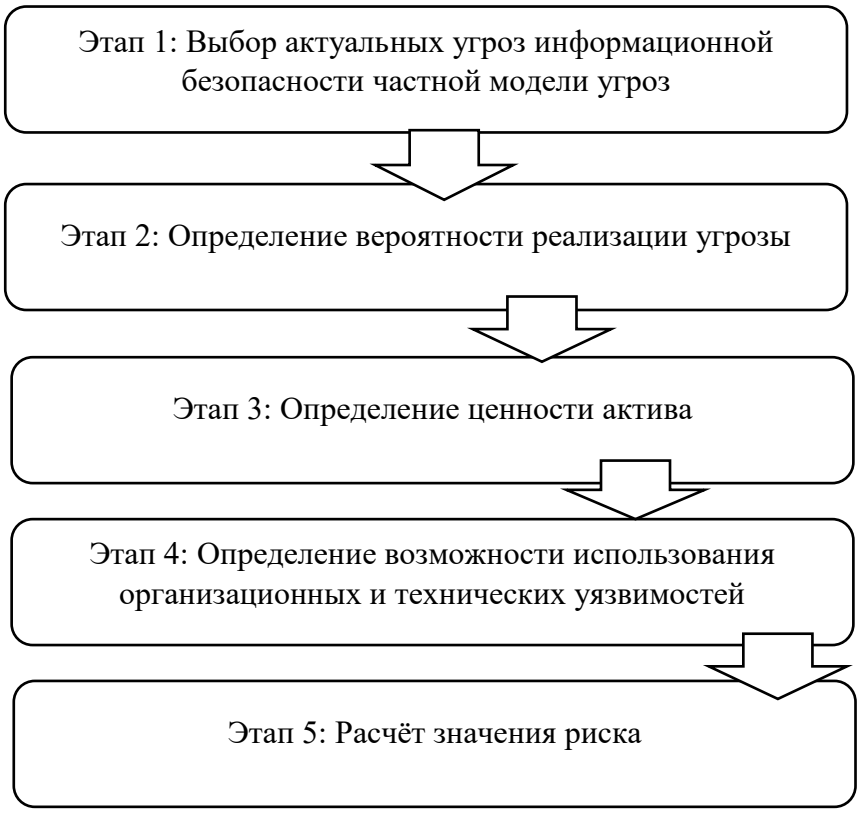

Рисунок 6 – Поэтапный алгоритм оценки рисков

Этап 1. Выбор актуальных угроз информационной безопасности частной модели угроз. На этом шаге используют частную модель угроз и формируют список актуальных угроз информационной безопасности активов предприятия.

Этап 2. Определение вероятности реализации угрозы. Из-за того, что на один актив могут воздействовать сразу несколько угроз, следует определить шанс реализации каждой из них. Вероятность воплощения хотя бы одной из возможных угроз y1, y2, ..., yn, где n – количество угроз, равняется разности единицы и произведения вероятностей противоположных событий. Вероятность противоположных событий определяется как разность единицы и вероятности угроз.

Этап 3. Определение ценности актива. Ценность актива зависит от стоимости информационного актива. В большинстве случаев определение точной стоимости активов и компании в целом невозможно, поэтому чаще всего ценность актива находится в диапазоне чисел от 0 до 1 и показывает отношение стоимости актива к стоимости бизнеса в целом.

Этап 4. Определение использования организационных и технических уязвимостей. Эксперты, собранные специальной комиссией, анализируют используемые организационные меры защиты для определения доли уязвимости. В ходе анализа всем выполняемым организационным мерам присваивается значение «1», которые не исполняются – значение «0». Далее суммируются только значения «1», «0» не учитываются.

В таблице 9 представлено соответствие выполняемых мер защиты информации и коэффициент уязвимости организационных мер информационной защиты. Возможность использования технических уязвимостей проводится экспертным методом, на основе анализа применяемых технических мер защиты информации. Во время выполнения анализа всем выполняемым организационным мерам присваивается значение «1», которые не исполняются – значение «0». Далее все значения «1» суммируются, остальные не учитываются.

Таблица 9 – Соответствие выполняемых организационных мер защиты информации и коэффициентов уязвимости организационных мер защиты информации

Сумма применяемых мер защиты, баллов	Показатель уязвимости (k_0)
14-17	0,01
8-13	0,25
Менее 8	0,5
Не выполняются	0,9

В таблице 10 показано соответствие применяемых технических мер по защите информации и показатель их уязвимости.

Таблица 10– Соответствие выполняемых технических мер защиты информации и коэффициентов уязвимости технических мер защиты информации

Сумма применяемых мер защиты, баллов	Показатель уязвимости (k_t)
15-19	0,01
9-14	0,25
Менее 9	0,5
Не выполняются	0,9

Этап 5.Расчёт значения риска. Процедура оценки рисков реализации включает в себя ряд факторов: коэффициент ценности актива, вероятность происшествия, среднеарифметическое значение коэффициентов возможности применения организационных уязвимостей и возможность применения технических уязвимостей и риска несоответствия требованиям законодательства. Коэффициент ценности актива показывает ценность информационной безопасности и критичность актива по отношению к бизнесу в целом.

В данной методике процесс количественной оценки риска реализации хотя бы одной из угроз, входящих в перечень актуальных угроз по отношению к конкретному активу угроз устанавливается для каждого типа актива, на который оказывает воздействие совокупность угроз информационной безопасности, что способствует дискретному определению риска наступления неблагоприятных событий для каждого типа актива. Формула (5) расчета риска реализации угроз из перечня актуальных угроз с учетом уязвимостей для конкурентного актива выглядит следующим образом:

$$R = P_{\text{угр}} R_n C \frac{k_0 + k_t}{2} 100\%, \quad (5)$$

где R, % – уровень риска возникновения угроз информационной безопасности в числовом выражении;

Ругр – вероятность появления хотя бы одной из угроз, входящих в перечень актуальных угроз;

Rn – риск несоответствия установленным требованиям законодательства;

С – ценность информации;

Ko – вероятность использования уязвимостей;

Kt – вероятность использования технических уязвимостей;

5) стадия пять – определение допустимого риска. Допустимым риском считается риск, который считается приемлемым в данной ситуации при существующих общественных ценностях. Расчет допустимого риска требуется для того, чтобы не затрачивать лишние ресурсы. Если угроза существует, но шансы на ее последующую реализацию, со стороны злоумышленников крайне малы, то в большинстве случаев затраты ресурсов на ее устранение попросту бессмысленны.

После проводим оценку уровня рисков для активов предприятия по предложенной методике. Для этого выбирается несколько значимых активов информационной составляющей предприятия и каждому из них присваивается значение, рассчитанное по приведенным выше формулам. Результаты оценки рисков предприятия представлены в Приложении Г.

Рекомендованное значение риска не должно превышать 5 %. По итогам таблицы можно отметить, что уровень риска по всем исследуемым активам предприятия соответствует рекомендованному значению. Это свидетельствует о высокой степени защиты информации предприятия.

Наибольший уровень риска информационной безопасности отмечается по следующим активам:

– условия индивидуальных трудовых договоров с работниками и руководителями;

– планы и методы продвижения услуг на рынок;

–ИНН, документы об уплате налогов и обязательных платежах;

– детальные планы финансовых вложений в развитие организации.

Это обусловлено воздействием ряда различных факторов. Так, высокий уровень риска по перечисленной информации связан с повышенной вероятностью использования организационных и технических уязвимостей, а также высокой ценностью указанной информации для предприятия.

На основании полученных результатов рекомендуется в рамках управления информационными рисками предприятия внедрять и использовать существующие политики безопасности. В основу разработки политики безопасности можно положить международные стандарты безопасности информационных систем, в частности ISO 17799. Таким образом, можно рекомендовать ряд мероприятий, направленных на повышение информационной безопасности предприятия. К ним относятся:

–использование только лицензионного авторизованного программного обеспечения;

–обеспечение безопасности файлов и программного обеспечения, полученных из внешних сетей, через внешние сети или из любой другой среды;

–разграничение обязанностей, направленное на минимизацию риска нештатного использования информации пользователями;

–резервное копирование важной служебной информации и программного обеспечения на постоянной основе;

–обеспечение постоянного контроля за сетевыми ресурсами;

–использование сменных носителей информации и своевременная их утилизация;

–контроль доступа к информации со стороны сотрудников и третьих лиц и т. д.

Предложенные рекомендации могут быть использованы на любом предприятии в процессе управления информационными рисками и при разработке системы управления информационной безопасностью предприятия.

В заключение можно отметить, что для успешного выявления уязвимостей информационной безопасности ООО «Транснефть-Восток» необходимо создать базу данных, которая рассчитывает защищенность системы информационной безопасности. Для формирования базы данных была рекомендована методика оценки рисков информационной безопасности. Создание такой методики позволяет упростить задачу формирования базы данных при помощи систематизации данных и определения необходимых направлений защиты. Эта методика построена на определении численного показателя риска информационной безопасности для дальнейшего принятия мер по защите информации. Таким образом, создание данной методики выступает ключевым фактором в формировании базы данных.

ЗАКЛЮЧЕНИЕ

Любая компания в процессе своей деятельности постоянно подвергается влиянию различных факторов, они могут негативно отразиться на результатах ее хозяйственной деятельности. Экономическая безопасность организации представляет собой состояние защищенности предприятия от влияния внутренних и внешних факторов, позволяющее ему более эффективно использовать свой экономический потенциал в процессе снижения и устранения существующих рисков в процессе достижения главной цели коммерческой деятельности.

В современных условиях постоянного роста известных и возникновения новых видов информационных угроз усиливается актуальность обеспечения надежной защиты информационных ресурсов предприятия. И информационная безопасность предприятия выступает одной из составляющих элементов экономической безопасности и представляет собой состояние защищенности информации, обеспечивающее ее целостность, конфиденциальность, аутентичность и доступность.

Основной целью экономической безопасности предприятия является обеспечение устойчивости и результативности его работы в настоящее время и развитие предприятия в перспективе, что требует определенного набора методов и подходов. В основе системы экономической безопасности предприятия лежит ряд принципов, таких как комплексность, приоритетность мер предупреждения, непрерывность, законность, экономность, взаимодействие, компетентность и плановость.

Элементами экономической безопасности являются финансовая безопасность, кадровая, информационная, технико-технологическая, политико-правовая. Решение всех поставленных перед специалистами экономической безопасности задач, требует создания целостной системы, отраженной в концепции по обеспечению экономической безопасности предприятия.

Обладая информационными ресурсами, предприятию необходимо

проверять и защищать их для обеспечения экономической безопасности в целом. Оценка уровня экономической безопасности организации требует определения критериев экономической безопасности организации.

Анализу информационных рисков в настоящее время отводится важное место в структуре экономической безопасности предприятия. Подходы к оценке и управлению информационными рисками обусловлены сферой деятельности объекта и его целями. Анализ методических подходов и инструментов, которые используются для оценки информационных рисков, позволяет сделать вывод о необходимости комплексной системы защиты информации. В настоящее время не существует какой-либо единой универсальной для большинства предприятий методики, необходима адаптация общей методики оценки информационных рисков под потребности конкретного предприятия на основании специфики его деятельности. Процесс управления рисками включает ряд этапов: идентификацию, анализ рисков, определение необходимых мер и принятие решений, направленных на максимизацию положительных и минимизацию отрицательных последствий рисков.

В качестве объекта исследования в работе было выбрано общество с ограниченной ответственностью «Транснефть-Восток»,входящее в состав структуры ПАО «Транснефть». Основной вид деятельности ООО «Транснефть-Восток» – транспортирование по трубопроводам нефти. Основными направлениями обеспечения информационной безопасности предприятия являются физические мероприятия и программно-технические средства защиты конфиденциальной информации, формирование целостной системы защиты информации.

Анализ методических подходов, используемых на предприятии для обеспечения информационной защищенности, позволил сделать вывод о том, что ООО «Транснефть-Восток» при оценке рисков применяет подход, в основе которого лежат матрицы, оформленные в виде таблицы с заранее установленными значениями. Такой метод предусматривает выявление наиболее критичного актива компании в плане оценки рисков информационной

безопасности по «штрафному баллу». По результатам проведенного с применением данного подхода анализа были определены угрозы информационной безопасности предприятия, к которым относятся нарушение конфиденциальности информации, аутентичности информации, нарушение наблюдаемости данных, нарушение целостности данных.

В качестве меры совершенствования оценки рисков информационной безопасности предприятия было рекомендовано использование разработанной автором методики, которая позволяет определять защищенность системы информационной безопасности и производить расчет рисков информационной безопасности. Она направлена на систематизацию данных и определение необходимых направлений защиты. В основу такой методики положено определение численного показателя риска информационной безопасности для дальнейшей разработки мероприятий по защите информации. Применение рекомендованной методики на практике позволит повысить уровень информационной безопасности предприятия и экономической безопасности предприятия в целом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" (с изменениями и дополнениями от 23 сентября 2005 г., 13 июля 2015 г.)
2. Указ Президента Российской Федерации от 12 мая 2009 г. N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года"
3. О коммерческой тайне: федер. закон Российской Федерации от 29 июля 2004г. № 98- ФЗ: офиц.текст – Москва: Эксмо, 2017. – 16с.
4. О безопасности [Электронный ресурс]: фед. закон от 5.03.1992 № 2446-1 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/
5. Распоряжение Правительства Российской Федерации «Цифровая экономика Российской Федерации» от 28.07.2017 г. №1632-р/Консультант Плюс . - Режим доступа: http://www.consultant.ru (дата обращения: 06.01.2019).
6. Абалкин Л. И. Экономическая безопасность России: угрозы и их отражение// Вопросы экономики. 2014. № 12.
7. Архипов А., Городецкий А., Михайлов Б. Экономическая безопасность: оценки, проблемы, способы обеспечения // Вопросы экономики. 2015. № 12.
8. Бабаш, А.В. Информационная безопасность. Лабораторный практикум : Учебное пособие / А.В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – М.:КноРус, 2016. – 136 с.
9. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга [Текст] / Журнал «Вопросы кибербезопасности» – 2018. - № 1 (25). – С. 28-38.
10. Бетелин В. Б. Суперкомпьютерные технологии в России: состояние и проблемы развития// Вестник Российской академии наук. Т. 85, № 11. 2015. С. 971-975.
11. Экономическая безопасность : учебник для вузов / под общ. ред. Л. П. Гончаренко. — 2-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 340 с. — (Серия : Специалист).
12. Байнев В. Ф. Экономика предприятия и организация производства. Учебное пособие для студентов вузов / В. Ф. Байнев. – М.: Издательство ДИС, 2015. – 321 с

13. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. –М.:Риор, 2017. – 400 с.
14. А. Бирюков "Информационная безопасность: защита и нападение" 2-е изд. (2017)-350
15. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. –М.: Форум, 2015. – 368 с.
16. Гафнер, В.В. Информационная безопасность: Учебное пособие / В. В. Гафнер. –Рн/Д: Феникс, 2017. – 324 с.
17. Глобальное исследование утечек конфиденциальной информации в 2017 году // Аналитический центр InfoWatch, 2018. - 23 с.
18. Глухов, Н. И. Оценка информационных рисков предприятия : учебное пособие / Н. И. Глухов – Иркутск : ИрГУПС, 2013. – 148 с.
19. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечениябезопасности». НациональныйстандартРФ. Часть 3. Методы менеджмента безопасности информационных технологий». Приказ Федерального агентства по техническому регулированию и метрологии от 7 июня 2007 г. № 122-ст. Режим доступа: https://www.altell.ru/legislation/standards/13335-3.pdf
20. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2010. – 384 с.
21. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. –М.: Форум, 2015. – 240 с.
22. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.
23. Карзаева Н.Н., Бабанская А.С. Экономическая безопасность. Учебное пособие/Н.Н. Карзаева, А.С. Бабанская. -М.: Изд-во РГАУ-МСХА им К.А. Тимирязева, 2016. -290 с

24. Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. –М.:КноРус, 2013. – 136 с.
25. Кругликов С.В., Дмитриев В.А., Степанян А.Б., Максимович Е.П. Информационная безопасность информационных систем с элементами централизации и децентрализации[Текст] / Журнал «Вопросы кибербезопасности» – 2020. - № 1 (35). – С. 2-7.
26. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. –М.: ГЛТ, 2016. – 280 с.
27. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.
28. Международный ISO/IEC стандарт 2700. Вторая редакция 2013-10-01. Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности – ТребованияISO/IEC 27001:2013 (E). Режим доступа: https://pqm-online.com.
29. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. –М.: Флинта, 2013. – 448 с.ъ
30. Нурдинов Р. А. Оценка рисков безопасности информационной системы на основе модели деструктивных состояний и переходов // Материалы конференции ИБРР-2015 / СПОИСУ. СПб., 2015. С. 372-373.
31. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т. Л. Партыка, И.И. Попов. –М.: Форум, 2018. – 88 с.
32. Петров, С.В. Информационная безопасность: Учебное пособие / С. В. Петров, И.П. Слинькова, В.В. Гафнер. –М.: АРТА, 2012. – 296 с.
33. Раевская О.Г., Кутовая Е.О. Финансовые последствия от возможной утечки конфиденциальной информации // Электронный научный журнал «APRIORI. Серия: Гуманитарные науки» WWW.APRIORI-JOURNAL.RU. 2016 № 1.
34. Семененко, В.А. Информационная безопасность / В.А. Семененко. –М.: МГИУ, 2011. – 277 с.

35. Симонов В.М., Огарок А.Л. Конструирование алгоритмов сложной обработки информации. Информационные технологии и методы. - Saarbrücken: LAP LAMBERT Academic Publishing, 2017. - 224 с. - ISBN: 978-620-205350-1.
36. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2017. – 304 с.
37. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил ме-неджмента информационной безопасности» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] - Режим доступа - http://docs.cntd.ru/document/1200103619 (дата обращения 26.05.2018).
38. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] - Режим доступа - http://docs.cntd.ru/document/1200058325 (дата обращения 25.05.2018).
39. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] - Режим доступа - http://docs.cntd.ru/document/1200105710 (дата обращения 25.05.2018).
40. Стандарт NIST SP800-30 «Руководство по управлению рисками для систем информационных технологий. Рекомендации Национального института Стандартов и технологий» // Режим доступа: http://library.egov.ifmo.ru/sites/default/files/Risk_management.pdf

41. Стандарт BS 7799-2:2005 «Практические правила управления информационной безопасностью» // Режим доступа: http://iso-management.com/wp-content/uploads/2013/12/ISO-27001.pdf
42. Стандарт РС БР ИББС-2.2-200 «Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации» //Режим доступа: http://docs.cntd.ru/document/902189338
43. СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования. Доступно на: https://online.zakon.kz/Document/?doc_id=30435994&doc_id2 (от 15 сентября.2018г.)
44. BS ISO\\IEC 27001:2005. BS 7799-2:2005. Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасность - Требования
45. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2018. - 352 с.
46. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. –М.: Гелиос АРВ, 2017. – 336 с.
47. Шаньгин, В.Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. –М.: ДМК, 2014. – 702 с.
48. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории: учебник для бакалавриата и магистратуры. М.: Издательство Юрайт, 2017. 309 с
49. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В. И. Ярочкин. – М.: Акад. Проект, 2018. – 544 с.
50. Сайт ООО «Транснефть-Восток». – [Электронный ресурс]Режим доступа: https://vostok.transneft.ru/.
51. Потери и утечки данных // Tadviser. Государство. Бизнес. ИТ [Электронный ресурс] / URL: http:/www.tadviser.ru/index.php/ (дата обращения 15.12.2018).

52. Центр кибербезопасности указал, где находятся основные источники кибератак [Электронный ресурс] - Режим доступа: https://tass.ru/politika/5897810.
53. Утечка информации: субъекты, каналы, последствия: [Электронный ресурс] URL: http://www.itbestsellers.ru/statistics/detail.php?ID=21397
54. Общие критерии оценки защищенности информационных технологий, Общие критерии // Википедия [Электронный ресурс] - Режим доступа - https://ru.wikipedia.org/wiki/Общие_критерии#Общие_критерии_в_России/ (дата обращения: 24.05.2018).
55. Стандарт ISO/IEC 15408 // Википедия [Электронный ресурс] - Режим доступа - http://www.lghost.ru/lib/security/kurs2/theme02_chapter04.htm/ (дата обращения: 26.05.2018).

ПРИЛОЖЕНИЕ А

Сравнительный анализ наиболее известных методик анализа рисков информационной безопасности

Критерии сравнения	RiskWatch (США)	CRAMM (Великобритания)	ГРИФиКОНДОР Digital Security Office (Россия)
1.Поддерживаемые стандарты	ISO 17799, TCSEC («Оранжевая книга») и другие	ISO 17799, ISO 15408 и другие	ISO 17799, ISO 27001 и другие
2. Способы оценки рисков	Количественный	Качественный и количественный	Качественный и количественный
3. Используемые технологии оценки рисков	Методика предсказания годовых потерь (Annual LossExpectancy – ALE)	Методика предсказания годовых потерь (Annual LossExpectancy – ALE)	Проводится оценка соотношения ущерба и риска в результате нарушения конфиденциальности, целостности и доступности информации
4. Наличие статистики по инцидентам в области ИБ	Имеется	Не имеется	Не имеется
5. Наличие базы данных по угрозам, уязвимостям, контрмерам в области ИБ	Обширная база по уязвимостям – опросник для выявления уязвимостей содержит более 600 вопросов	Имеется объемная база данных, содержащая 3000 контрмер	Имеется база данных по угрозам (собственная разработка классификации угроз) и уязвимостям (опросники)
6. Оценка надежности персонала	Отсутствует	Отсутствует	Отсутствует
7. Организационный уровень анализа рисков	Отсутствует	Имеется	Имеется
8. Программно-технический уровень анализа рисков	Имеется	Имеется	Имеется

Продолжение приложения А

Критерии сравнения	RiskWatch (США)	CRAMM (Великобритания)	ГРИФиКОНДОР DigitalSecurityOffice (Россия)
9.Оценка эффективности внедрения контрмер	Используется оценка возврата от инвестиций (Returnon Investment – ROI)	Используется более 10 способов оценки величины ущерба, в том числе оценка возврата от инвестиций (Returnon Investment – ROI)	Используется оценка возврата инвестиций на информационную безопасность (ROSI)
10. Содержание методики анализа рисков	1 этап: определяется предмет исследования (описываются параметры: тип организации, состав ИС, базовые требования в области ИБ). 2 этап: вводятся данные. Подробно описываются ресурсы, потери и классы инцидентов, которые выводятся путем сопоставления категории потерь и категории ресурсов. Задаются частота возникновения Угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.	1 этап: определяется достаточность применения средств базового уровня или необходимость проведения более детального анализа. Так выглядит одна из шкал оценки ресурсов: 2 балла – менее$1000; 6 баллов –от$1000 до $10 000; 8 баллов- от $10 000 до$100 000; 10 баллов- свыше $100 000. 2 этап: производится идентификация рисков и оценка их величины. При низкой оценке по всем используемым критериям (3 балла и ниже) считается, что система требует базового уровня защиты и вторая стадия исследования пропускается. 3 этап: решается вопрос о выборе адекватных контрмер	1 этап: определяется полный список информационных ресурсов, представляющих ценность, которые объединяются в сетевые группы. 2 этап: вводятся все виды ценной информации с привязкой к объектам ее хранения (сервера, рабочие станции и т.д.); указывается ущерб по каждой группе ценной информации, по всем видам угроз. 3 этап: определяются пользовательские группы, виды Доступа (локальный и/или удаленный)и права (чтение, запись, удаление) пользователей. 4 этап: указываются средства защиты, вводится информация о затратах на обеспечение ИБ.

Продолжение приложения А

11. Особенности отчетной документации	Варианты отчета: - краткие итоги; - отчет о стоимости защищаемых ресурсов и ожидаемых потерях от реализации угроз; - отчет об угрозах и контрмерах; - отчет о roi; отчет о результатах аудита ИБ	Варианты отчетов: - отчет по анализу рисков; - общий отчет по анализу рисков; - детализированный отчет по анализу рисков	Состав отчета: - инвентаризация ресурсов; - риски по видам информации; - риски по ресурсам; - соотношение ущерба и риска информации и ресурса; - выбранные контрмеры; - рекомендации экспертов
12.Системные требования	Операционная система - Windows 2000/XP Процессор - Intel Pentium или совместимый; Оперативная память - 256 MB; Свободное дисковое пространство – 30 MB для инсталляции	Операционная система: Windows XP Windows 2000 Windows NT Windows Me Windows 98 Процессор - 1000 Mhz ; Оперативная память - 128 MB; Свободное дисковое пространство - 50 MB	Операционная система: Windows 2000, Windows XP Оперативная память: 256 Mb (минимальная), 512 Mb (рекомендуется) Свободное дисковое пространство (для диска, где расположены данные пользователя): 300 Mb
13. Критерии сравнения	RiskWatch (США)	CRAMM (Великобритания)	ГРИФиКОНДОР Digital Security Office (Россия)
14. Наличие специальной подготовки и высокой квалификации аудитора в области ИБ	Требуется	Требуется	Не требуется
15. Цена	Стоимость лицензии от 10 000 долл. за одно рабочее место	Стоимость лицензии от 2 000 до 5 000 долл. за одно рабочее место	Стоимость лицензии от 1 000 долл. за одно рабочее место

Окончание приложения А

16. Возможность адаптации продукта под конкретные потребности организации (гибкость методики)	Имеются списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты, из них нужно выбрать те, что реально присутствуют в организации. Имеется возможность корректировки вопросов, исключение или добавление новых.	Сложность внесения дополнений в базу данных, однако имеется удобная система моделирования ИС с позиции безопасности: 400 типов ресурсов ИС, более 25 различных видов ущерба, 38 типов угроз безопасности, более 150 возможных комбинаций ущерба, угрозы и уязвимости, 7уровней риска.	Имеются списки категорий защищаемых ресурсов, угроз, уязвимостей имер защиты, из них нужно выбрать те, что реально присутствуют в организации. Имеется редактор баз требований, предоставляющий возможность самостоятельно создавать и работать с любыми другими стандартами и базами требований.

ПРИЛОЖЕНИЕ Б

Оценка информационных активов предприятия

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка (ед.изм.)	Количественная оценка (ед.изм.)
Сведения делового характера						
Внутренний регламент деятельности	Детальные планы финансовых вложений в развитие организации	в электронном виде	директор	стоимость его воссоздания	тыс.рублей	очень высокая
	Планы и методы продвижения услуг на рынок	в электронном виде	директор	репутация компании	тыс. .рублей	высокая
Информационный актив по торгово-экономическим вопросам						
Обработка заявок клиентов	Номенклатура и количество услуг по взаимным обязательствам	в электронном виде	менеджер	утрата доступности	тыс.рублей	средняя
Внутренний регламент деятельности	Сведения о расчетных и операциях по банковским счетам	в электронном виде	главный бухгалтер	утрата доступности	тыс.рублей	очень высокая
	Информация об эффективности сделок, договоров	в электронном виде	директор	утрата доступности	тыс.рублей	средняя
	ИНН, документы об уплате налогов и обязательных платежах	в электронном виде	главный бухгалтер	утрата доступности	тыс.рублей	высокая

Продолжение приложения Б

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка (ед.изм.)	Количественная оценка (ед.изм.)
Информационный актив о предоставляемых услугах						
Обработка заявок клиентов	Информация об обработанных и необработанных заказах	в электронном виде	менеджер	стоимость его воссоздания	тыс.рублей	средняя
Внутренний регламент деятельности	Проекты по автоматизации организации и бизнес-процессов, находящиеся в разработке	в электронном виде	директор	стоимость его воссоздания	тыс.рублей	высокая
Информационный актив по вопросам обеспечения безопасности						
Внутренний регламент деятельности	Сведения об организации и состоянии физической охраны зданий	в электронном виде	директор	стоимость его воссоздания	тыс.рублей	очень высокая
	Информация о защищаемых информационных ресурсах	в электронном виде	директор	утрата доступности	тыс.рублей	очень высокая
	Базы данных ООО «Транснефть-Восток»	в электронном виде	системный администратор	стоимость его воссоздания	тыс.рублей	очень высокая
	Информация о детальной структуре корпоративной сети	в электронном виде	системный администратор	утрата доступности	тыс.рублей	очень высокая
Информационный актив по организационно-управленческой деятельности						
Внутренний регламент деятельности	Условия индивидуальных трудовых договоров с работниками и руководителями	в электронном виде	главный бухгалтер	репутация компании	тыс.рублей	средняя

Окончание приложения Б

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка (ед.изм.)	Количественная оценка (ед.изм.)
Продукция организации						
Получение прибыли	Услуги и товары	материальный объект	директор	первоначальная стоимость актива	тыс. рублей	высокая
Оборудование						
Обеспечение необходимых условий работы	Компьютеры, принтеры, телефоны, кабели и т.п.	материальный объект	директор	первоначальная стоимость актива	тыс. рублей	средняя

ПРИЛОЖЕНИЕ В

Результаты оценки уязвимости активов

Группы уязвимости Содержание уязвимостей	Актив № 1	Актив № 2	Актив №3	Актив № 4	Актив № 5	Актив № 6	Актив №7
1. Среда и инфраструктуры							
Неправильное использование физических средств доступа в здание	низкий	низкий	низкий	низкий	низкий	низкий	низкий
Нестабильность в работе электросети	низкий	низкий	низкий	низкий	средний	низкий	низкий
2. Аппаратное обеспечение							
Отсутствие графика периодических замен						средний	
Отсутствие контроля за изменением конфигураций						низкий	
3. Программное обеспечение							
Отсутствие механизма идентификации и аутентификации	низкий	низкий	низкий	низкий			низкий
Отсутствие аудиторских проверок	низкий	низкий	низкий	низкий	низкий	низкий	низкий
Отсутствие контроля загрузки и использования программного обеспечения	низкий	низкий	низкий	низкий		низкий	низкий

Окончание приложения В

Группы уязвимости Содержание уязвимостей	Актив № 1	Актив № 2	Актив №3	Актив № 4	Актив № 5	Актив № 6	Актив №7
4. Коммуникация							
Незащищенные линии связи	высокий	высокий	высокий	высокий		высокий	высокий
Отсутствие аутентификации и идентификации получателей и отправителей	высокий	высокий	высокий	высокий		высокий	высокий
Отсутствие подтверждения посылок и получения сообщений	высокий	средний	средний	средний		средний	средний
5. Документ (документооборот)							
Хранение в незащищенном месте	низкий	низкий	низкий	низкий	низкий		низкий
Бесконтрольное копирование	низкий	низкий	низкий	низкий	низкий		низкий
6.Персонал							
Недостаточная подготовка персонала	низкий	низкий	низкий	низкий	низкий	низкий	низкий
Отсутствие механизма отслеживания	низкий	низкий	низкий	низкий	низкий	низкий	низкий
7. Общие уязвимые места							
Отказы системы вследствие отказа одного из элементов						низкий	
Неадекватный итог осуществления технического обслуживания					низкий	низкий	

ПРИЛОЖЕНИЕ Г

Оценка рисков ООО «Транснефть-Восток» по методике оценки рисков информационной безопасности

Актив	Вероятность появления угроз, Ругр	Риск несоответствия установленным требованиям законодательства,Rn	Ценность информации,C	Вероятность использования уязвимостей Ko	Вероятность использования технических уязвимостей Kt	уровень риска возникновения угроз информационной безопасности,R
Детальные планы финансовых вложений в развитие организации	0,35	0,1	0,9	0,2	0,4	0,9
Планы и методы продвижения услуг на рынок	0,45	0,1	0,8	0,3	0,4	1,3
Сведения о расчетных и операциях по банковским счетам	0,10	0,1	0,9	0,2	0,2	0,2
Информация об эффективности сделок, договоров	0,50	0,1	0,5	0,2	0,2	0,5
ИНН, документы об уплате налогов и обязательных платежах	0,25	0,2	0,7	0,3	0,3	1,1
Проекты по автоматизации организации и бизнес-процессов, находящиеся в разработке	0,25	0,2	0,7	0,2	0,2	0,7

Окончание приложения Г

Сведения об организации и состоянии физической охраны зданий	0,30	0,2	0,8	0,1	0,1	0,5
Информация о защищаемых информационных ресурсах	0,20	0,1	0,9	0,1	0,1	0,2
Базы данных ООО «Транснефть-Восток»	0,15	0,1	0,9	0,1	0,1	0,1
Информация о детальной структуре корпоративной сети	0,15	0,2	0,9	0,1	0,1	0,3
Условия индивидуальных трудовых договоров с работниками и руководителями	0,45	0,2	0,5	0,3	0,4	1,6
Услуги и товары	0,30	0,1	0,7	0,2	0,2	0,4

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, управления и природопользования
кафедра финансов

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И.С. Ферова
подпись
«_17_» __06___ 2020 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (НА ПРИМЕРЕ ООО «ТРАНСНЕФТЬ-ВОСТОК»)

Научный руководитель _____ канд. экон. наук, доцент Е.А. Шнюкова
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ К.О.Ничипуренко
подпись, дата инициалы, фамилия

Рецензент _____ нач. отдела сырья и соб-го МТОАО «РУСАЛ Менеджмент»
подпись, дата должность М.С. Толмачёв
инициалы, фамилия

Красноярск 2020