Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, государственного управления и финансов

Кафедра финансов и управления рисками

УТВЕРЖДАЮ
Заведующий кафедрой

_____ И.С. Ферова
подпись инициалы, фамилия
«_____»_____ 2022 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (НА ПРИМЕРЕ ПАО «ГАЗПРОМ»)

Руководитель	_____	к.э.н., доцент	И.Г. Кузьмина
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		Ю.С. Киевский
	подпись, дата		инициалы, фамилия
Рецензент	_____	Руководитель департамента информационных технологий СФУ	К.Н. Захарьин
	подпись, дата	должность, ученая степень	инициалы, фамилия
Нормоконтролер	_____		Е.В. Шкарпетина
	подпись, дата		инициалы, фамилия

Красноярск 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Топливно-энергетический комплекс является основой современной экономики. Предприятия нефтегазодобывающей и нефтеперерабатывающей отраслей характеризуются высокой степенью монополизации со стороны государства. Для РФ нефтегазовая отрасль имеет особое значение, поскольку формирует существенную долю федерального бюджета. По данным Минфина за последние несколько лет доля доходов от нефтегазового сектора составляет от 35 до 55%, что обуславливает актуальность исследуемой в настоящей работе темы. Поскольку в современном мире невозможно представить работу крупнейших топливно-энергетических предприятий без цифровизации бизнес-процессов, необходимо понимать насколько эффективно функционирует информационная составляющая экономической безопасности крупнейшей отечественной нефтедобывающей компании.

Цель исследования – сформулировать рекомендации, направленные на совершенствование информационной безопасности транснациональной энергетической компании ПАО «Газпром».

Задачи дипломной работы:

1) изучить теоретические аспекты оценки информационной безопасности предприятия;

2) рассмотреть существующие методики оценки информационной безопасности предприятия;

3) проанализировать современное состояние экономики топливно-энергетического комплекса РФ;

4) произвести апробацию существующих методик оценки информационной безопасности предприятия, выбрав в качестве объекта ПАО «Газпром»;

5) выявить основные недостатки в сложившейся системе обеспечения информационной безопасности ПАО «Газпром»;

6) рассмотреть направления совершенствования эффективности системы информационной безопасности ПАО «Газпром».

Объектом научно-исследовательской работы является система информационной безопасности ПАО «Газпром».

Предмет исследования – подходы к оценке и повышению эффективности информационной безопасности предприятия.

В процессе написания данной работы применялись общенаучные (анализ, синтез, сравнение, описание) и экономические методы познания.

Практической базой исследования послужили финансовая отчетность, локальные акты предприятия и рабочий опыт автора, полученный в результате прохождения производственной практики.

В первой главе настоящей работы рассматриваются теоретические аспекты экономической и информационной безопасности предприятия.

Во второй главе научной работы определяются основные показатели, характеризующие информационную безопасность предприятия. Рассматриваются методики определения уровня экономической и информационной безопасности предприятий.

В третьей главе дипломной работы дается характеристика топливно-энергетического комплекса, в частности ПАО «Газпром». Проводится многоаспектная оценка информационной безопасности предприятия с помощью методик, описанных в международных стандартах обеспечения информационной безопасности предприятий. Выявлены слабые места данной системы и описаны направления минимизации существующих рисков.

Работа состоит из введения, трех глав, заключения, списка использованных источников и приложения; включает 7 иллюстраций, 4 таблицы, 3 вложения и 4 формулы.

1 Теоретические аспекты информационной и экономической безопасности предприятия

1.1 Экономическая безопасность предприятия: понятие, сущность и структурные элементы

В настоящее время в мире наблюдается зависимость и уязвимость экономики перед глобальными катаклизмами. По этой причине государства вынуждены решать вопросы, касающиеся минимизации отрицательных последствий, вызванных негативными событиями. Понятие «национальная безопасность» напрямую связанно с «экономической безопасностью», что обуславливает ее актуальность.

В.Ш. Уразгалиев определяет безопасность как «состояние субъекта, при котором вероятность изменения присущих этому субъекту качеств и параметров внешней среды невелика, меньше определенного интервала» [31].

В отечественном законодательстве в ст.1 №390-ФЗ от 28.12.2010 г. дано определение «безопасности» как «состояния защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» [5]. К основным объектам относят личность, общество и государство.

Существует множество подходов к определению экономической безопасности. Зарубежные экономисты при рассмотрении данного понятия делают акцент на социально-экономической направленности. В официальных документах США и ряда европейских стран термин «экономическая безопасность» редко употребляется. Однако с точки зрения безопасности нередко рассматриваются те или иные экономические вопросы. Впервые данное понятие было использовано Рузвельтом во время экономического кризиса в США.

Положения экономической безопасности были закреплены во Франции в 1964 г. в законе «О национальной безопасности» [30]. Управленческие решения опираются на два основных критерия:

1) недопущение в ведущих секторах экономики внешней зависимости;

2) минимизация асимметрии экономического развития субъектов народного хозяйства.

Рассмотрим определения, данные отечественными исследователями.

А.И. Илларионов рассматривает экономическую безопасность как «сочетание экономических, политических и правовых условий, обеспечивающих в долгосрочной перспективе производство максимального количества экономических ресурсов на душу населения наиболее эффективным способом» [21].

По мнению Л.И. Абалкина экономическая безопасность являет собой «состояние экономической системы, позволяющее ей развиваться динамично, эффективно и решать социальные задачи и при котором государство имеет возможность выравнивать и проводить в жизнь независимою экономическую политику» [8].

По мнению Ю.С. Курочкина экономическая безопасность – способность экономики удовлетворять внутренний спрос и компенсировать предложение извне собственными ресурсами [32].

В.А. Савин определяет экономическую безопасность как «систему защиты жизненных интересов России». В качестве основных объектов защиты автор выделил [27]:

1) народное хозяйство;

2) отдельные регионы государства;

3) отдельные сферы и отрасли хозяйства;

4) субъекты хозяйственной деятельности.

Таким образом, мы можем вывести ниже следующее определение.

Экономическая безопасность — это экономическая система, находящаяся в состоянии защищенности, способная к саморегулированию внутренней среды и адаптации к внешнему воздействию изменяющихся условий. Данное определение достаточно «широкое», поэтому обратимся к классическим определениям экономической безопасности предприятия.

Принято выделять два основных подхода, определяющих данное понятие. Первый заключается в определении через подавление всех потенциальных и реальных угроз. Второй же допускает наличие угроз, однако подразумевает способность предприятия к снижению негативного воздействия.

В.К. Сенчагов подразумевает под экономической безопасностью предприятия защищенность его «потенциала» от активных и пассивных угроз. Под потенциалом подразумевается четыре составляющих предприятия, наиболее подверженных риску, – технологическая, производственная, научно-техническая и кадровая.

В качестве примера угроз автором приведена неблагоприятная внешняя среда, являющаяся последствием подрыва экономической безопасности государства [28]. Таким образом, автор тесно переплетает экономическую безопасность предприятия и государства.

Необходимость обеспечения экономической безопасности обусловлено ее способностью предотвратить либо ослабить воздействие текущих и потенциальных угроз. Своевременно принятые меры по ее обеспечению способны в значительной мере сократить расходы, возникающие в результате уменьшения ущерба от воздействия неблагоприятных факторов.

Помимо руководства предприятия в обеспечении экономической безопасности заинтересовано и государство, так как состояние защищенности национальной экономики достигается путем укрепления ее основных звеньев.

Для определения значения экономической безопасности для предприятия необходимо рассмотреть ее цели, задачи, основные объекты и субъекты. Так, под объектами понимается [17]:

1) территория отдельно взятого предприятия;

2) все объекты, расположенные на территории предприятия:

- здания и сооружения;

- товарно-материальные ценности;

- носители информации, составляющей коммерческую тайну;

3) особые объекты (необходимо применение дополнительных мер безопасности):

- сотрудники, имеющие доступ к конфиденциальной информации;

- руководство предприятия.

Субъекты безопасности предприятия делятся на две большие группы: внутренняя и внешняя. К первой относятся все сотрудники, осуществляющие деятельность внутри предприятия:

1) специализированные субъекты: служба экономической безопасности, спасательная служба, комитет безопасности, пожарная часть;

2) полуспециализированные субъекты: юридический отдел, медицинская часть;

3) остальной персонал.

К внешней группе относятся учреждения, деятельность которых не может контролироваться предприятиям. Цель данных органов сводится к формированию, реализации и защиты хозяйственной деятельности [10]:

1) правоохранительные органы;

2) органы исполнительной власти;

3) законодательные органы;

4) суды;

5) научно-образовательные учреждения.

Основная цель экономической безопасности предприятия состоит в обеспечении функционирования организации, предупреждении, своевременном обнаружении, предотвращении внутренних и внешних угроз, ликвидации их последствий [9]. Иными словами, главная цель сводится к ликвидации угроз, затрудняющих достижение основных целей бизнеса.

Выделим основные задачи экономической безопасности предприятия [14]:

- изучение причин появления угроз, влекущих снижение уровня безопасности предприятия;

- определение вероятности наступления основных угроз экономической безопасности;

- прогнозирование вреда;

- создание организационной структуры, призванной предупредить наступление неблагоприятных факторов;

- разработка комплекса мероприятий по минимизации последствий наступления угроз;

- совершенствование механизма экономической безопасности;

- повышение имиджа предприятия.

Рассмотрим структуру экономической безопасности с точки зрения Е.И. Кузнецовой, представленную на рисунке 1.

Рисунок 1 – Уровни организационной структуры экономической безопасности [24]

Данная структура показывает прямое влияние основания схемы (безопасность личности и предприятия) на национальную безопасность. Наличие «слабостей» в обеспечении защищенности от угроз в каждом предыдущем уровне сказывается на последующих [24].

Таким образом, обеспечение экономической безопасности государства требует создания благоприятной среды для поддержания состояния защищенности личности и предприятий.

На безопасность предприятия прямое воздействие оказывают такие понятия как «уязвимость», «устойчивость», «развитие» и «управляемость». Поэтому мы можем определить ее как состояние защищенности интересов предприятия в условиях постоянно изменяющейся внутренней и внешней среды [35].

Экономическую безопасность можно также представить в виде состояния защищенности от различных угроз. Виды угроз представлены на рисунке 2.

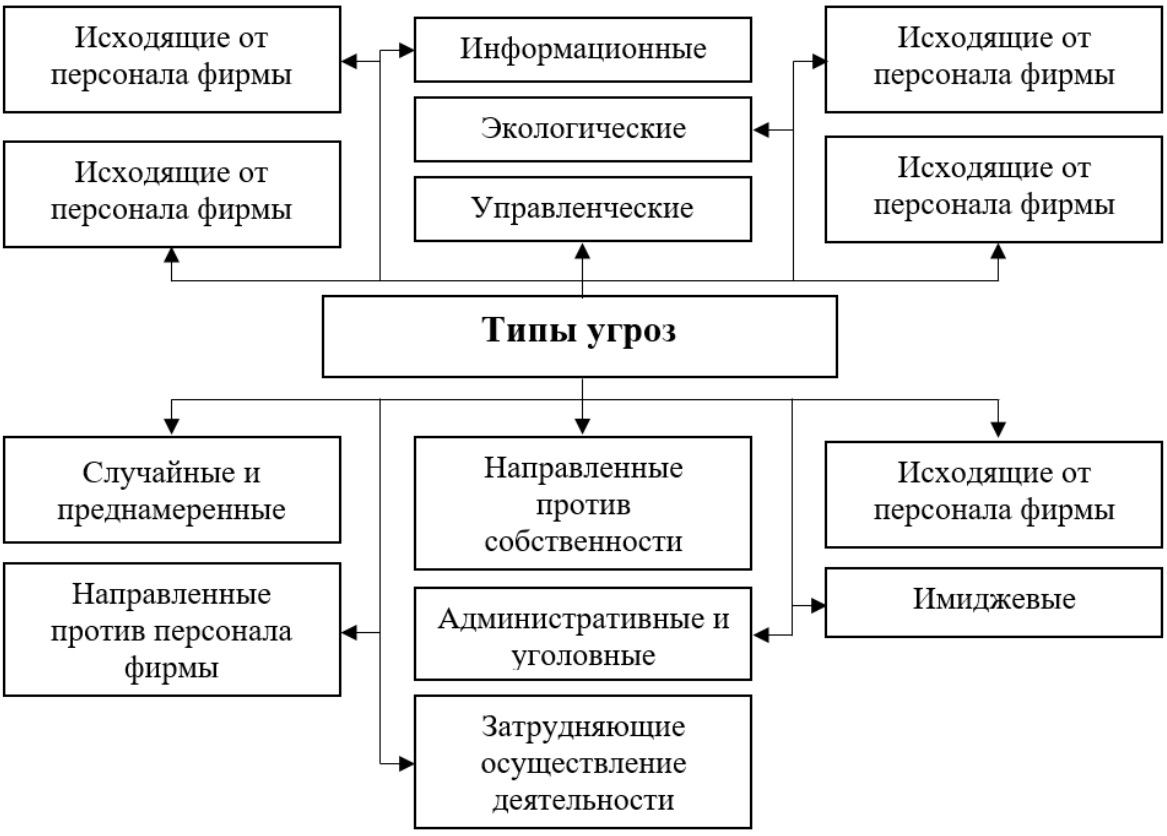

Рисунок 2 – Типы угроз [4, 19, 20]

Под угрозой следует понимать совокупность условий и факторов дестабилизации, создающих опасность интересам предприятия [23]. Их

изучение является важным элементом поддержания экономической безопасности на должном уровне. Самым популярным способом классификации является выделение внутренних (реальный сектор экономики и внутренняя среда компании) и внешних угроз (внешнеполитические и внешнеэкономические). Помимо этого, существует множество способов классификации [47]. Перечислим некоторые из них:

1) по сфере возникновения;

2) по характеру – объективные и субъективные;

3) по цели, например, материальные и финансовые;

4) по возможности и сложности прогнозирования;

5) по вероятности наступления;

6) по возможности измерения;

7) по возможности устранения;

8) по масштабу воздействия.

Таким образом, экономическая безопасность предприятия является комплексным понятием включающее совокупность факторов, связанных как с внутренним состоянием предприятия, так и с внешними факторами.

1.2 Информационная безопасность и ее влияние на экономическую безопасность предприятия

Экономическая безопасность предприятия состоит из нескольких частей. Повышение устойчивости одного из элементов влечет за собой укрепление системы в целом. Следовательно, для обеспечения экономической безопасности предприятия необходимо рассмотреть ее основные составляющие, которые представлены на рисунке 3.

Рисунок 3 – Составляющая экономической безопасности предприятия [25]

Силовая (физическая) составляющая включает в себя техническую составляющую физической защиты объекта. В нее входят – КПП, система видеонаблюдения, инструкций, разработанных для сотрудников, служба охраны. Основные критерии оценки физической безопасности – высокая компетенция персонала, точность разработанной инструкции и исправность оборудования охранной системы.

Экологическая составляющая – защищенность природной среды от потенциального негативного воздействия предприятия. Оценка данного элемента осуществляется путем анализа вероятности наступления чрезвычайных ситуаций в результате деятельности предприятия, а также прогнозирования возможного ущерба окружающей среде. Также оценивается ущерб от повседневной деятельности.

Финансовая безопасность отвечает за разумность использования ресурсов предприятия. Является одним из важнейших элементов экономической безопасности, так как данный элемент обеспечивает независимость организации. Под ней подразумевается бюджет и распределение между структурными подразделениями.

Политико-правовая безопасность – обеспечение стабильности работы организации путем своевременного изучения правовых норм, а также своевременное их внедрение в делопроизводство. Критерием эффективной

работы данного элемента служит оценка частоты правонарушений со стороны компании и их сотрудников в процессе работы [26].

Кадровая безопасность – это процесс минимизации рисков и угроз системе безопасности со стороны персонала. К такому риску относится:

- ненадлежащие выполнение служебных обязанностей;

- отсутствие мотивации у сотрудников;

- низкая квалификация кадров, влекущая за собой соответствующие риски;

- конфликты на рабочем месте, замедляющие рабочий процесс.

Интеллектуальная составляющая экономической безопасности представляет собой систему по предотвращению всех видов шпионажа, обеспечение патентов, привлечение квалифицированных кадров. И данный элемент также входит процесс анализа рынка, изучение деятельности партнеров и конкурентов.

Технологическая составляющая – подразумевает за собой контроль за техническим обеспечением на всех этапах деятельности предприятия.

Информационная безопасность – защита любой информации, не являющейся общедоступной; включает в себя защиту материальных носителей. Под защитой информации следует понимать практику предотвращения несанкционированного доступа, раскрытия, использования, изменения, искажения, исследования, копирования или уничтожения. Данный блок имеет наибольшее влияние на вышерассмотренные составляющие экономической безопасности, так как в каждом из них присутствует информация, составляющая коммерческую тайну [33].

На данный момент информационная безопасность наиболее тесно переплетается с интеллектуальной, кадровой и технической составляющими безопасности. Таким образом, данная система является многоступенчатой структурой и является приоритетной в отделе экономической безопасности предприятия.

Далее рассмотрим схему обеспечения информационной безопасности предприятия, представленную на рисунке 4.

Рисунок 4 – Система обеспечения информационной безопасности хозяйствующего субъекта [37, 16]

Все подсистемы связаны информационной защищенностью, поскольку с помощью информационной системы достигается связь между отдельными объектами, что еще раз подтверждает значение информационной безопасности современных хозяйствующих субъектов.

Рассмотрим основные риски и угрозы информационной безопасности предприятия, изображенные на рисунке 5.

Рисунок 5 – Классификация источников угроз информационной безопасности [18]

Риск – это событие, при реализации которого возникает положительное, либо негативное влияние на цель. Риск имеющий положительное влияние называется возможностью, отрицательное – угрозой.

Помимо классического разделения рисков и на внутренние и внешние, их подразделяют на три этапа [12]:

1) утечка информации, составляющей коммерческую тайну. Главная опасность в возможности использования информации конкурентами в целях нанесения ущерба или полного вытеснения организации с рынка;

2) риск технического сбоя – влечет за собой безвозвратное уничтожение информации, трудности в ее передачи, увеличение сроков ее обработки;

3) риск в результате форс-мажорных обстоятельств – невозможно прогнозировать.

В узком смысле можно опрежелить риск, как вероятность возникновения упущенной выгоды или убытка. Вероятность риска – вероятность наступления определенного события.

Уязвимость определяется, как слабость в системе защиты. Рост числа уязвимостей влечет за собой повышение вероятности реализации угроз. При разработке модели оценки риска информационной безопасности предприятия неободимо учитывать [13]:

- наличие обязательств предприятия закрепленных в действующих договорах и НПА;
- ценность информации;
- возможные риски при безвозвратной утере информации;
- последствия опубликования конфедециальной информации.

Оценка рисков является одним из основополагающих инструментов создания защиты. Необходимость ее проведения обусловлена последующим принятием мер поддержки системы информационной и экономической безопасности. Один из инструментов оценки – формулы и авторские методики, однако главной трудностью является труднодоступность данных и их достоверность.

2 Методические подходы к оценке информационных рисков предприятия

2.1 Определение показателей, характеризующих информационную безопасность

Для успешного существования предприятия в эпоху постиндустриального этапа экономики жизненно важно поддерживать систему информационной безопасности предприятия. К задачам данной системы относится:

1) обеспечение хранения информации предприятия;

2) обеспечение доступа к информации;

3) ограничение к доступной информации;

4) обеспечение сохранности информации при работе с ней;

5) минимизации риска краж данных.

Одна из главных проблем в обеспечении системы информационной безопасности – определение состояния данной системы на текущий момент, определение отдельных показателей и их пороговых значений, оценивающих информационную безопасность [2].

В классическом определении риск информационной безопасности состоит из трех основных элементов:

1) вероятность существования внешних и внутренних угроз;

2) степень потенциального воздействия на систему;

3) вероятность существования уязвимости в системе безопасности.

Для обеспечения безопасности предприятия достаточно полного исключения одной из переменных. Например, при отсутствии угроз не имеет значение наличие уязвимостей, при отсутствии уязвимостей – угрозы не способны воздействовать на систему. Согласно ISO/IEC 27001 метод обеспечения информационной безопасности должен иметь результаты,

поддающиеся анализу и сравнению [37]. Рассмотрим ряд формул для оценки рисков, предложенных различными руководствами.

«Risk management guide for information technology systems» приводит следующую формулу оценки риска (формула (1)) [50]:

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

где R – вероятность наступления риска;

P(t) – вероятность реализации угрозы (качественная шкала с тремя уровнями оценки);

S – воздействие угрозы на актив предприятия.

Конечное R представляет собой число, которое возможно ранжировать и оценить посредством бальной интерпретации.

Следующую формулу содержит ГОСТ Р ИСО/МЭК ТО 13335-3-2007 (формула (2)) [22]. В отличие от вышеприведенного способа оценки, в данном стандарте не оценивается воздействие угрозы на актив предприятия:

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

где R – вероятность наступления риска;

P(t) – вероятность реализации угрозы (качественная шкала с тремя уровнями оценки);

P(v) – вероятность наличия уязвимости (качественная шкала с тремя уровнями оценки);

C – ценность актива (оценка происходит путем присвоения бальных значений от 0 до 4).

Сопоставление качественных оценок для показателя, характеризующего ценность актива, производится предприятием и носит субъективный характер из-за отсутствия строго определенных критериев.

Далее рассмотрим формулу, описанную в спецификации BS 7799-2:2005 (формула (3)) [51]:

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

где R – вероятность наступления риска;

C – ценность актива (оценка происходит путем присвоения бальных значений от 0 до 4);

L(t) – уровень угрозы;

L(v) – уровень уязвимости.

Для показателя R существует стандарт, по которому происходит интерпретация вероятности наступления риска.

Таблица 1 – Балльная интерпретация вероятности наступления риска в BS 7799-2:2005

Значение	**Интерпретация**
0-2	Низкий риск – допустимо пренебрегать вероятностью наступления.
3-5	Средний риск – существенная угроза, требующая принятия мер по минимизации негативного воздействия
6-8	Высокий риск – необходимо устранять в первую очередь, так как затрагивает наиболее ценные активы при наибольшей вероятности наступления.

Следующая формула оценки риска информационной безопасности предложена стандартом РС БР СББС-2.2-200 (формула (4)):

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

где R – вероятность наступления риска;

P(v) – вероятность наличия уязвимости;

C – ценность актива.

Оценка вероятности реализации угрозы осуществляется по следующей шкале [7]:

Таблица 2 – Интерпретация вероятности риска информационной безопасности предложена стандартом РС БР СББС-2.2-200

Значение (%)	Интерпретация
0	Полное отсутствие угрозы. Возможно в случае применения идеальной системе защиты (отсутствии информации на электронном и бумажном носителе), либо при отсутствии какой-либо ценности в рассматриваемом активе.
До 21	Низкий риск – как правило, относится к допустимому пределу.
До 50	Значительный риск – возникает необходимость укрепления системы информационной безопасности
Более 50	Высокий риск – необходимо устранять в первую очередь, так как затрагивает наиболее ценные активы при наибольшей вероятности наступления.

После рассмотрения всех вышеперечисленных показателей оценки информационной безопасности необходимо отметить, что значительным недостатком является оценка коэффициентов в виде условных значений. Они не имеют единиц измерения, применяемых в деятельности организации, что не дает полного представления об уровне риска. Таким образом, мы можем использовать данные показатели исключительно в качестве вспомогательных средств.

2.2 Методика определения уровня экономической безопасности и информационной безопасности предприятия

Отличительной особенностью информационной безопасности является ее нелинейность. Непрекращающееся развитие технологий и повсеместная цифровизация не позволяют разработать универсальную методику оценки и внедрения системы безопасности. Изменение стандартов обеспечения

безопасности должно учитывать изменения, происходящие в отрасли, местное законодательства и индивидуальные потребности исследуемого предприятия.

Главная проблема обеспечения информационной безопасности крупных организаций – необходимость в непрерывном совершенствовании. Данная задача осложняется проблемами реализации – обеспечить изменение всей системы одновременно зачастую невозможно. Поэтому приходится «дробить» изменения. Последствием этого решения является необходимость адаптировать персонал к новым изменениям.

Помимо перечисленных проблем необходимо учитывать интересы злоумышленников и реалии конкурентной среды. Именно по этой причине невозможно создать методику, учитывающую основные проблемы. Тем не менее, мы должны учитывать существующие концепции оценки информационной безопасности, описанные в международном стандарте по информационной безопасности.

BS 7799 разработан Британским институтом стандартов (BSI) при участии крупнейших коммерческих организаций. В 1995 году данный стандарт в Великобритании получил статус государственного [2].

Документ описывает более сотни механизмов контроля, призванных выстроить систему информационной безопасности. В мировой практике признается универсальность методов, так как они применимы к организациям независимо от их размера, территориального расположения и рода деятельности.

Необходимо отметить, что не существует сертификаций по данному стандарту, так как он является сборником существующих практик. Его можно рассматривать в качестве руководства по созданию и отладке системы обеспечения информационной безопасности на предприятии.

Данный стандарт определяет основные требования по реализации, мониторингу, проведения ревизии и поддержанию информационной безопасности предприятия. Документ подразумевает выстраивание системы

безопасности с непрерывным совершенствованием отдельно взятых элементов.

Стандарт содержит два основных блока. Первый раздел называется «Управление информационной безопасностью». Он рассчитан на руководителей и сотрудников, ответственных за создание, планирование и реализацию системы информационной безопасности.

Основные положения первого раздела гласят, что целью информационной безопасности является бесперебойная работа предприятия с минимизацией потенциального ущерба в результате наступления неблагоприятных событий.

Стандарт выделяет 10 регуляторов, которые необходимо рассмотреть в рамках исследования информационной безопасности. Стоит отметить, что все нижеперечисленные регуляторы относятся к структурным элементам информационной безопасности:

1) документация, описывающая политику информационной безопасности;

2) обучение персонала основным навыкам работы в рамках системы информационной безопасности, а также отдельных кадров обеспечивающих данную систему;

3) распределение обязанностей в раках поддержания информационной безопасности;

4) антивирусные средства;

5) уведомления о нарушения защиты;

6) план бесперебойной работы предприятия (в том числе при наступлении критических инцидентов);

7) система защиты документации;

8) система защиты данных (резервирование, безопасная передача);

9) контроль над соответствия политике информационной безопасности, описанной в соответствующих документах;

10) контроль копирования программного обеспечения, защищенного авторским правом.

Вторая часть стандарта носит название «Системы управления информационной безопасности» (СУИБ). Ключевой элемент данной системы – система управления рисками, в задачи которой входит исследование актуальных угроз и определение активов, требующих защиты. Необходимость анализа риска обусловлена возможностью снижения ущерба в результате наступления неблагоприятного исхода [1]. В процессе создания СУИБ, необходимо:

- определение приоритетных информационных ресурсов и их ранжирование по степени важности;
- выявление основных уязвимостей;
- определение механизмов управления информационными ресурсами;
- бесперебойный анализ СУИБ с целью поиска путей ее совершенствования.

Уровень риска устанавливается посредством определения уровня угрозы, ценности актива и степени его уязвимости. Ценностью ресурса является величиной ущерба в случае наращения его доступности или конфиденциальности.

В основу процесса управления лежит система PDCA (Plan-Do-Check-Act), включающая четыре фазы:

- планирование;
- реализация;
- оценка;
- корректировка.

Рассмотрим каждую стадию отдельно (представлена на рисунке 6):

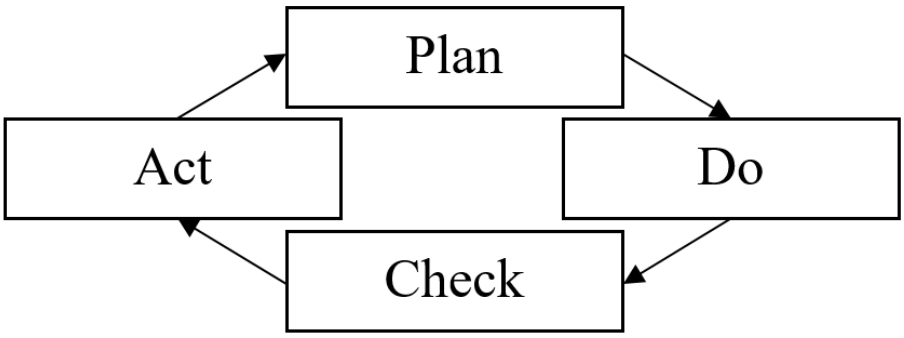

Рисунок 6 – Методика PDCA

Первый элемент – Plan (планирование).

Основная цель – оценка соответствия бизнес-процесса стратегическим целям организации. Этап считается завершенным после получения следующей информации:

- определение потребителя;

- обоснование, почему бизнес процесс компании представляет ценность потребителям произведенного продукта;

- исходные показатели результативности;

- целевые показатели результативности.

Также на данном этапе необходимо провести оценку показателей экономической безопасности. В качестве способа оценки нами предлагается использовать спектр-балльный метод А. Н. Салова и В. Г. Маслова.

Суть данного метода состоит в сравнении полученных коэффициентов с нормативными значениями и сопоставлении этого значения с определенными зонами: зона риска – 0 баллов; зона опасности – 1 балл; зона стабильности – 3 балла; зона благополучия – 5 баллов.

После чего по каждой группе коэффициентов находится средний балл и формируется оценка предприятия (приложение А). После расчета основных показателей следует провести балльную оценку [45]. Так, зона риска не оценивается, зоне опасности присваивается 1 балл, зона стабильности оценивается в 3 балла, зона благополучия получает максимальную оценку в 5

баллов. После оценивания каждой группы коэффициентов следует определение среднего балла по группам.

После проведения расчетов согласно представленным выше методикам следует обратить внимание на показатели, выходящие за пределы нормативных значений, с целью предложения мероприятий по укреплению уровня экономической безопасности.

Следующим этапом является проектирование внутреннего устройства процесса. Результатом служит описание следующих пунктов:

- действия, составляющие процесс;

- описание результата принятых действий;

Do (действие). На данной стадии происходит внедрение модификаций, разработанных на предыдущем этапе. В рамках научной работы невозможна реализация описанного этапа, однако в теории на данном шаге должно содержаться описание вероятных событий, способных затруднить процесс совершенствования информационной безопасности.

Check (проверка). Целью данного этапа является сравнение показателей эффективности с ожидаемыми значениями.

Act (корректировка). Осуществляется на основании предыдущего этапа. Корректировка обеспечивает беспрерывность процесса, несмотря на изменение внешних условий.

К наиболее слабым местам данного метода оценки можно отнести следующее:

- отсутствие определенного порядка оценки;

- субъективность в определении уровня ценности информации для компании;

- отсутствие числовой интерпретации экспертного заключения.

По этой причине необходимо составить сводную таблицу (Приложение Б), дающую визуальную интерпретацию общей картины информационной безопасности.

Присвоение баллов осуществляется посредством экспертной оценки. К зоне риска относятся показатели, способные подорвать общий уровень экономической безопасности компании. К зоне опасности относятся проблемы, требующие решения в ближайшее время. Стоит отметить, что проблемы зоны риска и опасности не способны навредить системе информационной безопасности без наличия дополнительных внутренних или внешних угроз.

3 Анализ информационной безопасности и рекомендации по снижению ее рисков для ПАО «Газпром»

3.1 Характеристика предприятия ПАО «Газпром»

Топливно-энергетический комплекс (далее ТЭК) является основой современной экономики. Предприятия нефтегазодобывающей и нефтеперерабатывающей отраслей характеризуются высокой степенью монополизации со стороны государства.

На данный момент подавляющее большинство нефтегазовых предприятий, около 90%, функционируют в качестве холдинговых компаний. Поясним, что вертикальная интеграция – это объединение на финансово-экономической основе различных технологически взаимосвязанных производств. Как правило, существует головная компания, разрабатывающая общие планы достижения финансовой цели, и дочерние компании, занимающиеся непосредственно исполнением [29].

Для РФ нефтегазовая отрасль имеет особое значение, поскольку формирует существенную долю федерального бюджета. По данным Минфина, за последние несколько лет доля доходов от нефтегазового сектора составляет от 35 до 55%.

Добываемые ресурсы способны в полной мере удовлетворить внутренний спрос на топливо, что обеспечивает энергетическую безопасность РФ.

По причине сильнейшей зависимости отечественной экономической системы от нефтегазового сектора, курс национальной валюты напрямую зависим от изменения мировых цен на нефть.

Налог на добычу полезных ископаемых, налог на имущество и проч. (за исключением налога на прибыль) составляют самый большой удельный вес в операционных расходах нефтегазовых компаний – от 22 до 60%. Таким образом, себестоимость добычи и реализации нефти и газа в большей степени

формируется за счёт налогов и иных обязательных платежей в пользу государства [38, 43, 44].

ТЭК формирует национальный бюджет и обеспечивает экономическую безопасность, а также обеспечивает занятость на рынке труда. Разработка новых месторождений требует создания соответствующий инфраструктуры в целях обеспечения безопасных условий труда.

Нефтегазовая отрасль включает свыше 2300 месторождений нефти. Из них:

- около 60% находится в западной Сибири;
- на Восточно-Уральскую базу приходится 22%;
- Северные месторождения составляют 5%;
- 1% находится на Кавказе.

Также на западную Сибирь приходится 90% от общей добычи газа на территории РФ.

Как было описано выше, разработка новых месторождений влечет за собой создание инфраструктуры. Так как свыше 65% месторождений находятся в труднодоступных районах, возникает необходимость обеспечения способа транспортировки ресурсов.

Помимо строительства дорог специального назначения появляется необходимость в развитии городов Восточной Сибири, а также в создании новых поселений на территории северных месторождений в целях обеспечения их рабочей силой.

Одной из крупнейших транснациональных энергетических компаний является ПАО «Газпром». Компания входит в четверку крупнейших производителей нефти в Российской Федерации. «Газпром» также владеет крупными генерирующими активами на территории России. Их суммарная установленная мощность составляет порядка 16% от общей установленной мощности российской энергосистемы. Кроме того, компания занимает первое место в России по производству тепловой энергии. Стоит отметить, что более 50% акций входит в государственную собственность.

Перечислим основные направления деятельности компании:

- проведение комплекса георазведывательных мероприятий;
- добыча нефти, газа и газового конденсата;
- транспортировка добытой продукции;
- хранение и переработка продукции;
- переработка полезных ископаемых;
- реализация нефти, газа и газового конденсата;
- реализация переработанной продукции (топливо).

Суммарная доля ПАО «Газпром» в отечественных запасах газа превышает 70%. До 2013 года организация являлась монополистом в области экспорта газа. На данный момент остается монополистом в области экспорта трубопроводного газа.

ПАО «Газпром» на протяжении нескольких лет остается мировым лидером в области добычи природного газа. На него приходится свыше 12% мировой и 68% российской добычи. По состоянию на начало 2022 года компания активно реализует проекты по освоению газовых ресурсов арктического шельфа, полуострова Ямал, Дальнего Востока, Восточной Сибири, а также ряд проектов в области разведки и добычи углеводородов за рубежом. Доля запаса природного газа ПАО «Газпром» в России составляет 71 %, за рубежом превышает 16%.

Общая протяженность системы транспортировки ПАО «Газпром» составляет 170 тысяч километров, что делает ее крупнейшей в мире.

Стратегическая цель ПАО «Газпрома» – укрепление статуса лидера среди глобальных энергетических компаний. Реализация цели достигается посредством:

- диверсификации рынков сбыта;
- использования научно-технического потенциала в области добычи и переработки полезных ископаемых;
- обеспечения энергетической безопасности;

- обеспечение устойчивого развития, а также роста эффективности деятельности.

Миссия ПАО «Газпром»: «надежное, эффективное и сбалансированное обеспечение потребителей природным газом, другими видами энергоресурсов и продуктами их переработки».

ПАО «Газпром» позиционируется как вертикально интегрированная компания, что предполагает объединение исходных компонентов производственного цикла, переработку, распределение и продажу продуктов переработки и другие мероприятия в рамках одной компании производства.

Данный тип организационной структуры управления означает деятельность во всем цикле продукта – от разведки и разработки нефтяных и газовых месторождений, транспортировки жидкой и газообразной продукции, комплексной переработки продукта до его реализации конечным потребителям. В «Газпроме» все это сопровождается научными исследованиями и инновационным процессом, поэтому можно с делать вывод, что данная структура соответствует технологии.

В 2020 г. среднесписочная численность работников Группы достигла 477,6 тыс. человек. При этом среднесписочная численность работников основных обществ Группы «Газпром» по добыче, транспортировке, подземному хранению и переработке газа составила 261,1 тыс. человек, ПАО «Газпромнефти» – 77,4 тыс. человек [41].

Структура персонала основных обществ Группы Газпром по добыче, транспортировке, подземному хранению и переработке газа в 2020 году выглядит следующим образом:

- руководители – 14,2 %;
- специалисты – 33,4 %;
- рабочие – 52,4 %;
- прочие служащие – 5,4 %.

Структура корпоративного управления ПАО «Газпром» является линейной, представлена на рисунке 7.

Рисунок 7 – Структура корпоративного управления ПАО «Газпром»

Высшим органом управления ПАО «Газпром» является Общее собрание акционеров, которое проводится ежегодно. Проводимые помимо годового Общие собрания акционеров являются внеочередными.

Правом голоса на Общем собрании акционеров обладают акционеры — владельцы обыкновенных или привилегированных акций. Любой акционер лично или через своего представителя имеет право на участие в Общем собрании акционеров. Собрание является правомочным, если в нем приняли участие акционеры, обладающие в совокупности более чем половиной голосов.

В компетенцию Общего собрания акционеров, в частности, входит внесение изменений в Устав Общества, утверждение годовых отчетов и

аудитора Общества, распределение прибыли, избрание членов Совета директоров и Ревизионной комиссии, принятие решений о реорганизации или ликвидации Общества, а также об увеличении или уменьшении его уставного капитала.

Совет директоров осуществляет общее руководство деятельностью Общества, за исключением решения вопросов, отнесенных к компетенции Общего собрания акционеров. Члены Совета директоров Общества избираются Общим собранием акционеров на срок до следующего годового Общего собрания акционеров. Совет директоров, в частности, определяет приоритетные направления деятельности Общества, утверждает годовой бюджет и инвестиционные программы, принимает решения о созыве Общих собраний акционеров, об образовании исполнительных органов Общества, дает рекомендации по размеру дивиденда по акциям.

Председатель Правления (единоличный исполнительный орган) и Правление (коллегиальный исполнительный орган) осуществляют руководство текущей деятельностью Общества. Они организуют выполнение решений Общего собрания акционеров и Совета директоров и подотчетны им. Председатель Правления и члены Правления избираются Советом директоров на 5 лет. Правление, в частности, разрабатывает годовой бюджет, инвестиционные программы, перспективные и текущие планы деятельности Общества, готовит отчеты, организует управление потоками газа, осуществляет контроль за функционированием Единой системы газоснабжения России.

В Администрацию ПАО «Газпром» входят следующие департаменты:

- департамент автоматизации систем управления технологическими процессами;

- департамент бухгалтерского учета;

- департамент внешнеэкономической деятельности;

- департамент внутреннего аудита и контроля за финансово-хозяйственной деятельностью дочерних обществ и организаций;

- департамент инвестиций и строительства;

- департамент маркетинга, переработки газа и жидких углеводородов;

- департамент по добыче газа, газового конденсата, нефти;

- департамент по информационной политике;

- департамент по работе с регионами Российской Федерации;

- департамент по транспортировке, подземному хранению и использованию газа;

- департамент по управлению имуществом и корпоративным отношениям;

- департамент по управлению делами;

- департамент по управлению персоналом;

- департамент цифровой трансформации;

- департамент стратегического развития;

- департамент экономической экспертизы и ценообразования;

- финансово-экономический департамент;

- центральный производственно-диспетчерский департамент;

- юридический департамент.

Также в ПАО «Газпром» входит 80 дочерних предприятий со 100% долевым участием компании, 29 компаний с более чем 50% участием, 39 компаний с менее чем 50% участием. Современное состояние объекта и системы управления можно охарактеризовать как прочное и стабильное.

3.2 Оценка существующих организационных мер по обеспечению информационной безопасности ПАО «Газпром»

Ядро каждой крупной компании – это ERP-система (система планирования ресурсов предприятия); в ней проходят все значимые для бизнеса процессы. В том числе: закупка, доставка, оплата продукции; управлением человеческими ресурсами, продуктами и финансовым планированием. Информация, находящаяся в ERP-системах, представляет

особую ценность для компании. Неправомерный доступ к данной информации способен понести за собой ощутимые потери, вплоть до полной приостановки бизнеса.

Согласно отчету Ассоциации специалистов по расследованию хищений/мошенничества (ACFE), в период с 2006 по 2010 гг. потери от внутренних реализованных угроз, связанных с информационной безопасностью, составили порядка 7% от ежегодной выручки. Именно поэтому особое внимание в изучении информационной безопасности компании должно быть уделено функционированию ERP-системы предприятия.

Одна из наиболее известных в мире ERP-систем — mySAP ERP (SAP R/3). Данная система принята в качестве основной в исследуемой организации SAP это полнофункциональное ERP–решение, представляющее собой набор пакетов и модулей, которые можно развертывать и дополнять по мере необходимости. В решение можно включать дополнительные возможности:

- мобильный сервис;
- деятельность на базе портала (SAP-portal);
- бизнес–аналитика.

Возможность подключения новых модулей реализована за счет технологии интеграции SAP NetWeaver [42].

В ПАО «Газпром», как и в любой крупной компании, присутствуют непрофильные виды деятельности и предприятия, не входящие в основную производственную цепочку. Этим объясняется то, что несмотря на всю мощь и масштабируемость SAP, на предприятиях отрасли находят применение и другие ERP–системы. К ним относятся: 1С и Microsoft Business Solutions–Axapta.

Основным достоинством 1С и Microsoft Axapta является открытость. Если в силу специфичности бизнес–процессов базовая функциональность оказывается недостаточной, система может быть доработана силами программистов.

3.3 Разработка рекомендаций по усилению информационной безопасности исследуемой компании

Результат анализа информационной безопасности ПАО «Газпром» свидетельствует о высоком уровне защищенности предприятия от внутренних и внешних угроз. Предприятие использует новейшее оборудование и

программное оснащение. При этом за обеспечение системы информационной безопасности отвечает специально обученный персонал, а пользователи системы постоянно получают теоретическую информацию в рамках поддержания безопасной инфраструктуры. Однако несмотря на детально проработанную систему защиты от внутренних и внешних угроз, в системе информационной безопасности ПАО «Газпром» присутствуют слабые места.

ЗАКЛЮЧЕНИЕ

Конечной целью исследовательской работы являлось составление рекомендаций, направленных на совершенствование информационной безопасности транснациональной энергетической компании ПАО «Газпром».

В процессе достижения данной цели были изучены подходы к определению понятия «экономическая безопасность предприятия», определены структурные элементы, а также рассмотрены методики оценки экономической безопасности предприятия. В дальнейшем осуществлен анализ и проведена оценка системы информационной безопасности предприятия, а также представлены рекомендации по ее повышению.

Информационная безопасность предприятия находится на высоком уровне, обеспечена защита от внутренних и внешних угроз. К слабым местам ПАО «Газпром» можно отнести:

1) использование облачных сервисов в качестве одного из способов резервирования информации;

2) наличие человеческого фактора в первом уровне аутентификации для доступа к рабочему месту специалиста;

3) использование зарубежного ПО в делопроизводстве компании;

4) возможность выполнения сотрудниками служебных обязанностей физически находясь за пределами РФ;

5) использование личных мобильных устройств при входе в рабочий кабинет сотрудника;

6) возможность использования почты сотрудника для промышленного шпионажа.

В заключительной главе научной работы представлены основные направления решения данных проблем. Ключевой сложностью является отсутствие возможности решения каждой из представленных проблем в отрыве от создания новых рисков и угроз.

Так, отказ от использования облачных сервисов повлечет за собой трудности к доступу информации для сотрудников, находящихся на дистанционном либо гибридном режиме работы. Наряду с этим, отказ приведет к увеличению риска безвозвратной потери информации, поскольку предприятие лишается одного из способов резервирования информации. Запрет на привлечение сотрудников, пребывающих за рубежом, автоматически повлечет за собой уход наиболее ценных кадров. Любой из предложенных выше способов аутентификации не лишен недостатков. Также невозможен полный отказ от использования зарубежного ПО в пользу отечественной продукции.

Как было сказано выше – система информационной безопасности ПАО «Газпром» находится на высоком уровне, однако нельзя закрывать глаза на ее недостатки, поскольку наличие даже незначительных угроз может привести к масштабной утечке либо безвозвратной ликвидации информации, которая способна полностью приостановить бизнес-процессы предприятия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 ГОСТ Р ИСО/МЭК 27001-2006 Национальный стандарт российской федерации. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности [Электронный ресурс] // электронный фонд правовой и нормативно-технической информации – Режим доступа: URL https://docs.cntd.ru/ (дата обращения: 15.05.2022).

2 ГОСТ Р ИСО/МЭК 17799 2005. Информационная технология. Практические правила управления информационной безопасностью. – М: Стандарты-информ, 2006. – 55с. (дата обращения: 15.05.2022).

3 О коммерческой тайне: федер. Закон Российской Федерации от 29 июля 2004г. №98-ФЗ: офиц. текст – Москва: Эксмо, 2017. – 16 с. (дата обращения: 15.02.2022).

4 О Стратегии экономической безопасности Российской Федерации на период до 2030 года [Электронный ресурс]: Указ Президента РФ от 13 мая 2017 г. N 208 // Справочная правовая система «Консультант плюс». – Режим доступа: URL: http://www.consultant.ru/ (дата обращения: 28.02.2022).

5 Российская Федерация. Законы «О безопасности» : Федеральный закон от 28.12.2010 № 390-ФЗ : [Электронный ресурс] (принят Государственной думой 7 декабря 2010 года : одобрен Советом Федерации 15 декабря 2010 года) // Справочная правовая система «Консультант плюс». – Режим доступа: URL: http://www.consultant.ru/ (дата обращения: 01.03.2022).

6 Указ Президента РФ от 13.05.2017 №208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» [Электронный ресурс] // Справочная правовая система «Консультант плюс». – Режим доступа: URL:http://www.consultant.ru/document/cons_doc_LAW_216629/942772dce30cfa36b671bcf19ca928e4d698a928/ (дата обращения: 02.02.2022).

7 Цифровая экономика Российской Федерации [Электронный ресурс]: Распоряжение Правительства Российской Федерации от 28.07.2017 г. №1632-

р // Справочная правовая система «Консультант плюс». – Режим доступа: URL: http://www.consultant.ru/ (дата обращения: 06.04.2022).

8 Абалкин Л.И. Экономическая безопасность России // Социально-политический журнал. 1997. № 5. 3 с.

9 Аверьянова О.В. Система и структура обеспечения экономической безопасности / О.В. Аверьянова // Экономика, управление, финансы : материалы IV междунар. науч. конф. (г. Пермь, апрель 2015 г.). – Пермь, 2015. – с. 14-16.

10 Архипов А., Городецкий А., Михайлов Б. Экономическая безопасность: оценки, проблемы, способы обеспечения / А. Архипов, А. Городецкий, Б. Михайлов // Вопр. экономики. – 2013. – № 12. – С. 36-44.

11 Архипов А., Городецккий А., Михайлов Б. Экономическая безопасность: оценки, проблемы, способы обеспечения // Вопросы экономики. 2015. №12.

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 Басалай С.В. Построение системы управления рисками для повышения экономической безопасности [Текст] / С.В. Басалай // Микроэкономика. – 2016. – № 2. – С. 70-80.

15 Бетелин В.Б. Суперкомпьютерные технологии в России: состояние и проблемы развития // Вестник Российской академии наук. Т. 85, № 11. 2015. С. 971-975.

16 Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. №4. 66 с.

17 Воропай Н.И., Сендеров С.М., Рабчук В.И. Стратегические угрозы экономической безопасности предприятия / Н.И. Воропай, С.М. Сендеров, В.И. Рабчук // ЭКО. – 2016. – № 12. – С. 42-58.

18 Глухов Н.И. «Оценка информационных рисков предприятия: учебное пособие». Иркутск ИрГУПС, 2013. 148 с.

19 Гордиенко Д.В. Основы экономической безопасности государства [Текст] : курс лекций / Д.В. Гордиенко. – М: Финансы и статистика, ИНФРА М, 2009.

20 Дворядкина Д.Б., Новикова Н.В. Экономическая безопасность [Текст] : учеб. Пособие – Екатеринбург, 2010.

21 Илларионов А.И. Критерии экономической безопасности / А. И. Илларионов // Вопросы экономики. — 1998. – №10.

22 Информационные технологии. Методы и средства обеспечения безопасности. Ч. 3. Методы менеджмента безопасности информационных технологий : ГОСТ Р ИСО/МЭК ТО 13335-3-2007. – Введ. 01.09.2007. – М. : Стандартинформ, 2007. – 76 с.

23 Красноярский край в цифрах 2019: Стат.сб./Красноярскстат. – Красноярск, 2020. – 159 с.

24 Кузнецова Е.И. Экономическая безопасность: учебник и практикум для вузов / Е.И. Кузнецова. – Москва: Юрайт, 2018. – 294 с.

25 Лелюхин С.Е. Экономическая безопасность в предпринимательской деятельности: учебник / С.Е. Лелюхин, А.М. Коротченков, У.В. Данилова. Москва: Проспект, 2017. 336 с.

26 Рогулин Ю.П. Экономическая безопасность хозяйствующих субъектов: логические схемы: учебное пособие / Рогулин Ю.П. Москва: Прометей, 2019. 136 с.

27 Савин В.А. Некоторые аспекты экономической безопасности России / В.А. Савин // Международный бизнес России. — 1995. — № 9. — 14 с.

28 Сенчагов В.К. Инновационные преобразования как императив экономической безопасности региона: система индикаторов / В.К. Сенчагов,

Ю.М. Максимов, С.Н. Митяков, О.И. Митякова // Инновации. 2011. №5. С. 56-61.

29 Терегулова Н.Ф. Финансовая устойчивость нефтегазовых предприятий // Новые технологии в газовой промышленности (газ, нефть, энергетика) : тезисы докладов XII Всероссийской конференции молодых ученых, специалистов и студентов. – 2017. – 375 с.

30 Титов В.В. Экономическая безопасность субъекта Российской Федерации/ В.В. Титов // Вестник Санкт-Петербургского университета МВД России. – №1 (53). – 2012. – с. 218-221.

31 Уразгалиев В.Ш. Экономическая безопасность : Учебник и практикум для вузов / В.Ш. Уразгалиев. – Москва : Юрайт, 2019. – 675 с.

32 Чотчаева М.З. Налоговая безопасность государства как элемент экономической безопасности / М.З. Чотчаева // Глобальный научный потенциал. – 2014. –№10 – с.88-92.

33 Шульц В.Л. Безопасность предпринимательской деятельности в 2 ч. Часть 1: учебник для академического бакалавриата / В.Л. Шульц, А.В. Юрченко, А.Д. Рудченко; под редакцией В.Л. Шульца. Москва: Издательство Юрайт, 2019, 288 с.

34 Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории: учебник для бакалавриата и магистратуры. М.: Издательство Юрайт, 2017. 309 с.

35 Экономическая и национальная безопасность [Текст]: учебник / под ред. Е.А. Олейникова. –М.: Экзамен. 2005.

36 Ярочкин В.И., Информационная безопасность: Учебние для вузов / В.И. Ярочкин. -– М.: Акад. Проект, 2018. – 544 с.

37 Международный ISO/IEC стандарт 2700. Вторая редакция 2013-10-01. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ Системы менеджмента информационной безопасности Требования [Электронный ресурс] // FSTEC Russia – федеральная служба по техническому и экспортному контролю – Режим доступа: URL https://fstec.ru/ (дата обращения: 08.05.2022).

38 Отчётность ПАО «Газпром» [Электронный ресурс] // Официальный сайт ПАО «Газпром». — URL: https://www.gazprom.ru/investors/disclosure/ reports/ (дата обращения: 02.05.2022).

39 Официальный сайт ПАО «Газпром». — URL: https://www.gazprom.ru/about/legal/policy-personal-data/ (дата обращения: 04.05.2022).

40 Официальный сайт ПАО «Газпром». [Электронный ресурс] — URL: https://sustainability.gazpromreport.ru/2018/2-people-inside/2-8-training/ (дата обращения: 02.05.2022).

41 Официальный сайт ПАО «Газпром». [Электронный ресурс] — URL: https://www.gazprom.ru/careers/statistics/ (дата обращения: 02.05.2022).

42 Програмные продукты для компаний [Электронный ресурс] // программное обеспечение SAP — URL: https://www.sap.com/ cis/index.html?url_id=auto_hp_redirect_cis (дата обращения: 08.05.2022).

43 Финансовая (бухгалтерская) отчётность ПАО «НК «Роснефть» // Официальный сайт ПАО «НК «Роснефть». — URL: https://www.rosneft.ru/Investors/statements_and_presentations/ Statements/ (дата обращения: 15.05.2022).

44 Финансовые результаты ПАО «Лукойл» [Электронный ресурс] // Официальный сайт ПАО «Лукойл» — URL: https://lukoil.ru/ (дата обращения: 05.05.2022).

45 Шегурова В.П. Сравнительная характеристика различных методик рейтинговой оценки финансового состояния промышленного предприятия / В. П. Шегурова, Е. В. Леушина. — Текст : непосредственный // Экономическая наука и практика : материалы III Междунар. науч. конф. (г. Чита, апрель 2014 г.). — Т. 0. — Чита.: Издательство Молодой ученый, 2014. — с. 80-84. — URL: https://moluch.ru/conf/econ/archive/94/ 5387/ (дата обращения: 08.05.2022).

46 Электронная торговая площадка «Группы Газпромбанка» — URL: https://etpgpb.ru/procedure/tender/price_request/78804-postavka-litsenzii-antivirusa-kasperskiy-dlya-nuzhd-ooo-gazprom-/ (дата обращения: 06.05.2022).

47 Funin O. A., Grunin S. O. economic security of the organization. St. Peters burg: Peter, 2002.

48 ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management [Электронный ресурс] // Интернетпортал – URL: http://ce.sharif.edu/courses/95-96/2/ce746-1/resources/root/Resources/ISO-IEC%2027005-2011-Risk%20Management.pdf (дата обращения: 16.05.2022).

49 NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments [Электронный ресурс] // электронный фонд правовой и нормативно-технической информации – Режим доступа: URL https://docs.cntd.ru/ (дата обращения: 08.05.2022).

50 Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology : NIST 800-30. – USA. – 2002. – 56 p. (дата обращения: 06.05.2022).

51 Specification of the information security management system: BS 7799-2:2005. – Introduction. 01.07.2005. – England. - 2005. – 86 p. (дата обращения: 03.02.2022).

ПРИЛОЖЕНИЕ А

Спектр-балльный метод А. Н. Салова и В. Г. Маслова

Наименование показателя	Зона риска	Зона опасности	Зона стабильности	Зона благополучия
Коэффициент текущей ликвидности	менее 1,2	1,2–1,5	1,5–1,8	более 1,8
Коэффициент обеспеченности собственными средствами	менее 0,05	0,05–0,1	0,1–0,15	более 0,15
Коэффициент соотношения чистых активов и уставного капитала	менее 1,0	1,0–1,5	1,5–2,0	более 2,0
Коэффициент рентабельности использования всего капитала	менее 0,05	0,05–0,1	0,1–0,15	более 0,15
Коэффициент использования собственных средств	менее 0,07	0,07–0,15	0,15–0,2	более 0,2
Коэффициент рентабельности продаж	менее 0,1	0,1–0,2	0,2–0,3	более 0,3
Коэффициент рентабельности по текущим затратам	менее 0,15	0,15–0,3	0,3–0,4	более 0,4
Коэффициент автономии	менее 0,5	0,5–0,65	0,65–0,8	более 0,8
Коэффициент соотношения привлеченных и собственных средств	более 0,8	0,8–0,5	0,5–0,2	менее 0,2
Коэффициент дебиторской задолженности	более 0,15	0,15–0,1	0,1–0,05	менее 0,05
Коэффициент абсолютной ликвидности	менее 0,2	0,2–0,3	0,3–0,4	более 0,4
Коэффициент промежуточной (быстрой) ликвидности	менее 0,7	0,7–0,85	0,85–1,0	более 1,0
Коэффициент обеспеченности запасами краткосрочных обязательств	менее 0,4	0,4–0,6	0,6–0,8	более 0,8
Общий коэффициент оборачиваемости	менее 0,4	0,4–0,6	0,6–0,8	более 0,8
Коэффициент оборачиваемости запасов	менее 2,0	2,0–3,0	3,0–4,0	более 4,0
Коэффициент оборачиваемости собственных средств	менее 0,8	0,8–0,9	0,9–1,0	более 1,0

ПРИЛОЖЕНИЕ Б

Балльная интерпретация основных регуляторов PDCA

Наименование регулятора	Зона риска	Зона опасности	Зона стабильности	Зона благополучия
проработанность документации, связанной с ИБ	1-2	3-5	6-8	9-10
обучение персонала	1-2	3-5	6-8	9-10
распределение обязанностей	1-2	3-5	6-8	9-10
уровень оснащения антивирусными программами	1-2	3-5	6-8	9-10
скорость и полнота уведомлений о нарушениях защиты	1-2	3-5	6-8	9-10
бесперебойность работы компании	1-2	3-5	6-8	9-10
уровень защиты документации	1-2	3-5	6-8	9-10
проработка системы хранения/передачи информации	1-2	3-5	6-8	9-10
контроль над соответствием политике ИБ	1-2	3-5	6-8	9-10
контроль над копированием ПО, защищенного авторским правом	1-2	3-5	6-8	9-10

ПРИЛОЖЕНИЕ В

Формулы расчета коэффициентов Спектрально-балльного метода А. Н. Салова и В. Г. Маслова

Название группы	Коэффициент	Формула
I. Показатели оценки структуры баланса	Коэффициент текущей ликвидности	$\frac{\text{Об. активы}}{\text{Кратк. обяз.}}$
	Коэффициент обеспеченности собственными средствами	$\frac{\text{СК} - \text{ВНА}}{\text{Об. активы}}$
	Коэффициент соотношения чистых активов и уставного капитала	$\frac{\text{А} - \text{Задол. уч. по взн в УК} - \text{ДСО} - \text{КСО} - \text{ДБП}}{\text{Уставный капитал}}$
II. Показатели рентабельности	Коэффициент рентабельности использования всего капитала	$\frac{\text{ЧП}}{\text{Асрг}}$
	Коэффициент использования собственных средств	$\frac{\text{ЧП}}{\text{СК}_{\text{срг}}}$
	Коэффициент рентабельности продаж	$\frac{\text{ВП}}{\text{Выручка}}$
	Коэффициент рентабельности по текущим затратам	$\frac{\text{ВП}}{\text{Себестоимость продаж}}$
III. Показатели финансовой устойчивости	Коэффициент автономии	$\frac{\text{Собственный капитал}}{\text{Валюта баланса}}$
	Коэффициент соотношения привлеченных и собственных средств	$\frac{\text{Собственный капитал}}{\text{Заёмный капитал}}$
	Коэффициент дебиторской задолженности	$\frac{\text{ДЗ}_{\text{срг}}}{\text{Выручка}}$
IV. Показатели платежеспособности	Коэффициент абсолютной ликвидности	$\frac{\text{ДС} + \text{КФВ}}{\text{КСО}}$

Окончание приложения В

Название группы	Коэффициент	Формула
	Коэффициент промежуточной (быстрой) ликвидности	$\frac{ДС + КФВ + ДЗ}{КСО}$
	Коэффициент обеспеченности запасами краткосрочных обязательств	$\frac{СК - ВНА}{З}$
V. Показатели деловой активности	Общий коэффициент оборачиваемости	$\frac{Выручка}{Активы_{срг}}$
	Коэффициент оборачиваемости запасов	$\frac{Выручка}{Запасы_{срг}}$
	Коэффициент оборачиваемости собственных средств	$\frac{Выручка}{СК_{срг}}$

Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, государственного управления и финансов

Кафедра финансов и управления рисками

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И.С. Ферова
подпись инициалы, фамилия
«15» июня 2022 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (НА ПРИМЕРЕ ПАО «ГАЗПРОМ»)

Руководитель	_____	к.э.н., доцент	И.Г. Кузьмина
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		Ю.С. Киевский
	подпись, дата		инициалы, фамилия
Рецензент	_____	Руководитель департамента информационных технологий СФУ	К.Н. Захарьин
	подпись, дата	должность, ученая степень	инициалы, фамилия
Нормоконтролер	_____		Е.В. Шкарпетина
	подпись, дата		инициалы, фамилия

Красноярск 2022