Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт социально – гуманитарных технологий
Направление подготовки 38.04.02 Менеджмент
Кафедра менеджмента

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Защита от внутрикорпоративного мошенничества в крупных технологических компаниях

УДК 005.332.5.:005.334:366.46

Студент

Группа	ФИО	Подпись	Дата
3АМ5Б	Засорин И.А.		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Данков А.Г.	к.и.н.		

КОНСУЛЬТАНТЫ:

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Черепанова Н.В.	к.ф.н.		

Нормоконтроль

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель	Громова Т.В.			

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
Менеджмента	Чистякова Н.О.	к.э.н.		

Томск - 2017г.

Планируемые результаты обучения по ООП 38.04.02 Менеджмент

Код результата	Результат обучения (выпускник должен быть готов)
Общепрофессиональные и профессиональные компетенции	
$Р_1$	Умение применять теоретические знания, связанные с основными процессами управления развитием организации, подразделения, группы (команды) сотрудников, проекта и сетей; с использованием методов управления корпоративными финансами, включающие в себя современные подходы по формированию комплексной стратегии развития предприятия, в том числе в условиях риска и неопределенности
$Р_2$	Способность воспринимать, обрабатывать, анализировать и критически оценивать результаты, полученные отечественными и зарубежными исследователями управления; выявлять и формулировать актуальные научные проблемы в различных областях менеджмента; формировать тематику и программу научного исследования, обосновывать актуальность, теоретическую и практическую значимость избранной темы научного исследования; проводить самостоятельные исследования в соответствии с разработанной программой; представлять результаты проведенного исследования в виде научного отчета, статьи или доклада
$Р_3$	Способность анализировать поведение экономических агентов и рынков в глобальной среде; использовать методы стратегического анализа для управления предприятием, корпоративными финансами, организацией, группой; формировать и реализовывать основные управленческие технологии для решения стратегических задач
$Р_4$	Способность разрабатывать учебные программы и методическое обеспечение управленческих дисциплин, умение применять современные методы и методики в процессе преподавания управленческих дисциплин
Общекультурные компетенции	
$Р_5$	Способность понимать необходимость и уметь самостоятельно учиться и повышать квалификацию в течение всего периода профессиональной деятельности, развивать свой общекультурный, творческий и профессиональный потенциал
$Р_6$	Способность эффективно работать и действовать в нестандартных ситуациях индивидуально и руководить командой, в том числе международной, по междисциплинарной тематике, обладая навыками языковых, публичных деловых и научных коммуникаций, а также нести социальную и этическую ответственность за принятые решения, толерантно воспринимая социальные, этические, конфессиональные и культурные различия

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт социально – гуманитарных технологий
Направление подготовки (специальность) 38.04.02 Менеджмент
Кафедра менеджмента

УТВЕРЖДАЮ:
Зав. кафедрой менеджмента

_____ _____ Чистякова Н.О.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Магистерской диссертации

Студенту:

Группа	**ФИО**
3АМ5Б	Засорину Ивану Александровичу

Тема работы:

Защита от внутрикорпоративного мошенничества в крупных технологических компаниях	
Утверждена приказом директора (дата, номер)	№ 2714/с от 18.04.2017

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	1. Нормативно-правовые документы. 2. Научная литература. 3. Данные о деятельности предприятий, полученные в ходе прохождения преддипломной практики.

Перечень подлежащих исследованию, проектированию и разработке вопросов	1. Теоретические основы системы экономической безопасности для защиты от внутрикорпоративного мошенничества. 2. Анализ ситуации на предприятиях-объектах исследования с точки зрения защиты от внутрикорпоративного мошенничества. 3. Практические рекомендации по созданию системы экономической безопасности для защиты от внутрикорпоративного мошенничества.
Перечень графического материала	
Консультанты по разделам выпускной квалификационной работы	
Раздел	**Консультант**
Социальная ответственность	Черепанова Н.В.
Английская часть	Гаспарян Г.А.
Названия разделов, которые должны быть написаны на русском и иностранном языках:	
Теоретические основы экономической безопасности на предприятии	Theoretical basis of economic security in the enterprise

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	

Задание выдал руководитель:

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент	Данков А.Г.	к.и.н.		

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
ЗАМ5Б	Засорин Иван Александрович		

Реферат

Выпускная квалификационная работа содержит 120 страниц, 8 рисунков, 4 таблицы, 38 использованных источников, 1 приложение.

Ключевые слова: Внутрикорпоративное мошенничество, экономическая безопасность предприятия.

Объектом исследования является система экономической безопасности на крупных технологических предприятиях. Предметом исследования являются организационные инструменты защиты предприятия от внутрикорпоративного мошенничества.

Цель работы - выявить направления и методы борьбы с внутрикорпоративным мошенничеством для улучшения экономической безопасности крупного технологического предприятия.

В процессе исследования проводился анализ хозяйственной деятельности предприятия, изучались принципы функционирования системы экономической на предприятии.

В результате исследования были предложены наиболее эффективные меры по защите предприятия от внутрикорпоративного мошенничества.

Степень внедрения: принято к внедрению.

Область применения: экономика и управление на предприятии.

Экономическая эффективность/ значимость работы: в работе даны практические рекомендации по созданию системы экономической безопасности и защите от внутрикорпоративного мошенничества.

В будущем планируется применить результаты исследования в практической деятельности.

Оглавление

Введение

В современных условиях, когда достижения национальной экономики обеспечиваются усилиями предприятий на внутренних рынках, особое внимание уделяется внутренней безопасности данных предприятий.

Основными проблемами, представляющими угрозу экономической безопасности предприятий, в настоящее время стали угрозы, связанные с внутрикорпоративным мошенничеством, до сих пор данной проблеме уделялось мало внимания, хотя эта проблема является весьма актуальной в современных условиях развития рыночных механизмов.

Внутрикорпоративное мошенничество – чаще всего совсем не то мошенничество, о котором идет речь в Уголовном кодексе РФ. Как правило, под ним понимаются злоупотребления сотрудников и других лиц, которые могут принимать решения по сделкам, распоряжаться денежными средствами предприятия или влиять на принятие решений с целью незаконного получения личного дополнительного дохода, тем самым нанося ущерб предприятию.

Существует мнение, что бороться с этим бесполезно. Но на сегодняшний день большинство руководителей заинтересованы в том, чтобы свести к минимуму риски, связанные с этими явлениями, раскрыть уже совершенные злоупотребления и предотвратить рецидивы.

Актуальность данной темы обусловлена тем, что предприятия осуществляя свою деятельность постоянно находятся в условиях различных внешних и внутренних рисков реагируя на данные риски исходя из их значимости и ущерба, который они могут причинить предприятию. Внутрикорпоративное мошенничество в современных реалиях можно выделить в отдельную группу риска, которая несет для предприятия дополнительную рисковую нагрузку, толкая руководство предприятия на борьбу не только с рисками, связанными с производственной деятельностью, но и на борьбу с собственными сотрудниками.

Обобщая можно сказать, что основными проблемами при борьбе с данного вида угрозами являются:

Отсутствие определенных составляющих экономической безопасности с точки зрения внутрикорпоративного мошенничества;

Затруднения с определением оценочных критериев эффективности экономической безопасности с точки зрения внутрикорпоративного мошенничества;

Таким образом, **целью данной выпускной квалификационной работы** является – выявить направления и методы борьбы с внутрикорпоративным мошенничеством для улучшения экономической безопасности крупного технологического предприятия.

Для реализации поставленной цели, необходимо решить следующие **задачи:**

– Рассмотреть теоретические основы экономической безопасности предприятия.

– Провести сравнительный анализ систем экономической безопасности предприятий АО «Импера» и АО «Кроника».

– Предложить свое видение данной проблемы, а также методы, которые, по нашему мнению, являлись бы не менее эффективными в борьбе с внутрикорпоративным мошенничеством с точки зрения экономической безопасности предприятия.

Объектом исследования является система экономической безопасности на крупных технологических предприятиях.

Предметом исследования являются организационные инструменты защиты предприятия от внутрикорпоративного мошенничества.

Методы исследования. В ходе проведения данного исследования были использованы методы эмпирического исследования (наблюдение и сравнение); методы, используемые как на эмпирическом, так и на теоретическом уровне исследования (анализ и синтез, индукция и дедукция, моделирование и др.),

методы теоретического исследования (восхождение от абстрактного к конкретному).

Практическая и научная значимость. Научная значимость работы заключается в разработке собственной модели функционирования системы экономической безопасности на предприятии. Также в ходе исследования были получены результаты практического характера, а именно разработаны новые принципы и инструменты защиты от внутрикорпоративного мошенничества в частных и государственных технологических компаниях.

В ходе подготовке данного исследования был использован широкий спектр учебной и научной литературы. Среди всего спектра работ по данной теме стоит отметить книгу «Экономическая безопасность предприятия». Суглобов А. Е., Хмелев С. А., Орлова Е. А. Юнити-Дана. 2013 год, 272 страницы. Данная книга дает комплексное представление о системе экономической безопасности фирмы и ее составляющих. Представлены классификация и оценка опасностей и угроз коммерческой организации, рассмотрены предпринимательские риски и управление ими, общая структура и характеристика компонентов предпринимательского риска, методика расчета локальных и интегральных показателей экономической безопасности коммерческой организации. Приводятся основные способы реализации угроз бизнесу в российских условиях и методы противодействия им, количественной оценке событий, угроз и степени обеспечения экономической безопасности фирмы при помощи матриц событий, выбора оптимальной стратегии предприятия, достижения поставленных целей.

Так же необходимо отметить монографию «Экономическая и информационная безопасность предпринимательства». А. А. Одинцов. 2012 г. 336 страницы. В данной книге приведены сведения, касающиеся государственного регулирования и внутрифирменного управления в сфере обеспечения экономической и информационной безопасности предпринимательства. Рассмотрены методология, организация, информационное обеспечение, экономические методы, эффективность,

правовая основа и кадровое обеспечение с учетом отечественного и зарубежного опыта работы в области экономической безопасности.

Особую роль при подготовке работы сыграла книга «Экономическая безопасность». Грунин О.В, Макаров М.Б, Михайлов Е.В, Скаридов К.Г. Дрофа. 2014 г. 272 страницы. В данной книге излагаются теоретические и практические вопросы обеспечения экономической безопасности. Особое внимание уделяется проблемам анализа и прогнозирования состояния экономической безопасности на различных уровнях хозяйствования, а также проблеме криминализации экономики и основным способам ее разрешения.

1 Теоретические основы системы экономической безопасности

1.1 Экономическая безопасность, основные определения

В настоящее время вопросы обеспечения условий экономического роста предприятия выходят на первый план. На экономический рост предприятия может оказывать влияние общеэкономическая ситуация в мире в целом и в государстве в частности. Экономическая ситуация в государстве, кроме ряда прочих факторов, находится в зависимости от способности соответствующих государственных органов обеспечить как экономическую безопасность государства, так и хозяйствующих субъектов —предприятий. В современных условиях процесс успешного функционирования и экономического развития российских предприятий во многом зависит от совершенствования их деятельности в области обеспечения экономической безопасности.

Как это ни странно, в официальных документах РФ отсутствует понятие экономической безопасности предприятия (организации, юридического лица). Поэтому приведем несколько мнений авторов книг, посвященных экономической безопасности предприятий.

По мнению Е.А. Олейникова, «экономическая безопасность предприятия — это состояние наиболее эффективного использования корпоративных ресурсов для предотвращения угроз и для обеспечения стабильного функционирования предприятия в настоящее время и в будущем». В другом труде — «Стратегия бизнеса», подготовленного к изданию Институтом стратегического анализа и развития предпринимательства, — сказано, что «экономическая безопасность предприятия – это такое состояние данного хозяйственного субъекта, при котором жизненно важные компоненты структуры и деятельности предприятия характеризуются высокой степенью защищенности от нежелательных изменений» [3,2].

Н.В. Матвеев предлагает следующее определение экономической безопасности предприятия: «это состояние предприятия, при котором обеспечивается стабильность его функционирования, финансовое равновесие и

регулярное извлечение прибыли, возможность выполнения поставленных целей и задач, способность к дальнейшему развитию и совершенствованию».

В литературе встречаются и другие очень близкие к цитируемым определения экономической безопасности предприятия. Например, то, что «экономическая безопасность - это состояние наиболее эффективного использования всех видов ресурсов в целях предотвращения (нейтрализации, ликвидации) угроз и обеспечения стабильного функционирования предприятия в условиях рыночной экономики».

По мнению О.В. Климочкина, экономическая безопасность предприятия (фирмы, корпорации) — это «состояние защищенности его жизненно важных интересов в финансово-экономической, производственно-хозяйственной, технологической сферах от различного рода угроз, в первую очередь социально-экономического плана, которое наступает благодаря принятой руководством и персоналом системы мер правового, организационного, социально-экономического и инженерно-технического характера» [2].

Проанализировав понятийный аппарат, на наш взгляд, наиболее полно отражает и раскрывает сущность трактовки «экономическая безопасность» следующее определение: «экономическая безопасность предприятия — это обеспечение защищенности жизненно важных интересов предприятия от внутренних и внешних угроз, организуемое администрацией и коллективом предприятия путем реализации системы мер правового, экономического, организационного, инженерно-технического и социально-психологического характера».

Целью обеспечения экономической безопасности предприятия является ограждение его собственности и сотрудников от источников внешних и внутренних угроз безопасности, предотвращение причин и условий, порождающих их [11].

1.2 Угрозы экономической безопасности

Для каждого предприятия экономические угрозы сугубо индивидуальны и зависят от ряда факторов (отрасль, масштаб предприятия, сфера деятельности и т.д.), все угрозы делятся на две категории «внешние» и «внутренние». Вместе с тем, на наш взгляд, указанные категории включают отдельные элементы, которые приемлемы практически к любому субъекту хозяйственной деятельности. Для более удобного восприятия внешних и внутренних угроз, мы объединили их в таблицу [5].

Таблица 1 – Внешние и внутренние угрозы экономической безопасности предприятия

Внешние угрозы	**Внутренние угрозы**
Активное участие представителей власти и управления в коммерческой деятельности.	Действия или бездействия (в том числе умышленные и неумышленные) сотрудников предприятия, противоречащие интересам его коммерческой деятельности, следствием которых могут быть нанесение экономического ущерба Предприятию.
Использование криминальных структур для воздействия на конкурентов.	Утечка или утрата информационных ресурсов (в том числе сведений, составляющих коммерческую тайну и / или конфиденциальную информацию).
Отсутствие законов, позволяющих в полном объеме противодействовать недобросовестной конкуренции.	Подрыв делового имиджа в бизнес-кругах.
Отсутствие в стране благоприятных условий для проведения научно-технических исследований.	Возникновение проблем во взаимоотношениях с реальными и потенциальными партнерами (вплоть до утраты важных контрактов).
Отсутствие подробной и объективной информации о субъектах предпринимательской деятельности и об их финансовом положении.	Конфликтных ситуаций с представителями криминальной среды, конкурентами, контролирующими и правоохранительными органами, производственный травматизм или гибель персонала и т.д.
Отсутствие культуры ведения дел в предпринимательской среде.	

Как положительное влияние внешней среды следует рассматривать технические и управленческие нововведения, которые оказывает комплексное воздействие на деятельность всего предприятия. Предприятие может принять эти нововведения к реализации, а может и игнорировать их, однако

необходимость учитывать нововведения диктуется рядом объективных причин. В результате инновационных процессов появляются новые способы и средства производства. Это объективно предопределяет необходимость активного вмешательства предприятий в инновационные процессы, критического анализа возможных средств и способов изготовления одного и того же вида продукции. Но это только одна сторона вопроса. Вторая — многообразие форм организации производства и труда, путей повышения эффективности производства. Необходимость учитывать появляющиеся нововведения как в области технологии производства, так и в сфере организации производства и управления обусловлена, как минимум, двумя причинами, а именно возможностью: снизить издержки производства и тем самым увеличить прибыль и получить конкурентные преимущества на рынке; расширить занимаемый сегмент рынка или выход на новые рынки сбыта. В конечном итоге и первое, и второе направления должны привести к росту прибыли предприятия, укреплению его конкурентных позиций на рынке и повышению уровня экономической безопасности [5].

Следует отметить, что сегодня не все руководители предприятий готовы в полной мере оценить необходимость создания надежной системы экономической безопасности. Особенно же сложно бывает определить конкретные действия, необходимые для защиты тех или иных жизненно важных ресурсов. Вследствие этого, многие руководители ограничиваются созданием на предприятии охранных структур, почти полностью, исключая из арсенала организационно – технические и правовые методы, средства и способы защиты информации.

Меры обеспечения сохранности информации на отдельном предприятии могут быть различны по масштабам и формам и зависеть от производственных, финансовых и иных возможностей предприятия, от количества и качества охраняемых секретов. При этом выбор таких мер необходимо осуществлять, исходя их принципа разумной достаточности, придерживаясь в финансовых расчетах «золотой середины», так как чрезмерное закрытие информации, так

же, как и халатное отношение к ее сохранению, могут вызвать потерю определенной доли прибыли или привести к серьезным убыткам.

Порядок действий для защиты жизненно важных ресурсов предприятия подразумевает, в первую очередь то, что необходимо дать классификацию всем факторам риска, которые могут наступить в процессе деятельности предприятия. Таким образом, все факторы риска, опасности и угрозы, могут быть сгруппированы по следующим классификационным признакам:

1) По возможности прогнозирования:

– прогнозируемые - возникающие при известных обстоятельствах, выявленные из прошлого опыта и обобщенные отраслевой наукой и закрепленные в законах, стандартах, руководящих технических материалах и иных нормативных документах;

– непредсказуемые - форс-мажорные обстоятельства, технологические достижения и открытия, и иные, неизбежные, по существу.

2) По источнику происхождения:

– объективные возникают без участия и помимо воли субъектов системы - состояние рыночной конъюнктуры, технологические достижения и открытия, форс-мажорные обстоятельства и т. д.;

– субъективные - умышленные или неумышленные действия людей, органов власти и государственных организаций, конкурентная борьба, преступность и иные, влияющие на экономические отношения предприятия на рынке.

3) По возможности предотвращения:

– форс-мажорные отличаются непреодолимостью воздействия (природные катаклизмы, техногенные катастрофы, войны, эпидемии, которые заставляют решать и действовать вопреки намерению) и представляют особую сложность предотвращения бюджетными средствами;

– предотвратимые могут быть предусмотрены на стадии планирования бизнеса, процессов и технологий для минимизации или полного предотвращения возможного ущерба в случае реализации фактора риска.

4) По вероятности наступления:

– явные, очевидные, обусловленные рыночными (экономическими и юридическими) законами;

– латентные - неявные, временно скрытые и трудно обнаруживаемые. их проявление или не проявление может быть обусловлено экономической конъюнктурой, следствием макроэкономических явлений, а также конкурентной борьбой и способами ее ведения. внезапность их проявления может иметь субъективный характер и трудно прогнозируема даже при известной вероятности наступления.

5) По природе их возникновения:

– экономические - конъюнктурные (рыночные) изменения;

– политические - смена власти, введение эмбарго;

– правовые - законодательное регулирование деятельности, лицензирование, таможня;

– техногенные - аварии и катастрофы, истощение ресурсов;

– экологические - истощение ресурсов, климатические изменения;

– конкурентные - "черный" PR, недобросовестная конкуренция;

– контрагентские - неисполнение обязательств, мошенничество;

– и др.

6) По значимости или существенности ущерба:

– несущественные - не влияющие на рыночное состояние компаний;

– существенные - потеря значительной части материальных и финансовых ресурсов;

– значительные - утрата конкурентных преимуществ, возможно банкротство;

– катастрофические - невозможно продолжение хозяйственной деятельности, неизбежное банкротство.

7) По степени вероятности:

– невероятные - при крайне низкой вероятности совпадения обстоятельств возникновения угрозы;

– маловероятные - не требуют планирования превентивных мер как разновидность форс-мажорных обстоятельств;

– вероятные - слабо прогнозируемые, требующие планирование в зависимости от значимости ущерба;

– весьма вероятные - прогнозируемые, планируемые и обеспеченные бюджетом;

– неизбежные - легко прогнозируемые, обусловленные природой возникновения, планируемые и обеспеченные бюджетом.

8) По признаку их осуществления во времени:

– непосредственная - с определенной вероятностью осуществления;

– близкая (до 1 года) - прогнозируемая и планируемая;

– далекая (свыше 1 года) - не предусматривается текущим бюджетом.

9) По признаку их осуществления в пространстве:

– на территории предприятия;

– на территории, прилегающей к предприятию;

– на территории региона;

– на территории страны;

– на зарубежной территории.

10) По способам осуществления:

– промышленный шпионаж;

– хищение;

– вербовка и подкуп персонала;

– психологическое воздействие на персонал;

– технологический доступ;

– другие.

11) По сфере возникновения:

– внутренние факторы связаны с хозяйственной деятельностью предприятия и его персонала. Обусловлены бизнес-процессами и оказывающие влияние на результаты хозяйственной деятельности - форма и качество управления предприятия, соблюдение технологий, организация труда и социальной сферы персонала и многие другие;

– внешние возникают за пределами предприятия, связаны с конъюнктурой рынка и средой функционирования предприятия, изменение которых могут привести к возникновению ущерба - социально-экономические, политические, юридические, технологические, криминалистические и другие. [7]

Действия же, определяемые как угрозы, сознательно направлены на получение какой – либо выгоды от экономической дестабилизации предприятия, от посягательств на ее экономическую безопасность.

Деятельность руководства предприятия, несмотря на рискованный характер, в общем соответствует действующему законодательству. Угрозы, как правило, предполагают нарушение законодательных норм (той или иной отрасли права — гражданского, административного, уголовного) и предполагают определенную ответственность лиц, их осуществляющих. Для угроз экономической безопасности предпринимательской деятельности характерны три признака:

– сознательный и корыстный характер;

– направленность действий на нанесение ущерба субъекту предпринимательства;

– противоправный характер.

Как уже было сказано выше все угрозы можно разделить на внешние и внутренние. Отсюда следует что действия, рассматриваемые как угрозы, также можно разделить на внутренние и внешние. К внешним могут относиться,

например, хищение материальных средств и ценностей лицами, не работающими на данном предприятии, промышленный шпионаж, незаконные действия конкурентов, вымогательство со стороны криминальных структур. Внутренние угрозы — разглашение собственными сотрудниками конфиденциальной информации, низкая квалификация специалистов, разрабатывающих деловые документы (договоры), неэффективная работа службы экономической безопасности и лиц, отвечающих за проверку контрагентов. Наибольшую опасность, как правило, представляют внешние угрозы, поскольку внутренние угрозы зачастую — это реализация внешних «заказов».

По статистике 81,7 процентов угроз совершается либо самим персоналом предприятия, либо при его прямом или опосредованном участии (внутренние угрозы); 17,3 процентов — это внешние угрозы или преступные действия; 1,0 процентов — угрозы со стороны случайных лиц [4].

Но не смотря на сложную экономическую обстановку как на внешних, так и на внутренних рынках России, по данным министерства внутренних дел (МВД) в 2016 году по сравнению с январем – декабрем 2015 года на 3,3 процента сократилось число преступлений экономической направленности, выявленных правоохранительными органами. Всего выявлено 108,8 тысяч преступлений данной категории, удельный вес этих преступлений в общем числе зарегистрированных составил 5,0 процентов. Материальный ущерб от указанных преступлений (по оконченным и приостановленным уголовным делам) составил 397,98 млрд. руб. Тяжкие и особо тяжкие преступления, в общем числе выявленных преступлений экономической направленности, составили 59,9 процентов. Подразделениями органов внутренних дел выявлено 93,5 тысяч преступлений экономической направленности, их удельный вес в общем массиве преступлений экономической направленности составил 86 процентов.

Также стоит отметить, что по данным Российского обзора экономических преступлений за 2016 год почти половина всех компаний и

организаций (48 процентов) столкнулись с экономическими преступлениями за последние два года. Однако это значительно ниже результата в 2014 году, когда соответствующий показатель составил 60 процентов. Тем не менее уровень экономической преступности в России остается выше, чем общемировой средний показатель (36 процентов), а также выше результатов по «большой семерке развивающихся стран» (29 процентов) и странам Восточной Европы (33 процента). Стоит отметить, что из числа тех, кто столкнулся с экономическими преступлениями за последние два года, 33 процента зафиксировали более 10 случаев мошенничества. [39].

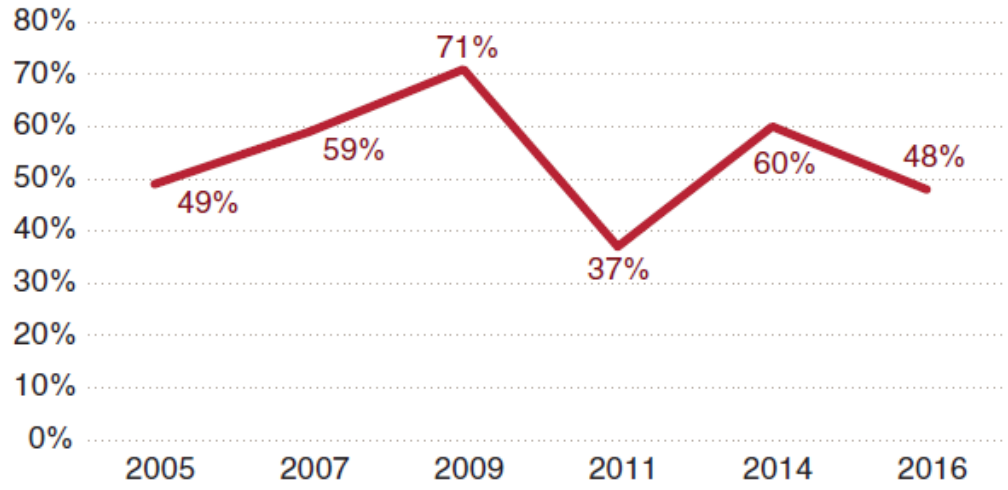


Рисунок 1 – Уровень экономической преступности в России

Снижение уровня экономической преступности в России можно объяснить несколькими причинами. Во-первых, многие руководители предприятий свидетельствуют об усилении роли функции внутреннего аудита, а также о совершенствовании других механизмов выявления мошеннических действий. Практика показывает, что предприятия, которые разработали механизмы выявления противоправных действий и реализовали программы управления рисками мошенничества, лучше подготовлены к выявлению и предотвращению мошенничества. Во-вторых, в последнее время в России произошли большие изменения в области противодействия коррупции, включая законодательные инициативы, направленные на применение передовой международной практики.

Рисунок 2 – Наиболее распространенные виды экономических преступлений

Как можно заметить в России самым распространенным видом экономического преступления считается незаконное присвоение активов. Например, 72 процента руководителей в России предприятия которых столкнулись с экономическими преступлениями, стали жертвами незаконного присвоения активов. Неудивительно, что незаконное присвоение активов преобладает над другими видами экономических преступлений. Как правило, его легче выявить, поскольку этот вид мошенничества не такой сложный, как например взяточничество и коррупция или киберпреступления.

Мошенничество в сфере закупок товаров и услуг отметили 33% руководителей, что ставит его на второе место среди экономических преступлений, с которыми чаще всего сталкиваются предприятия в России. Стоит отметить, что количество руководителей в России, указавших этот вид экономического преступления среди самых распространенных, на 10% больше

среднего значения по всему миру. По нашему мнению, этот вид мошенничества представляет собой двойную угрозу, поскольку он оказывает негативное воздействие как на коммерческий, так и на государственный сектор.

В России количество руководителей, отметивших взяточничество и коррупцию, больше, чем в среднем по всему миру (30 процентов и 24 процента соответственно). Однако по сравнению с двумя годами ранее количество ответов, в которых были указаны взяточничество и коррупция, значительно уменьшилось – с 58 процентов в 2014 году до 30 процентов в 2016 году.

Киберпреступления были указаны в 32 процентах ответов. В результате они заняли второе место среди видов мошенничества, с которыми чаще всего сталкиваются предприятия. В то же время количество руководителей в России, указавших в своих ответах киберпрестпуления, оказалось меньше (23 процента), причем по сравнению с 2014 годом ситуация изменилась незначительно – два года назад таких руководителей было 25 процентов. Необходимо помнить, что значительный процент тех, кто не указал в своих ответах киберпрестпуления, возможно, пострадали от этого вида мошенничества даже не зная об этом. [39].

При этом стоит понимать, что любое экономическое преступление, в независимости от тяжести совершения, способно оказывать отрицательное воздействие на предприятие как в краткосрочной, так и в долгосрочной перспективе.

Рисунок 3 – Отрицательные последствия экономических преступлений

На долгосрочные результаты деятельности существенное воздействие оказывает косвенный ущерб, который включает широкий спектр последствий: приостановка деятельности, следственные и превентивные мероприятия, меры по устранению причин правонарушений и, что особенно важно, ущерб, который наносится морально – психологическому климату в предприятии и его деловой репутации. В России 50 процентов предприятий, которые столкнулись с экономическими преступлениями за последние два года, отметили, что противоправные действия оказали значительное отрицательное влияние на морально – психологический климат в предприятии. При этом руководителей в России меньше беспокоит отрицательное влияние экономических преступлений на отношения с партнерами по бизнесу (35 процентов) и на репутацию/имидж (34 процента).

Существует множество мотивов совершения экономических преступлений. Чаще всего возникает три самых распространенных фактора, обуславливающих совершение мошенничества (так называемый «Треугольник мошенничества»): возможность или способность совершить экономическое

преступление; определенная мотивация или внешнее давление; и возможность обосновать совершенное экономическое преступление/самооправдание.

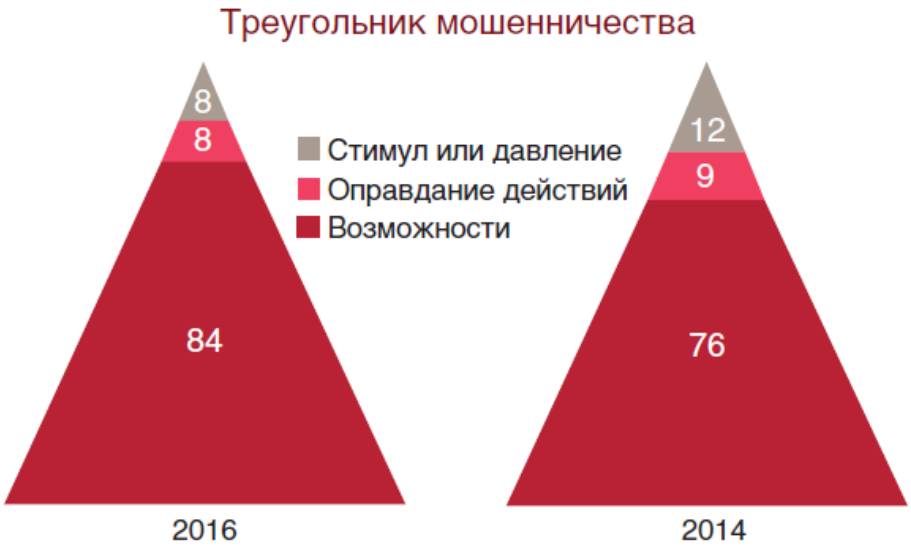


Рисунок 4 – Треугольник мошенничества

В России возможность или способность совершить преступление остается самым весомым фактором по мнению руководителей (84 процента). Его значимость выросла на 8 процентов по сравнению с 2014 годом. Мотивация или внешнее давление, а также возможность обосновать совершенное экономическое преступление/самооправдание находятся на одном уровне по своей значимости (8 процентов) [39].

Тенденция к увеличению доли этого фактора вызывает беспокойство. Это означает, что компании должны свести к минимуму такие «лазейки». Для этого необходимо применять упреждающий подход, с тем чтобы обеспечить эффективное управление существенными рисками мошенничества, используя механизмы выявления и предотвращения противоправных действий.

Продолжая анализировать статистические данные, можно заметить, что чаще всего внутренние угрозы совершаются людьми, хорошо осведомленными о всех тонкостях и нюансах деятельности предприятия, а также имеющих доступ к информации о финансовых сделках предприятия. Как показывает практика такими людьми почти всегда оказываются руководители внутренних структурных подразделений и их ближайшие заместители.

При совершении каких – либо действий, носящих характер угрозы, таких как:

- неправильное обращение с материальными ценностями;
- воровство, хищение;
- внутрифирменное мошенничество.

в первую очередь присутствует психологических фактор того что не потому, что это нужно сделать, а просто потому, что это можно сделать, а также лоббизм собственных интересов, целью которых является «нечестное» обогащение.

1.3 Инструменты обеспечения экономической безопасности

Одним из наиболее значимых элементов экономической безопасности предприятия являются инструменты ее обеспечения, которые представляют собой совокупность законодательных актов, правовых норм, побудительных мотивов и стимулов, методов, мер, сил и средств, с помощью которых обеспечивается достижения целей безопасности и решения стоящих задач. Стоит также отметить, что для каждого отдельно взятого предприятия, обеспечивающего свою экономическую безопасность перечень инструментов, будет сугубо индивидуальный.

Как показывает практика большинство российских предприятий используют те инструменты и методы, которые хорошо зарекомендовали себя в международной практике внутрикорпоративного мошенничества.

Рисунок 5 – Методы выявления мошенничества

Обращаясь к статистическим данным за последние два года, мы видим, что службы внутреннего аудита и службы безопасности компаний первыми выявляют большинство экономических преступлений (20 процентов и 15 процентов соответственно) [37].

Руководство предприятия, определяя характер мер и инструментов, обеспечения экономической безопасности должны исходить из особенностей сферы и масштабов деятельности предприятия, объектов, подлежащих защите, учитывать возможности материально-технического и финансового обеспечения мероприятий по безопасности, таким образом формируя систему. Все подразделения системы в полном объеме создаются лишь крупными предприятиями. Небольшие предприятия ограничиваются группами внутренней безопасности, состоящими из охранников и персонала, занимающегося настройкой и ремонтом технических средств защиты.

Системный подход к формированию и обеспечения экономической безопасности предприятия предполагает, что необходимо учитывать все реальные условия его деятельности, а сама система должна иметь четко

очерченные элементы, схему их действия и взаимодействия. Система обеспечения экономической безопасности предприятия состоит из нескольких блоков, одновременное действие которых призвано обеспечить достаточную для расширенного воспроизводства капитала предприятия прибыль, получаемую в результате соблюдения интересов предприятия, т.е. в результате взаимодействия предприятия с субъектами внешней среды. Система обеспечения экономической безопасности предприятия может иметь различную степень структуризации и формализации.

Действие системы обеспечения экономической безопасности предприятия призвано организационно оформить взаимодействия предприятия с субъектами внешней и внутренний среды. Результатом функционирования данной системы является поступление необходимых для организации процесса производства ресурсов и информации в соответствии с системой приоритетных интересов предприятия, минимизация затрат на приобретение ресурсов в необходимом количестве и должного качества.

Основное назначение системы обеспечения экономической безопасности предприятия заключается в создании и реализации условий, обеспечивающих экономическую безопасность предприятия. Эти условия определены исходя из критерия экономической безопасности и ее уровня. Действие системы должно быть направлено на обеспечение экономической безопасности в деятельности предприятия, как в настоящее время, так и на перспективу.

Условия обеспечения экономической безопасности предприятия нельзя рассматривать изолированно, они тесно взаимосвязаны. Реализация условий обеспечения экономической безопасности предприятия возможна либо с использованием мер организационного характера, которые, как правило, не нуждаются в инвестиционной поддержке (либо она незначительна), либо с привлечением определенного объема инвестиций. В первом случае речь идет о не капиталоемком создании условий обеспечения экономической безопасности предприятия, во втором — создание условий следует считать капиталоемким.

Понятно, что при недостатке прибыли предприятия должны в первую очередь реализовывать те условия обеспечения их экономической безопасности, которые не требуют инвестиционной поддержки. И только после завершения реализации не капиталоемких мероприятий по обеспечению экономической безопасности предприятия должны приступать к реализации условий, требующих инвестиционной поддержки.

Система экономической безопасности предприятия и механизм ее обеспечения предусматривают решение задач экономической безопасности не только специально созданным подразделением, а при активном участии всех отделов и служб предприятия в пределах возложенных на руководителей структурных подразделений обязанностей по проблемам безопасности.

Таким образом, главная роль в обеспечении экономической безопасности предприятия принадлежит его персоналу, кадровый потенциал или ресурс – это основной ресурс предприятия. Только он может приносить прибыль, но одновременно персонал является источником всех внутренних угроз экономической безопасности, и, в конечном счете, залог успеха любых управленческих инноваций - это лояльность и мотивированность сотрудников.

Проводя работу по обеспечению экономической безопасности предприятия, следует установить взаимосвязь угроз со стороны конкурентов, злоумышленников и рисков, возникающих в процессе деятельности предприятия во времени и в пространстве угроз. Пространство угроз охватывает объект защиты — персонал предприятия, имущество, финансовые средства, сведения, составляющие коммерческую тайну. Каждая угроза влечет за собой определенный ущерб — моральный или материальный, а противодействие призвано снизить его величину. Исходя из этого при создании системы экономической безопасности, необходимо опираться на такой инструмент как правовая база.

Правовой базой для создания СБ является Закон РФ «О частной детективной и охранной деятельности в Российской Федерации» от 11 марта 1992 г. № 2487-1, которым предусматривается, что предприятия,

расположенные на территории Российской Федерации, независимо от их организационно-правовых форм, вправе учреждать обособленные подразделения — службы безопасности для осуществления охранно – сыскной деятельности в интересах собственной безопасности.

Служба безопасности предприятия может выполнять следующие функции:

1) сбор сведений по гражданским делам на договорной основе с участниками процесса;

2) изучение рынка, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;

3) установление обстоятельств неправомерного использования в предпринимательской деятельности фирменных знаков и наименований, недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;

4) выяснение биографических и других характеризующих личность данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых договоров;

5) поиск без вести пропавших граждан;

6) поиск утраченного гражданами или предприятиями, учреждениями, организациями имущества;

7) сбор сведений по уголовным делам на договорной основе с участниками процесса;

8) защита жизни и здоровья граждан;

9) охрана имущества собственников, в том числе при его транспортировке;

10) проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации;

11) консультирование и подготовка рекомендаций клиентам по вопросам правомерной защиты от противоправных посягательств;

12) вооруженная охрана имущества собственников, а также использование технических и иных средств, не причиняющих вреда жизни и здоровью граждан, и окружающей среде, средства оперативной радио- и телефонной связи [13, 16].

Для обеспечения защиты экономической безопасности предпринимательской деятельности важное значение имеет создание собственной службы экономической безопасности (далее – СЭБ), которая будет в свою очередь также являться одним из инструментов обеспечения экономической безопасности на предприятии. Можно рекомендовать ряд этапов при создании СЭБ:

1) Принятие решения о необходимости создания СЭБ. Вопрос о создании системы экономической безопасности должен возникать в момент принятия решения об организации предприятия в зависимости от выбираемого им вида деятельности, объема предполагаемой к производству продукции, размера годового оборота и прибыли, использования секретов производства, количества работников и т.п. Учредители должны заранее предусмотреть необходимость создания системы экономической безопасности.

2) После государственной регистрации руководителями принимается окончательное решение о создании СЭБ. В случае положительного решения вопроса определяется ответственное лицо (группа лиц), которое будет непосредственно заниматься организацией СЭБ.

3) Определение общих задач СЭБ — предупреждение угроз, реагирование на возникшие угрозы и определение конкретных объектов защиты (персонал, информация, компьютерные системы, здания и помещения).

4) Разработка положения о СЭБ, определение структуры и утверждение штатов.

5) Набор кадров. Работниками СЭБ могут быть люди, специально и постоянно занимающиеся данной деятельностью как основной, и привлеченные специалисты (например, главный бухгалтер, юрист и пр.).

6) Непосредственная организация и функционирование СЭБ.

7) При подборе постоянных работников важнейшим требованием является профессиональная подготовка. В связи с этим предпочтение следует отдавать бывшим работникам правоохранительных органов (МВД, ФСБ, прокуратуры, налоговой полиции), имеющим опыт работы и подходящим по морально –деловым качествам для данной деятельности. Для службы физической защиты целесообразнее приглашать лиц, проходивших службу в спецназе, СОБРе, ОМОНе, которые обладают профессиональными навыками владения оружием и рукопашного боя.

Таким образом, подводя общий итог, касающейся инструментов, обеспечивающих экономическую безопасность, можно сказать что система обеспечения экономической безопасности, должна строиться на следующих принципах:

- комплексности и системности;
- своевременности;
- законности;
- плавности;
- взаимодействия;
- компетентности;
- сочетания гласности и конфиденциальности;
- эффективной защиты.

Инструменты обеспечения экономической безопасности предприятия должны охватывать, по нашему мнению, все принципы, представленные выше. Исходя из этих принципов, можно выделить инструменты экономической безопасности, которые квалифицируются следующим образом:

- управление рисками (диверсификация, страхование, хеджирование и др.;
- техническая защита (охрана, безопасность информации, кадровая политика);

– финансовая защита (финансовый мониторинг, управленческий учет и контроль, бюджетирование).

На основе данных принципов и инструментов обеспечения экономической безопасности предприятия, можно проанализировать соответствие уже существующих инструментов теоретически обоснованным принципам. Исходя из того, какие угрозы предприятие выделяет как наиболее важные, выбираются соответствующие инструменты обеспечения безопасности. По нашему мнению, использовать инструменты, охватывающие только один или несколько принципов, нецелесообразно [21].

1.4 Критерии оценки эффективности системы экономической безопасности

Основополагающим элементом при исследовании экономической безопасности предприятия является выбор ее критерия. Он предполагает признак или сумму признаков, на основании которых делается заключение о состоянии экономической безопасности предприятия.

Экономическую безопасность предприятия можно оценивать с помощью различных критериев:

1) Организационная сторона – в этом случае предполагается сохранение как самого предприятия, так и ее организационной целостности, нормальное функционирование основных подразделений (отделов, служб и т.п.). Основные подразделения фирмы (например, отдел снабжения, производственный отдел, финансовый отдел или бухгалтерия, служба маркетинга) выполняют все свои функции для достижения основной цели предприятия.

2) Правовая сторона – имеется в виду постоянное обеспечение соответствия деятельности фирмы действующему законодательству, что выражается в отсутствии претензий со стороны правоохранительных органов (или контрагентов) к фирме. Кроме того, отсутствуют потери от сделок с

внешними партнерами вследствие нарушения последними законодательства (умышленно либо неумышленно). Это обеспечивается юридической экспертизой всех осуществляемых операций и сделок, заключаемых договоров.

3) Информационная сторона – безопасность может быть оценена как сохранение состояния защищенности внутренней конфиденциальной информации от утечки или разглашения в различных формах.

4) Экономическая сторона – проявляется в стабильных или имеющих тенденцию к росту основных финансово-экономических показателях деятельности фирмы (таких как собственный капитал, объем годового оборота, прибыль, рентабельность). В них отражаются общие результаты обеспечения безопасности с организационной, правовой, информационной и собственно экономической сторон. Сюда могут входить такие показатели, как отсутствие штрафов, санкций со стороны государственных органов за нарушение законодательства (например, налогового, антимонопольного), отсутствие потерь от сделок с недобросовестными контрагентами [12].

Как можно заметить, критерии оценки экономической безопасности предприятия по своей специфики носят обобщённый характер, более того, большинство предприятий для оценки своей экономической безопасности чаще всего используют так называемый метод сравнения показателей.

Данный метод основан на анализе и сравнении общих показателей по результатам хозяйственной деятельности предприятия, на начало и конец года. После чего руководство предприятия само определяет степень важности и опасности от потерь, если такие имели место быть.

В России в настоящее время действует более 50 законов, регулирующих проблемы безопасности, но ни в одном из них не определена количественная оценка безопасности.

Но для более точной, количественной оценки, на сегодняшний день используется метод основанный на оценке эффективности деятельности структурных подразделений на основе соотношения бюджетов по предотвращению негативных воздействий и данных по предотвращенным и

реализовавшимся ущербам дает объективную картину эффективности деятельности всех структурных подразделений предприятия с позиций обеспечения функциональных составляющих экономической безопасности предприятия. Под функциональной составляющей экономической безопасности предприятия понимается совокупность процессов, которые составляют единую группу с точки зрения их функциональной роли в обеспечении экономической безопасности, иными словами анализируются функции различных подразделений в системе экономической безопасности предприятия [28].

Основными функциональными составляющими экономической безопасности предприятия являются:

1) Финансовая составляющая. Об ослаблении финансовой безопасности свидетельствуют:

- снижение ликвидности;
- повышение кредиторской и дебиторской задолженности;
- снижение финансовой устойчивости и т. п.

За данную составляющую экономической безопасности отвечают финансовые и экономические службы предприятия.

Оценка финансовой составляющей экономической безопасности может быть выполнена на основе многофакторной модели Э. Альтмана [4].

$$Z = 1{,}2 \times Коб + 1{,}4 \times Кнп + 3{,}3 \times Кр + 0{,}6 \times Кп + 1{,}0 \times Кот$$

где Коб — доля чистых оборотных средств в активах (отношение текущих активов за вычетом текущих обязательств к общей сумме актива); Кнп- рентабельность активов, исчисленная по нераспределенной прибыли; Кр - рентабельность активов, исчисленная по балансовой прибыли; Кп - коэффициент покрытия по рыночной стоимости собственного капитала (отношение рыночной стоимости обыкновенных и привилегированных акций к объему заемных средств по балансу); Кот - отдача всех активов (отношение чистой выручки от реализации к объему активов). В зависимости от величины Z можно прогнозировать вероятность банкротства предприятия:

Z <1,8 - очень высокая;

1,8<Z <2,7 - высокая;

2,8 ≤ Z≤ 2,9 - небольшая;

Z ≥ 3 - очень низкая.

Большую достоверность оценки финансовой безопасности может обеспечить подход, который позволяет определить степень финансовой устойчивости и соответственно степень финансовой безопасности предприятия.

Предполагается использование следующих показателей:

±Ec — излишек (+) или недостаток (-) собственных оборотных средств, необходимых для формирования запасов и покрытия затрат, связанных с хозяйственной деятельностью предприятия;

±Em— излишек или недостаток собственных оборотных средств, а также среднесрочных и долгосрочных кредитов и займов;

±En - излишек или недостаток общей величины оборотных средств.

2) Интеллектуальная составляющая. Негативное влияние на данную составляющую оказывают:

– уход ведущих высококвалифицированных работников, что приводит к ослаблению интеллектуального потенциала предприятия;

– снижение удельного веса инженерно-технических и научных работников в общем количестве работающих;

– снижение изобретательской и рационализаторской активности;

– снижение образовательного уровня работников, особенно лиц аппарата управления.

За данную составляющую безопасности должна отвечать кадровая служба (отдел кадров) и лично главный инженер. Уровень интеллектуальной составляющей экономической безопасности может быть определен следующим образом:

– текучесть работников высокой квалификации (отношение количества уволившихся работников к общему количеству работников данной квалификации);

– удельный вес инженерно-технических и научных работников (отношение их количества ко всему количеству работающих);

– показатель изобретательской (рационализаторской) активности (отношение количества изобретений (рацпредложений) к количеству работающих или инженерно - технических работников);

– показатель образовательного уровня (отношение количества лиц, имеющих высшее (специальное) образование в соответствии с профилем деятельности предприятия к общему количеству работающих) и т.п.

Эти и иные аналогичные показатели (коэффициенты) сравнивают с показателями других предприятий или анализируют в динамике (естественно, при этом учитывают экономические показатели деятельности анализируемого и сравниваемых предприятий).

Вначале значения всех показателей сводят в интегральный, используя следующую формулу (известный в математике метод расстояний) [27, 28]:

$$\Пи = \sum_{i=1}^{n} (1 - \delta i) * Bi$$

где n - количество показателей; Bi - вес итого показателя; δi - относительная оценка i-го показателя;

Величина δi рассчитывается по следующим правилам:

δi = Пi/Пmax, если предпочтительнее большее значение показателя;

δi = Пmin/Пi, если предпочтительнее меньшее значение показателя,

где Пi - значение i-го показателя; Пmin - наименьшее значение показателя (коэффициента) из всего количества сравниваемых предприятий (или завесь анализируемый период, если имеются данные, характеризующие в динамике только одно предприятие); Птах -наибольшее значение показателя (коэффициента) из всего количества сравниваемых предприятий (или за весь анализируемый период, если имеются данные, характеризующие в динамике только одно предприятие).

Аналогичные расчеты выполняют для всех сравниваемых предприятий (периодов времени). Далее выводят средние значения интегрального показателя (Пucp) для отрасли (рынка) или же для конкретного предприятия за ряд лет.

Если значение Пu, рассчитанное для анализируемого предприятия, меньше Пucp, то это свидетельствует об уровне интеллектуальной безопасности выше среднего. Если Пu> Пucp, то уровень безопасности ниже среднего. Значения Пu, попадающие в указанный выше интервал, свидетельствуют о среднем уровне безопасности.

3) Кадровая составляющая. К основным негативным влияниям относят:

- отток кадров;
- текучесть кадров;
- физическое старение кадров, старение их знаний и квалификации;
- низкую квалификацию кадров;
- совмещение основной деятельности с работой в других организациях, что сопряжено как с низкой отдачей работника, так и с возможным выходом конфиденциальной информации за пределы предприятия.

За данную составляющую безопасности должна отвечать кадровая служба (отдел кадров).

Расчет уровня безопасности для кадровой составляющей выполняют аналогично изложенному выше, внеся изменения в состав показателей. В ряде случаев показатели интеллектуальной и кадровой составляющей экономической безопасности предприятия объединяют.

4) Технологическая составляющая. К основным негативным влияниям относят:

- действия, направленные на подрыв технологического потенциала предприятия;
- нарушение технологической дисциплины;

– моральное старение используемых технологий.

Противодействием должна заниматься технологическая служба (контроль технологической дисциплины, совершенствование существующих и разработка новых эффективных технологий и т.п.).

Показатели уровня технологической безопасности могут быть рассчитаны аналогично двум предшествующим составляющим, однако состав показателей будет другим. Так, например, следует использовать следующие показатели, которые характеризуют технологический потенциал и технологическую безопасность предприятия (естественно, с учетом экономических результатов их деятельности):

– уровень прогрессивности технологий, рассчитываемый как отношение количества используемых прогрессивных современных технологий (на уровне лучших среди предприятий, работающих на конкретном рынке) к общему их количеству на предприятии;

– уровень прогрессивности продукции, рассчитываемый как отношение количества наименований, производимых новых прогрессивных видов продукции (на уровне лучших образцов среди предприятий, работающих на конкретном рынке) к общему их количеству;

– уровень технологического потенциала, рассчитываемый как доля технических и технологических решений на уровне изобретений в общем количестве новых решений, используемых в производственном процессе и т.д.

5) Правовая составляющая. Основными угрозами безопасности являются:

– недостаточная правовая защищенность интересов предприятия в договорной и прочей деловой документации;

– нарушение юридических прав предприятия и его работников;

– умышленное или неумышленное разглашение коммерчески важных сведений;

– нарушение норм патентного права [27, 26, 28].

Противодействием должна заниматься юридическая и патентно-лицензионная служба.

Уровень правовой безопасности может быть определен в зависимости от соотношения потерь, понесенных предприятием, вследствие нарушения правовых норм (например, выплаты по искам из-за нарушения юридических норм и прав), и общего размера предотвращенных потерь. Для оценки может быть предложена следующая шкала:

потерь нет - абсолютная правовая безопасность;

доля правовых потерь от 0 до 25% - нормальная правовая безопасность;

25% - 50% - нестабильное состояние;

50% - 75% - критическое состояние;

75% - 100% - кризисное состояние.

1.5 Результат работы системы экономической безопасности

Результатом работы системы экономической безопасности будут также являться критерии, которые руководство предприятия определяет для себя исходя из деятельности своего предприятия, которая в свою очередь зависит от ряда факторов, таких как отрасль, масштаб предприятия, сфера деятельности и многие другие.

Но общем результатом работы системы экономической безопасности для любого предприятия является создание и поддержание условий устойчивого функционирования предприятия как в макро-, так и в микросреде.

Основной смысл системы экономической безопасности состоит в том, что она должна носить упреждающий характер, а основными критериями оценки ее надежности и эффективности являются:

– обеспечение стабильной работы предприятия, сохранности и приумножения финансов и материальных ценностей;

– предупреждение кризисных ситуаций, в том числе различных чрезвычайных происшествий, связанных с деятельностью «внешних» и / или «внутренних» недоброжелателей.

Также для большинства предприятий результатом эффективного функционирования системы экономической безопасности является минимальное или отсутствие расхождения заявленных и фактических критериев по итогам отчетного периода.

2 Анализ ситуации на предприятиях-объектах исследования

2.1 Общие сведения об объектах исследования

2.1.1 Акционерное общество «ИМПЕРА»

В январе 1964 г. приказом № 2 Президиума Госкомитета по электронной технике СССР было открыто акционерное общество «ИМПЕРА» (далее АО «ИМПЕРА»).

Предпосылками создания АО «ИМПЕРА» именно явились существовавшая школа специалистов по материаловедению на кафедрах университета и в лабораториях физико-технического института, новые оригинальные результаты научно-исследовательских работ по выращиванию и изучению свойств материалов под руководством профессора В.А. Преснова, наличие в городе высокопрофессиональных кадров и возможности подготовки новых молодых специалистов-физиков. Директором института и его научным руководителем был назначен Виктор Алексеевич Преснов. Именно с его непосредственным участием связано зарождение и развитие на предприятии всех научных и приборных направлений. Перед АО «ИМПЕРА» были поставлены задачи разработки технологии выращивания арсенида галлия, изучения его свойств и создания новых классов приборов на его основе.

В АО «ИМПЕРА» были разработаны процессы получения эпитаксиальных структур широкой номенклатуры для СВЧ изделий (диодов Ганна, смесительных, умножительных, детекторных, импульсных диодов и др.), оптоэлектронных диодов ИК диапазона, интегральных схем. Большинство изделий, которые выпускались и выпускаются сегодня на заводе АО «ИМПЕРА», обеспечивались эпитаксиальными структурами, созданными в отделе материаловедения.

Прекрасно понимая, что комплексное развитие нового направления в отечественной электронике возможно только при наличии замкнутого цикла: исследование – разработка – выпуск разработанных изделий, Виктор

Алексеевич сумел убедить в этом Министерство электронной промышленности.

Главными направлениями разработок были:

1) изделия СВЧ электроники, (смесительные, детекторные, настроечные диоды с барьером Шоттки мм диапазона и монолитные интегральные схемы);

2) приборы на эффекте Ганна;

3) светодиоды и оптоэлектронные приборы.

2.1.2 Акционерное общество «КРОНИКА»

В 1991 году команда из семи человек создали предприятие на базе научной лаборатории.

За двадцать с лишним лет из коллектива в восемь человек компания выросла в одного из лидеров по производству радиоэлектронной аппаратуры в России.

АО «КРОНИКА» специализируется на производстве телекоммуникационного оборудования, контрольно-измерительной аппаратуры СВЧ и аксессуаров СВЧ тракта, СВЧ электроники, радаров для навигации и обеспечения безопасности.

Главное конкурентное преимущество компании — полный производственный цикл с собственной разработкой и производством продукции, начиная от электронной компонентной базы СВЧ и заканчивая серийными изделиями. АО «КРОНИКА» оперативно реагирует на потребности рынка, внедряет инновационные разработки, контролирует процесс создания технологии и передачи ее в производство, отслеживает качество выпускаемых изделий.

Сейчас у АО «КРОНИКА» более 1000 клиентов в России и за ее пределами, а география заказов распространяется от СНГ до стран Азии и Африки. Также офисы продаж АО «КРОНИКА» располагаются в Италии,

Бразилии, Вьетнаме и Южной Африке. В коллективе АО «КРОНИКА» более 30% - это разработчики, которые, благодаря своему таланту и профессионализму, каждый день предлагают новые инновационные решения в области радиоэлектроники.

Компания по праву занимает место одного из лучших инновационных предприятий в стране, является двукратным лауреатом национального рейтинга высокотехнологичных быстроразвивающихся компаний и победителем в номинации «Лучшее инновационное предприятие». С 2007 года продукция АО «КРОНИКА» входит в список «100 лучших товаров России».

Сегодня АО «КРОНИКА» располагается на 28 тысячах квадратных метров и насчитывает более 1500 сотрудников. Компания плотно сотрудничает с кафедрами и факультетами ведущих вузов России. В 2015 году АО «КРОНИКА» создали научно-образовательный центр «Радиоэлектроника СВЧ», который будет обеспечивать мировой уровень образовательной и научной деятельности в области разработки и создания перспективных образцов радиоэлектронной аппаратуры для систем радиолокации и радиовидения.

2.2 Структуры и механизмы, отвечающие за экономическую безопасность

Механизм обеспечения экономической безопасности предприятия необходим для создания условий, обеспечивающих эффективную деятельность всех элементов предприятия, а также высокую степень согласованности. Механизм должен обеспечивать экономическую безопасность на входе и выходе производственной системы, создавать надежные условия функционирования управляющей и управляемой систем. В механизм экономической безопасности предприятия входят следующие составляющие:

– Базовые принципы экономической безопасности предприятия;

– Функции, реализуемые процесс управления экономической безопасностью;

– Ресурсы;

– Цели обеспечения экономической безопасности функционирования предприятия.

Вышеперечисленные составляющие образуют структуру механизма обеспечения экономической безопасности функционирования предприятия.

Исходя из приоритетности структурного элемента, которое определяется внутренним регламентом предприятия, распределяются ресурсы на поддержку какого-либо элемента. Как правило приоритетность определяется исходя из анализа рисков, ресурсы распределяются пропорционально потерям от возможной экономической угрозы. Структурные элементы для каждого предприятия строго индивидуальны.

Рассмотрим стандартную структуру обеспечения экономической безопасности. На данном предприятии экономическая безопасность состоит из пяти элементов, таких как:

1) Организационно – правовая;
2) Физическая охрана;
3) Инженерно – техническая защита;
4) Криптография;
5) Информационный контроль.

Организационно – правовое направление разработки комплексной системы безопасности на предприятии, как это видно из названия, включает два этапа, такие как:

1) Правовое;
2) Организационное.

Правовое направление включает создание нормативно правовых актов на федеральном уровне, которые четко описывают, направление деятельности, иерархию структурных подразделений, призванных обеспечивать

экономическую безопасность предприятия, объекты и субъекты воздействия, а также критерии, по которым будет осуществляться контроль и многое другое.

Организационное направление, в какой-то мере дублирует правовое, разница заключается в том, что организационное направление создаёт саму систему контроля в виде нормативно правовых актов представленных как перечень мер и должностных инструкции внутри самого предприятия, но при создании системы и инструкций для внутреннего пользования, за основу берется именно правовая база, так как внутренние законы предприятия по обеспечению экономической безопасности не должны идти в разрез с федеральными нормами, в противном случае предприятие не находится под защитой государства.

Физическая охрана предприятия представляет собой комплекс мер, направленных на обеспечение именно физической безопасности функционирования предприятия, сохранность его материального имущества, а также защиту жизни и здоровья его сотрудников.

Физическая охрана предприятия нацелена на проведение проверок на предмет выявления рисков, угроз и возможных путей их предотвращения, а также продумывание системы, являющейся наиболее эффективной и рациональной для обеспечения безопасности.

Физическая охрана осуществляется при помощи непосредственного присутствия сотрудников охраны, задачами которых являются:

- Контроль пропускного режима;
- Досмотр автотранспорта;
- Предотвращение краж и хищений;
- Обход непосредственного объекта и прилегающей к нему территории;
- Контролинг системы видеонаблюдения;
- Контроль действий посетителей и сотрудников предприятия;
- Предотвращение несанкционированного доступа;

– Принятие первичных мер по устранению технических аварий и возгораний;

– Охрана материальных ценностей, находящихся в свободном доступе.

Физическая охрана регламентируется организационными нормативно – правовыми актами, полный комплект которых, подготавливает предприятие исходя из наиболее рационального и эффективного, по его мнению, обеспечению физической охраны.

Инженерно – техническая защита (далее ИТЗ) предприятия представляет собой совокупность взаимосвязанных технических и инженерных средств, обеспечивающих безопасное функционирование предприятия, сохранность имущества, информации, здоровья и жизни персонала и посетителей и предоставляющих оперативному персоналу необходимую информацию о состоянии безопасности объекта, позволяющую оперативно принимать меры по предотвращению нештатных ситуаций и ликвидации их последствий.

В состав ИТЗ, в зависимости от требований по безопасности предприятия, предъявляемых нормативно-техническими документами, которые формируются сотрудниками инженерной безопасности, могут входить те или иные подсистемы безопасности.

Наиболее полный перечень средств ИТЗ представлен в следующем виде:

– Пожарная сигнализации;
– Автоматическое пожаротушение;
– Речевое оповещение;
– Охранно –тревожная сигнализация;
– Контроль доступа (СКУД);
– Охранное видеонаблюдение;
– Оперативная и диспетчерская связь;
– Система сбора и обработки информации;

– Структурированная кабельная сеть;

– Средства технической укрепленности и др.

Системы управления доступом позволяют ограничить доступ на объект определенным кругом лиц и выявлять случаи несанкционированного проникновения. В их задачу входит управление преграждающими устройствами (например, турникетами или дверьми).

Охранно – пожарная сигнализация предназначена для оповещения о возникновении возгорания и несанкционированном проникновении на объект. Различные датчики (движения, дыма, акустические, тепловые, вибрационные и контактные) передают информацию на контрольное устройство, и система оповещает людей о возникновении внештатной ситуации.

Системы видеонаблюдения используются для защиты от краж и контроля за деятельностью сотрудников. Цифровые системы позволяют наблюдать ситуацию на объекте в режиме реального времени.

Все средства, предназначенные для обеспечения инженерно – технической защиты, в обязательном порядке должны быть сертифицированы и включены в реестр сертифицированных средств инженерно – технической защиты и соответствовать требованиям качества ИСО 9001-94.

Криптография – это преобразования исходного текста на основе алгоритма в шифрованный текст. Современная криптография содержит в себе такие элементы, как асимметричные криптосистемы, системы электронной цифровой подписи, хеш – функции, управление ключами, получение скрытой информации, квантовую криптографию.

Задачами криптографии являются защита в виде шифрования внутренних и внешних каналов связи, а также защита систем хранения файлов, составляющих коммерческую тайну и файлов, являющихся носителями финансового состояния предприятия, а также информацию о сотрудниках предприятия.

Резервное копирование информации, находящейся в электронном виде и подлежащей криптографическому шифрованию, необходимо создать

физическое архивирование, охрану и доступ, к которому будет обеспечивать физическая охрана.

Также немаловажным аспектом экономической безопасности предприятия является защита информации, которая является главным нематериальным активом предприятия, так как может быть использована во благо или для нарушения деятельности предприятия, если произойдет утечка и важная информация попадет лицам, заинтересованным в подрыве производственной деятельности предприятия (конкурентам).

К информации, подлежащей особому контролю со стороны руководства обычно относят:

- Информацию, составляющую коммерческую тайну;
- Информацию о цене государственного и гражданского контрактов;
- Внутренний реестр сертифицированных компаний поставщиков;
- Техническую документацию;
- Информацию, содержащую личные данные сотрудников;
- Информацию, содержащую закупочные цены.

Как показывает практика, случается так, что сами сотрудники, несознательно или сознательно, разглашают «секретную» информацию, в основном это происходит за счет внешних и внутренних источников общения (электронная почта, различные мессенджеры). И как было описано выше встречаются случаи использования своего служебного положения рядовыми сотрудниками такой вид дестабилизации предприятия реализуется через раскрытие, локальной, но не менее важной, информации конкурентам.

Для предотвращения такого рода провокаций вводят информационный контроль, его суть состоит в том, что сотрудники службы безопасности предприятия снимают копии всех писем, отправленных с рабочего компьютера сотрудника и проводят анализ на «ключевые слова».

Но данная работа является довольно трудоемкой и занимает много времени, основным решением данной проблемы можно предложить автоматизировать данный процесс.

Для автоматизации информационного контроля была интегрирована так называемая система «защиты от потери информации». Данная система представляет собой пакет технологий, призванных предотвращать утечки конфиденциальной информации из информационной базы предприятия, а также включает в себя технические устройства (программные или программно – аппаратные) для такого предотвращения утечек.

Система строится на анализе потоков данных, обращающихся на внутренних информационных каналах предприятия и пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Главной задачей системы является предотвращение передачи конфиденциальной информации за пределы информационной системы предприятия. Такая передача (утечка) может быть намеренной или ненамеренной.

К основным задачам системы относятся:

– Архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;

– Предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, эротики, излишних объёмов данных и т.п.);

– Предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;

– Предотвращение использования работниками казённых информационных ресурсов в личных целях;

– Предотвращение использования работниками несанкционированных съемных носителей информации;

– Оптимизация загрузки каналов, экономия трафика;

– Контроль присутствия работников на рабочем месте.

Продукты автоматизированного анализа проходящей информации, уже давно существуют на рынке экономической безопасности основными производителями таких технологий являются такие компании как: InfoWatch, Zecurion, МФТИГАРДА.

Таким образом, в теории система обеспечения экономической безопасности должна быть тесно интегрирована в структуру безопасности предприятия, наряду с физической защитой и другими её элементами.

Однако на практике, современные тенденции развития бизнеса показывают, что определенной структуры с прописанными нормами, правилами и функциями на современных предприятиях нет. Более того современные предприятия зачастую неспособны дать четкого определения понятия «экономическая безопасность».

С точки зрения организации процесса обеспечения экономической безопасности, малые предприятия предпочитают простой информационный мониторинг, выражающейся в годовой бухгалтерской отчетности, передаваемой в налоговые органы для проверки, также, как показывает практика, малые предприятия практикуют делегирование полномочий, чаще данные полномочия передают бухгалтерам, бухгалтера совмещают как основную свою работу, связанную с ведением финансовой отчетности предприятия, так и отслеживают подозрительные, по их мнению, финансовые операции связанные с заключением контрактов и не только.

Для высокотехнологичных или крупных предприятий экономическая безопасность играет огромную роль, так как по сравнению с малыми предприятиями потери от каких-либо экономических угроз у крупных предприятий будут намного больше и исчисляются десятками миллионов рублей. Однако, как уже было сказано выше определенной структуры экономической безопасности на предприятиях нет, данный принцип не является исключением и для крупных предприятий.

Исходя из этого высокотехнологичные или крупные предприятия формируют индивидуальный алгоритм модели экономической безопасности

для предотвращения, минимизации внешних и внутренних угроз экономическому состоянию предприятия, в том числе его финансовым, материальным, информационным, кадровым ресурсам. Как правило алгоритм модели экономической безопасности основывается на сотрудничестве нескольких, порой не взаимосвязанных, структурных подразделений, отделов внутри предприятия.

Для примера рассмотрим и сравним структуры, отвечающие за экономическую безопасность на примере компании АО «КРОНИКА» и АО «ИМПЕРА».

2.3 Структуры и механизмы, отвечающие за экономическую безопасность, в АО «КРОНИКА»

Основными структурными подразделениями, участвующими в обеспечение экономической безопасности на АО «КРОНИКА», являются:

1) Департамент безопасности
2) Отдел материально технического обеспечения (ОМТО)
3) Отдел информационных технологий (ИТ)

Отдел материально технического обеспечения (далее ОМТО) занимается поиском поставщиков комплектующих, необходимых для производства основной продукции компании, а также заключает договора на поставку необходимых комплектующих, на взаимовыгодных условиях, ОМТО имеет право заключать сделки с поставщиками на сумму, не превышающую десяти миллионов рублей, в противном случае, для заключения сделки необходимо разрешение совета директоров.

Отдел информационных технологий (далее ИТ) занимается поддержкой и развитием ИТ-инфраструктуры предприятия.

Выделены несколько областей работы:

- поддержка внешних и внутренних серверов компании;
- системное администрирование;

– поддержка пользователей;

– осуществление контроля внутренних электронных каналов связи.

Специалисты ИТ отдела отвечают за системы защиты информации в компании, защиту сети от взлома и вирусов. Проверяют уязвимость инфраструктуры и сокращают риски. А также следят за утечкой информации, участвуют в разработке систем защиты и обеспечивают информационную безопасность, а именно следят за сохранением корпоративных сведений и важной коммерческой информации, т. е. конфиденциальностью.

Департамент безопасности, является основным из структур, описанных выше, так как аккумулирует всю необходимую информацию для обеспечения экономической безопасности при взаимодействии с различными отделами предприятия. Департамент безопасности не является чем –то обособленным, так как имеет свою собственную структуру, которая состоит из следующих обособленных субъектов, таких как:

– Отдел DLP (Data Leak Prevention);

– Отдел экономической безопасности;

– Отдел общей безопасности.

Рассмотрим функционал данных отделов более подробно.

Отдел DLP осуществляет сбор и изучение информации, которая поступает из разных отделов, на предмет выявления и предупреждения возможных угроз, связанных с экономической безопасностью. Основной задачей отдела DLP является защита информации, которая составляет коммерческую тайну, а также мониторинг трафика активности каналов корпоративной связи и поиском, и выявлением потенциальных неблагонадежных сотрудников путем проверки вручную и с помощью поисковых программ корпоративной почты сотрудников и иных известных каналов связи.

Отдел экономической безопасности осуществляет деятельность, связанную с экономической обоснованностью цен, заключаемых контрактов, а

также проверкой контрагентов, которые принимают на себя обязательства по контрактам.

Отдел общей безопасности осуществляет общую безопасность, деятельностью которой является разработка и введение нормативно – правовых актов и регламентов, регулирующих деятельность сотрудников и контроль за их исполнением. Более того в обязанности отдела общей безопасности входит осуществление физической охраны наиболее значимых объектов предприятия, а именно контроль пропускного режима, досмотр автотранспорта, предотвращение открытых краж и хищений со стороны рядовых сотрудников и так далее.

Таким образом формируется механизм, представляющий собой целостную систему, которая в свою очередь, состоит из отдельных, самостоятельных, но одновременно взаимосвязанных структурных элементов. Для удобства восприятия, мы объединили все выше сказанное в схему.

»

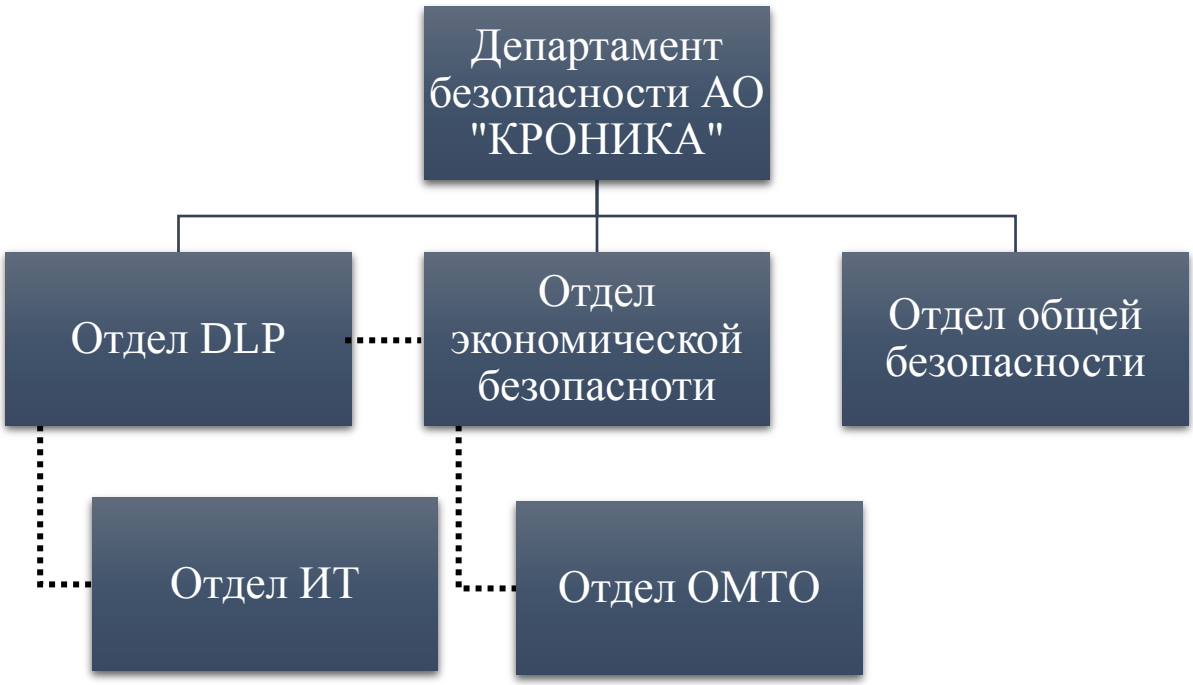


Рисунок 6 – Структура экономической безопасности на АО «КРОНИКА»

2.4 Структуры и механизмы, отвечающие за экономическую безопасность, в АО «ИМПЕРА»

Теперь рассмотрим структуру экономической безопасности на АО «ИМПЕРА»

Структура экономической безопасности на АО «ИМПЕРА» состоит из нескольких обособленных подразделений, которые тесно взаимодействуют друг с другом, создавая единый механизм. В структуру экономической безопасности на АО «ИМПЕРА» входят такие подразделения как:

1) Отдел управления закупками (далее ОУЗ)
2) Отдел материально технического обеспечения (далее ОМТО)
3) Планово – экономический отдел (далее ПЭО)
4) Закупочная комиссия

Отдел ОУЗ осуществляет подготовку, размещение документов на закупки исходя из плана – графика закупочной деятельности предприятия, а также проводит сбор заявок на участие и контроль за соблюдением правил в соответствие с законодательством о закупочной деятельности.

Отдел ОМТО осуществляет поиск необходимых товаров и комплектующих для производственной деятельности предприятия, а также осуществляет определение начальной (максимальной) цены заключаемых контрактов и проверку обоснованности цены заключаемого контракта.

Отдел ПЭО по своему функциональному предназначению похож на отдел ОМТО, более того данные отделы довольно тесно сотрудничают. Обязанностями отдела ПЭО является разработка плана – графика закупочной деятельности предприятия и расчет необходимых объемов поставок для непрерывной работы предприятия в долгосрочной перспективе.

Закупочная комиссия, осуществляет проверку контрагентов фирм, выигравших закупочный конкурс, исходя из информации, представленной отделами, описанными выше.

Для удобства восприятия, мы объединили все выше сказанное в схему.

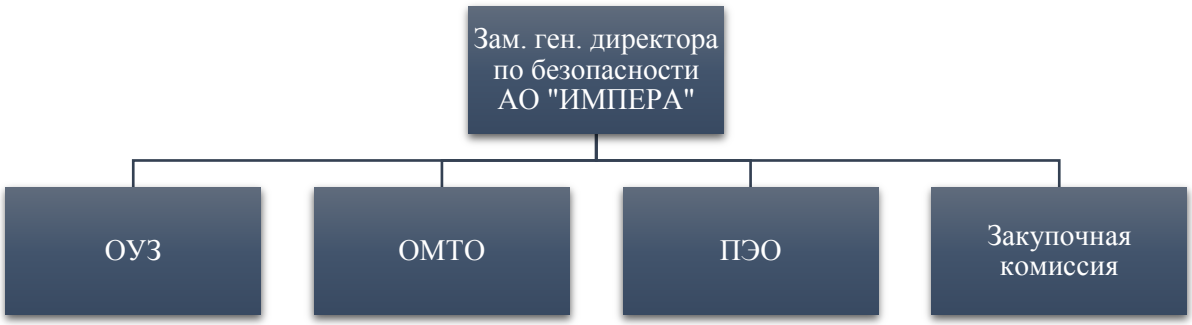


Рисунок 7 – Структура экономической безопасности на АО «ИМПЕРА»

Таким образом, подводя итог можно сказать, что на данных предприятиях присутствуют абсолютно разные структуры, призванные осуществлять экономическую безопасность, а также защиту от внутрикорпоративного мошенничества. Кроме этого, в структурах обеих организаций функции экономической безопасности тесно связаны с общей безопасностью. С одной стороны, это позволяет работать с проблемами безопасности комплексно. С другой, создает проблемы в четком определении функций отделов, которые работают непосредственно с вопросами экономической безопасности. В результате, четко не определен функционал данных департаментов и отделов, и не всегда понятно, чем конкретно они должны заниматься и какой функционал на них возлагается. Одной из важнейших проблем в этой сфере является кадровая проблема. В структурах, которые отвечают за экономическую безопасность предприятия, катастрофически не хватает квалифицированных специалистов, способных анализировать риски и угрозы в области экономической безопасности предприятия, своевременно выявлять их и оперативно реагировать. Эти сотрудники должны обладать компетенциями в экономической и юридической сфере, отличными навыками системного анализа и мышления.

2.5 Основные угрозы на предприятиях – объектах исследования

При выявлении основных проблем, связанных с экономической безопасностью на высокотехнологичных предприятиях, были проанализированы объекты исследования, в нашем случае это предприятия АО «КРОНИКА» и АО «ИМПЕРА».

Во-первых, необходимо отметить что АО «КРОНИКА» является частной компанией, а АО «ИМПЕРА» государственным предприятием, в рамках данных организаций была проанализирована уголовная практика, связанная с внутрикорпоративным мошенничеством в компаниях. Также были проанализированы таблицы рисков для данных предприятий, которые были сформулированы сотрудниками планово-финансовых отделов и служб безопасности. Кроме того, проводились устные интервью с начальниками отделов экономической безопасности, после чего были сделаны следующие выводы об основных угрозах.

Предприятие АО «КРОНИКА» имеет достаточно гибкую систему контроля и борьбы с различного вида угрозами как внешними, так и внутренними. Данная система представлена в виде мероприятий, нацеленных на выявление и ликвидацию разного рода угроз. Основу такой системы контроля составляет полная «прозрачность» действий. К основным угрозам, связанным с экономической безопасностью на АО «КРОНИКА» относятся:

1) Недобросовестные действия конкурентов.

К данной угрозе относится переманивание сотрудников, а также один из вариантов производственного шпионажа, внедрение своих сотрудников на предприятие.

Переманивание сотрудника невозможно осуществить через архивные базы данных внутри предприятия, так как все данные архива относятся к коммерческой тайне и доступ к ним имеют только определенные люди. Поэтому конкуренты действуют через базы высших учебных заведений (ВУЗов), проводя анализ тем дипломных работ, после чего конкуренты находят

автора работы и используя в основном инструменты «лучших условий работы», которые включают материальные, социальные и другие факторы, переманивают сотрудника на свое предприятие.

Данную проблему нельзя недооценивать, так как, при исполнении конкурентами всех вышеописанных действий, происходит так называемая «утечка мозгов», в связи с чем предприятие может нести колоссальные финансовые убытки.

2) Недобросовестные действия сотрудников предприятия и поставщиков.

Данная угроза представляет собой использование сотрудниками, в большинстве случаев это руководители обеспечивающих отделов, своего служебного положения для своей выгоды, но встречаются случаи использования своего служебного положения рядовыми сотрудниками.

Данную проблему довольно сложно подвергнуть строгому контроль, так как здесь основополагающим фактором является человеческий и психологический фактор.

Основным инструментом использования служебного положения является торговая наценка поставщика. Любое предприятие нацелено приобрести какие – либо комплектующие для производства с наиболее выгодной для него ценой, поэтому предприятие находится в постоянном поиске выгодных цен и поставщиков. Таким образом руководитель отдела снабжения за ранее заключает «тайный» договор с фирмой, которая предлагает приемлемую торговую наценку, недобросовестный сотрудник предлагает минимальную накрутку, как правило это 2 – 5 процента от заявляемой поставщиком цены.

Реальным случаем, подтверждающим данную угрозу, является случившийся в 2013 году инцидент на предприятии АО «КРОНИКА», формулировка данного случая полностью подходит под статью 159 ч.3 УК РФ «мошенничество, совершенное лицом с использованием своего служебного положения».

Кейс 1.

Начальник отдела ОМТО вступил в тайный сговор с фирмой – поставщиком продукции, сообщив путем переписки со своего рабочего места в информационной сети интернет конфиденциальную, являющуюся коммерческой тайной информацию, а именно предоставив фирме ЗАО «Х» рыночные цены, используемые для составления плана – графика закупок АО «КРОНИКА», далее фирма ЗАО «Х», участвуя в конкурсе на закупки незаконно завысив цену на 30% выше рыночной, пользуясь покровительством начальника ОМТО таким образом выиграв тендер на поставку необходимой продукции, после чего начальник ОМТО, следуя своему плану, нацеленному на незаконное обогащение и имея доступ к документообороту и процессу подготовки документов включает в цепочку поставок посредника фирму «Х2», которая юридически оформлена на директора фирмы «Х», после чего фирма «Х2» за свои услуги поставки начисляет торговую наценку равную 20% из этих 20% начальник ОМТО получил «откат» равный 5% из всего этого следует вывод что цена контракта была незаконно завышена на 50%.

Кроме этого, сами поставщики часто неправомерно завышают цену контракта на поставку необходимых предприятию ресурсов, путем включения в договор несуществующих опций или функционального потенциала ресурса, за которые взималась дополнительная плата. Так как предприятию необходим ресурс, обладающий определёнными функциональными свойствами, то это может нанести вред как технологической составляющей производства, так и финансовой.

Важно понимать то, что любое предприятие занято специфической экономической и торговой деятельностью, поэтому факторы внешних и внутренних угроз экономической безопасности для каждого предприятия будут индивидуальны. Формат угроз экономической безопасности также зависит от формы собственности (государственная и частная), вида деятельности и особенностей рынка, на котором работает компания. Необходимо отметить, что данные предприятия отличаются спецификой деятельности и юридическим

статусом, поэтому, исходя из специфики деятельности угрозы данных предприятий могут отличаться. Так, например, основным видом деятельности АО «ИМПЕРА» является исполнение заказов, связанных с государственными контрактами. Поэтому с одной стороны система экономической безопасности опирается на жесткую систему контроля над исполнением государственного заказа, что помогает избегать многих угроз. С другой стороны, для данного предприятия характерны специфические проблемы, которые редко встречаются в частном бизнесе.

Исходя из вышесказанного к основным угрозам, связанным с экономической безопасностью на АО «ИМПЕРА» относятся:

1) Недобросовестные действия сотрудников предприятия и поставщиков.

К недобросовестным действиям сотрудников стоит отнести деятельность закупочной комиссии, так как члены закупочной комиссии являются одним из подразделений механизма обеспечения экономической безопасности на предприятии, соответственно имеют доступ к специальным документам, отражающим перечень юридических лиц, выигравших конкурс на поставку необходимых для производства комплектующих, а также члены закупочной комиссии осведомлены о начальной(максимальной) цене контракта. Таким образом, если один или несколько сотрудников, входящих в закупочную комиссию имеют корыстный интерес, связанный с незаконным обогащением, то смогут пролоббировать свои интересы, путем открытого взаимодействия с поставщиками.

Все дальнейшие примеры происходили в одном из городов Центрального федерального округа Российской Федерации, свидетелями данных правонарушений были действующие сотрудники АО «ИМПЕРА», одним из таких примеров, подтверждающих недобросовестность закупочной комиссии, является инцидент, произошедший в 2012 году.

Кейс 2.

Суть данного инцидента заключается в следующем, закупочная комиссия, имея зарегистрированные на свое имя компании, учувствовали в конкурсе на поставку необходимого ресурса для деятельности предприятия, более того так как закупочная комиссия собирает заявки на участие и определяет победителя конкурса, то победителями всегда становились компании зарегистрированные на имя членов закупочной комиссии, при этом члены закупочной комиссии заранее зная о победе, неправомерно завышали цены контрактов в 2-3 раза. Таким образом, в данной ситуации мы видим прямое нарушение закона о закупочной деятельности, уголовного кодекса по ст. 159 ч.3, а также внутреннего регламента предприятия о конфликте интересов.

К недобросовестным действиям поставщиков относится неправомерные действия поставщиков, участвующих в конкурсах на поставки необходимых для деятельности предприятия ресурсов. В основном, все действия таких поставщиков основываются на нарушении Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" от 05.04.2013 N 44-ФЗ, также использования не регулируемых законом видов закупочной деятельности.

Примером подтверждающим вышесказанное, является инцидент, способствовавший открытию нового вида мошенничества на электронных площадках.

Кейс 3.

Суть данного инцидента заключается в следующем, путем электронных торгов на поставку продукции выиграла фирма ООО «Y», являющаяся фирмой оптовой торговли, после чего с данной фирмой был заключен контракт на 2 миллиона рублей, поставка осуществлялась по следующей схеме, после 50% предоплаты ООО «Y» отправляет продукцию, после получения предприятием продукции следует перевод оставшихся 50% суммы. Но после перевода 50% предоплаты в 1 миллион рублей, фирма ООО

«Y» перестала отвечать на звонки и каким – либо образом контактировать с другой стороной контракта. После данного случая началась тщательная проверка фирмы ООО «Y» вследствие которой выяснилось, что на руководителя данной фирмы зарегистрировано в общей сложности 15 обществ с ограниченной ответственностью на одном юридическом адресе. Местное отделение РОВД в возбуждение уголовного дела отказало, так как данный вид торгов на электронных площадках не подходит ни под одну статью о мошенничестве. Более того изначально сотрудник отдела экономической безопасности не был включен в состав закупочной комиссии, что не позволило выявить данные нарушения на начальной стадии, вследствие чего члены закупочной комиссии приняли решение самостоятельно, игнорируя все существующие протоколы проверки, что может являться доказательством их к причастности к данному инциденту.

Подводя итог можно сказать, что основные угрозы для экономической безопасности предприятий вне зависимости от форм собственности происходят в первую очередь от сотрудников, которые имеют прямой доступ к конфиденциальным данным, утеря или корыстное использование которых может нанести прямой экономический ущерб компании, и сделать ее объектом внутрикорпоративного мошенничества. Основная задача системы обеспечения экономической безопасности – работа с сотрудниками на предмет определения потенциальных рисков и выявления способов мошенничества внутри компании.

3 Практические рекомендации по созданию системы экономической безопасности

3.1 Создание системы экономической безопасности на предприятии

3.1.1 Основные принципы эффективного функционирования системы экономической безопасности

Как уже было сказано выше, защита компании от внутрикорпоративного мошенничества должна иметь системный подход, притом, что данная система должна строиться на полной «прозрачности действий», как сотрудников, так и руководителей компании.

Прозрачность действий с точки зрения системного подхода должна осуществляться за счет четко организованной системы контроля, которая в свою очередь должна быть распространена на все структурные подразделения предприятия. Как уже было сказано выше, основным катализатором угроз, связанных с внутрикорпоративным мошенничеством является доступ или утеря информации, содержащей сведения о финансово – хозяйственной деятельности предприятия и являющаяся коммерческой тайной.

Стоит отметить то, что на сегодняшний день, в условиях стихийно развивающихся информационных технологий, для любого предприятия вне зависимости от его размера и формы собственности информация является самым важным нематериальным активом, поэтому необходимо уделять особое внимание ее безопасности.

Система экономической безопасности, нацеленная на выявление, предотвращение и недопущение случаев внутрикорпоративного мошенничества должна основываться на трех основных составляющих, таких как:

1) Правовой (юридический) контроль;
2) Информационный контроль;
3) Экономический контроль.

Правовой контроль является основополагающим в данной системе, так как предусматривает решение данной проблемы на законодательном уровне, а именно внедрение и использование на предприятии таких законов как Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации", Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне", Федеральный закон "О государственном оборонном заказе" от 29.12.2012 N 275-ФЗ, Федеральный закон "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" от 05.04.2013 N 44-ФЗ.

Однако основной проблемой данных законодательных актов является то, что в данных законах нет четкого описания механизмов, призванных обеспечивать необходимые к исполнению обязательства, которые данные законы регламентируют. Проще говоря «законы рецептов не дают». Кроме того, с 2010 года утратил силу Закон РФ от 11.03.1992 N 2487-1 "О частной детективной и охранной деятельности в Российской Федерации" и в настоящее время служба безопасности не имеет законных оснований на существование. Но в целях предотвращения ущерба правам, законным интересам, жизни или здоровью граждан, легитимным (законным) способом при обеспечении частной безопасности может быть только получение возмездных услуг от частных детективов и охранных предприятий, деятельность которых подлежит лицензированию. Задачами лицензирования данных видов деятельности являются предупреждение, выявление и пресечение нарушений юридическим лицом, его руководителем и иными должностными лицами, а также индивидуальными предпринимателями, требований, которые установлены ФЗ от 04.05.2011 N 99 «О лицензировании отдельных видов деятельности» Данный закон подразумевает создание службы экономической безопасности, но опять же не прописывает четкие полномочия сотрудников.

Исходя из выше сказанного необходимо в рамках работы системы экономической безопасности (СЭБ) предоставлять предприятиям возможность

самим создавать правовую базу, регулирующую деятельность СЭБ с четко прописанными задачами, полномочиями, сферами деятельности и возможными взаимодействиями с другими структурными подразделениями организации.

Данное решение дает предприятию возможность создать абсолютно обособленную систему экономической безопасности, которая будет адаптирована только на конкретное предприятие, так как многие предприятия либо не разрабатывают собственную систему экономической безопасности, либо используют общемировые стандарты, которые не всегда могут подойти под конкретные предприятия.

Информационный контроль, действует и функционирует в рамках системы экономической безопасности и также является основным в общей картине работы СЭБ.

Так как именно информационный контроль является основой экономической безопасности, то во – первых необходимо также построить систему контроля внешних и внутренних информационных потоков и над деятельностью сотрудников.

Данная система контроля должна начинать работу с самого начального уровня, а именно с приема сотрудника на работу. Для этого необходимо подготовить и утвердить перечень документов, составляющих коммерческую тайну. При приеме сотрудника на работу в компанию необходимо ознакомить его с данным списком документов, если специальность сотрудника предусматривает работу с документами и этого списка, затем необходимо дать сотруднику подписать документ о неразглашение коммерческой тайны где будут указаны все документы, с которыми сотруднику придется работать.

Продолжая тему контроля рядовых сотрудников, также необходимо уделять внимание уже действующим сотрудникам. В данный момент на многих предприятиях используется ручной контроль каналов внутренней связи, а также корпоративных каналов связи сотрудников. Данный метод основан на поиске по «ключевым словам» всех возможных совпадений на корпоративной и

личной почте сотрудников. Для удобства и автоматизации данного процесса необходимо внедрить систему DLP.

Система DLP позволяет вести автоматизированный поиск по тем же «ключевым словам», только делая это в режиме реального времени. Но в работе данной системы присутствует довольно большой минус, данная система осуществляет мониторинг корпоративных почт, месседжеров и других каналов связи только по тем словам на которые была запрограммирована, поэтому возникает вопрос, что именно нужно искать. Данный минус является определяющим для большинства предприятий при принятии решения о внедрении данной системы. Поэтому, как уже было сказано выше необходимо создать перечень документов, которые составляют коммерческую тайну.

Таким образом система экономической безопасности должна опираться на механизмы контроля внешних и внутренних потоков, более того за работой системы должен следить квалифицированный сотрудник, через его компьютер должны проходить все протоколы о проверке данной системы корпоративных компьютеров сотрудников.

Кроме рядовых сотрудников информационному контролю должны быть подвергнуты сотрудники, являющиеся руководителями. Информационный контроль руководителей должен также включать в себя методы, описанные выше, а именно контроль внутренних потов информации. Помимо этого, необходимо подготовить и ввести регламент контроля уровня допуска с последующем его разделением в зависимости от занимаемой должности. Основным преимуществом данного предложения является то, что сотрудник, которому необходимо ознакомиться с информацией, составляющей коммерческую тайну, должен лично расписаться за ознакомление и не разглашение данной информации, затем сотрудник вносит имя, фамилию и должность данного сотрудника, в специальный реестр, который хранится в архиве. Также необходимо запретить делать копии документов, составляющих коммерческую тайну, а также особо ценные документы помечать специальными водяными знаками.

Экономический контроль в общей системе экономической безопасности занимает направляющую роль. Его роль заключается в подготовке и проведении оценки рисков на предприятии. Кроме того, необходимо также провести анализ рисков, связанных с каждым рядовым и ключевым сотрудником и структурными подразделениями на предприятии. Данная мера позволит точно увидеть цену вложений для контроля на каждого конкретного сотрудника и цену потерь от каждого сотрудника в зависимости от его положения и должности в организации. Более того расчет рисков позволит рационально распределить бюджет, так как позиции в организации имеющие наибольшую уязвимость к угрозам экономической безопасности, а также их структурные подразделения будут финансироваться и снабжаться механизмами контроля в первую очередь.

3.2 Организационная структура службы экономической безопасности

Одним и важнейших мероприятий по выявлению, предотвращению и недопущению экономических потерь, связанных с внутрикорпоративным мошенничеством по-нашему мнению является внедрение отдела экономической безопасности.

Проводя анализ предприятий, являющихся объектами исследования, мы сделали вывод о том, что большинство предприятий предпочитают создавать отдел экономической безопасности формально, мотивируя свое желание тем, что создание отдела экономической безопасности с точки зрения корпоративных процедур может нанести предприятию дополнительные финансовые затраты. Поэтому руководители данных предприятий предпочитают разделять обязанности и полномочия между другими структурными подразделениями, что является не совсем эффективным.

Отдел экономической безопасности должен быть интегрирован в общую организационную структуру предприятия и носить исключительно

контролирующую функцию. Для удобства восприятия объединим все выше написанное в схему.

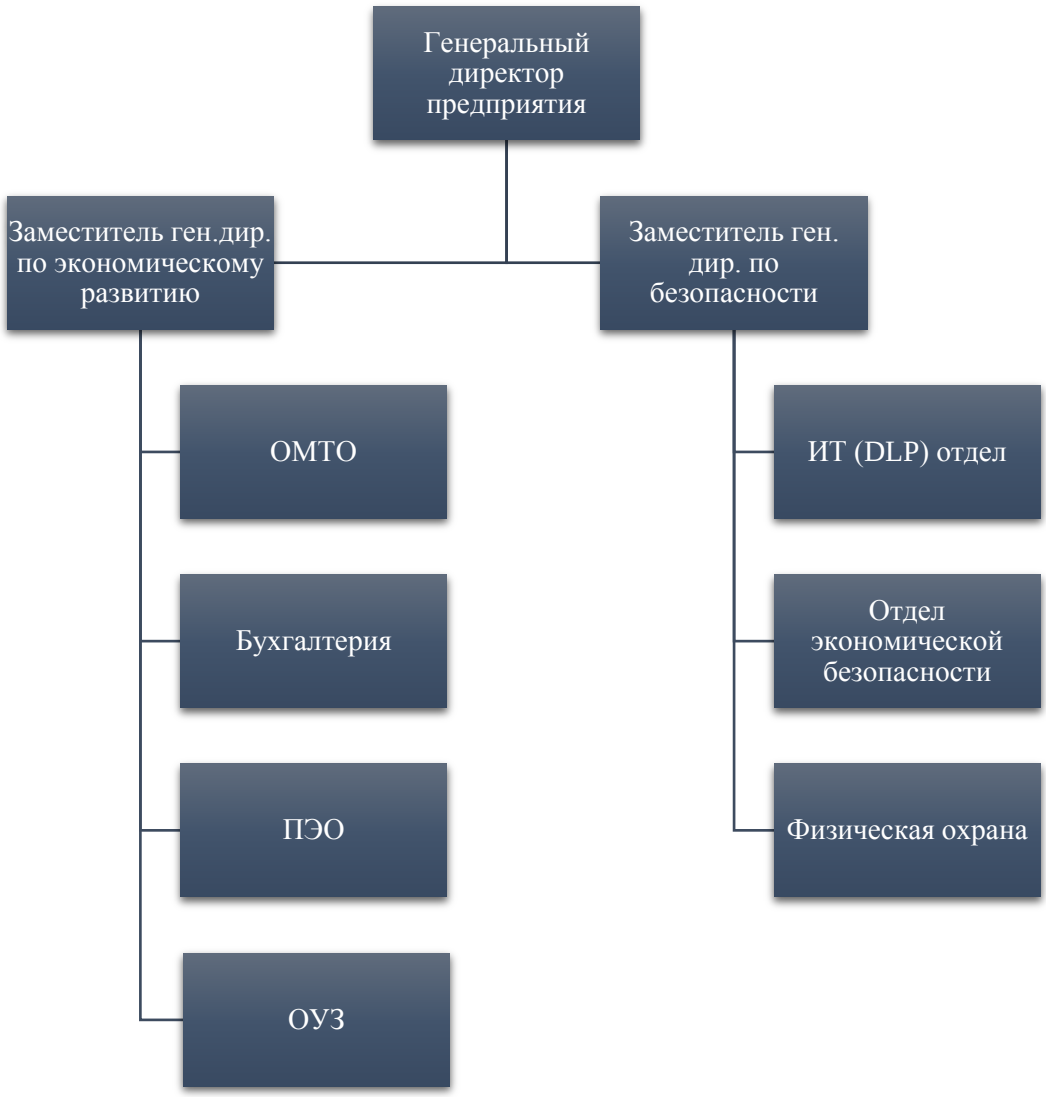


Рисунок 8 – Организационная структура службы экономической безопасности

Как уже было сказано выше, отдел экономической безопасности должен носить исключительно контролирующую функцию. Контролировать данный отдел должен структурные подразделения, которые являются наиболее опасными с точки зрения экономической безопасности. Как показывает практика наиболее опасными отделами являются отделы, связанные с закупочной деятельностью. Более того отдел экономической безопасности с точки зрения системного подхода не может быть структурно обособленной единицей, поэтому для образования целостной системы экономической

безопасности необходимо сотрудничество с другими структурными подразделениями.

Для более подробного изучения вопроса разберем функционал основных структурных подразделений, образующих систему экономической безопасности предприятия.

Основными структурными подразделениями, как видно на схеме 3 являются такие отделы, как:

– ИТ (DLP) отдел;
– Отдел экономической безопасности;
– Отдел физической охраны.

Функциями информационно технологического или DLP (Data Leak Prevention) отдела является:

– Контроль внутренних и внешних каналов связи;
– Контроль утечки информации на всех этапах закупки.

Обращаясь к статистике, можно отметить что большинство случаев внутрикорпоративного мошенничества, совершалось манипуляциями с информацией, составляющей коммерческую тайну и в полной уверенности отсутствия контроля за движением информационных потоков.

На данный момент многие предприятия пытаются контролировать потоки информации на предприятии, осуществляя данный контроль путем анализа всех входящих и исходящих потоков путем поиска по «ключевым словам» вручную. Но для того чтобы минимизировать трудозатраты по времени и качеству поиска необходимо автоматизировать данную процедуру.

Для автоматизации данного метода противодействию мошенничеству уже существуют автоматизированные системы контроля-DLP системы.

DLP система представляет собой пакет технологий, призванных предотвращать утечки конфиденциальной информации из информационной базы предприятия, а также включает в себя технические устройства (программные или программно – аппаратные) для такого предотвращения утечек.

Данная система способна в режиме «реального времени» производить анализ информационных потоков, предоставляя протоколы анализа руководителю ИТ (DLP) отдела. Более того данная система способна выявлять и блокировать несанкционированное подключение съемных носителей на отдельно взятом компьютере.

Отделом экономической безопасности должны осуществляться следующие функции:

– Контроль контрагентов;

– Проверка обоснованности цены контракта;

– Контроль конфликта интересов;

– Разработка регламента о защите информации, составляющей коммерческую тайну;

– Разработка критериев выбора поставщиков;

– Формирование планов-графиков закупочной деятельности предприятия.

В ведение сотрудников отдела экономической безопасности (далее ОЭБ) должны находится все элементы закупочной деятельности, а именно контракты, материально-техническое обеспечение, проведение различных тендеров и конкурсов.

Перед заключением контракта, сотрудники ОЭБ должны в обязательном порядке проверить стороны контракта, так называемых контрагентов. Проверка должна заключаться в тщательной проверке второй стороны заключаемого контракта через базы данных о предприятиях. В данную проверку в обязательном порядке должны входить такие пункты, как:

– Проверка юридического и физического адреса регистрации фирмы по ИНН и ОГРН;

– Проверка даты регистрации и совокупного времени нахождения на рынке;

– Проверка реестра недобросовестных поставщиков;

– Проверка номинального владельца фирмы на предмет владения им другими фирмами;

– Проверка фирмы на предмет уголовного преследования, различных видов бухгалтерской задолженности;

– Проверка на предмет конфликта интересов.

Такой алгоритм проверки должен применяться ко всем заявленным на участие в конкурсе или тендере фирмам.

После того как состоялась проверка фирмы, сотрудники ОЭБ должны проверить обоснованность цены, которую заявляет поставщик. Проверка цены осуществляется через базы производителей или же в свободном поиске, используя онлайн поисковики для поиска похожего по функционалу или идентичного товара. Если же сотрудники ОЭБ смогут найти необходимый ресурс по цене за единицу ниже чем предлагает поставщик, то цена признается завышенной.

Основной функцией сотрудников отдела экономической безопасности является разработка регламента по защите информации, составляющей коммерческую тайну, а также регламента, регулирующего доступ к такого рода информации.

Регламент о защите и доступе к информации, составляющей коммерческую тайну должен включать:

– Положение о доступе и уровнях доступа к информации;

– Положение об ознакомлении с информацией;

– Положение о неразглашении;

– Положение о хранении информации.

Теперь разберем каждое положение более подробно.

Доступ к информации должен осуществляться исходя из необходимости для конкретного сотрудника ознакомления с данной информацией. Кроме того, в зависимости от занимаемой должности на предприятии сотрудник может

получить доступ только к той информации, которая по значимости и важности соразмерна его должности.

Процесс ознакомления должен инициироваться сотрудником, которому по каким-либо причинам необходимо ознакомиться с информацией, представляющей важность для предприятия. Данный сотрудник в первую очередь должен написать заявления на имя руководителя ОЭБ с просьбой предоставить ему доступ к информации, указанной в заявление. После этого сотрудники ОЭБ начинают проверку сотрудника на предмет его благонадежности и связей, анализ персональных каналов корпоративной связи, должности на предприятии, а также проводят анализ целесообразности ознакомления с данной информацией, после чего руководитель ОЭБ выносит решение о предоставление ему доступа к информации в зависимости от должности сотрудника.

После того как решение было принято, сотрудники ОЭБ составляют пакет документов, которые сотрудник, получающий доступ должен будет подписать.

В данный пакет документов входит положение о неразглашении данным сотрудником информации, перечень которой также прилагается к данному документу и перечисляются возможные последствия для сотрудника в случае разглашения информации, а также запрет передавать данный документ третьим лицам и снимать копии с данного документа. После того как сотрудник подпишет данный пакет документов, он получает право на ознакомление с необходимой ему информацией. После ознакомления сотрудник должен поставить подпись и дату, а также указать полное имя и должность в реестре документооборота.

Если сотруднику нужна копия документа, то исходя от важности и конфиденциальности документа, сотрудник ОЭБ может снять копию, в обязательном порядке отметив это в реестре документооборота, получив копию на руки, сотрудник должен расписаться и поставить дату.

Но как уже было отмечено выше основой является должность сотрудника, если сотрудник, которому необходимо ознакомиться с информацией, представляющей стратегическое или иное значение для предприятия, входит в топ-менеджмент организации или является руководителем структурного подразделения, то он кроме выше описанных действий должен пройти дополнительное медицинское освидетельствование.

Положение о ознакомление с информацией должно включать в себя перечень документов, представляющих какую-либо коммерческую ценность или важность для предприятия и принципы ознакомления с данными документами.

Сотрудники ОЭБ должны также отслеживать внутренний документооборот. Так, например, если сотруднику необходимо ознакомиться с информацией и был получен для этого доступ. То сотрудники ОЭБ проверяют входит ли данная информация в перечень документов, представляющих ценность. Если такая информация там присутствует, то сотрудники ОЭБ имеют право запретить выносить данный документ за пределы отдела, более того для ознакомления сотрудник должен проследовать в специально оборудованную комнату где при получении документа он ставит подпись, полное имя, дату и время. При входе его обыскивают с помощью электромагнитных излучателей на предмет выявления фото, аудио и прочих цифровых носителей. После ознакомления сотрудник сдает документ сотрудникам ОЭБ где опять же ставить подпись, дату и время. Сотрудник ОЭБ передает данный документ в архив где также ставит подпись, полное имя, дату и время. Кроме того, сотрудники ОЭБ должны обладать техническими знаниями или получить квалификацию на предприятии, так как это напрямую зависит от пригодности и долговечности товара.

Положение о неразглашении должно обязательно использоваться при процедуре приема сотрудника на работу. При приеме сотрудника на работу, должна учитываться будущая его должность, степень ответственности и перечень документации, с которой сотруднику предстоит работать. Сотрудники

ОЭБ должны проверить все реестры документооборота на предприятии, которые необходимы для данной должности. Если документы, с которыми новый сотрудник будет работать входят в данный реестр, то при приеме на работу сотрудник должен подписать соглашение о неразглашении, в котором перечисляются конкретные документы, с которыми сотрудник имеет право знакомится и ответственность за разглашение которых он несет. Если же таких документов там нет, то сотрудник подписывает простое соглашение о неразглашении общего характера.

Функции отдела физической охраны заключаются в обеспечение безопасности сотрудников предприятия, контрольно-пропускного режима, безопасность материальных активов предприятия.

3.3 Процедуры организации закупочной деятельности

Как уже было отмечено выше, большинство инцидентов мошенничества происходят во время процедур, связанных с подготовкой и осуществлением закупок на предприятии.

На сегодняшний день согласно Федеральному закону № 44-ФЗ от 5 апреля 2013 года «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» закупочная деятельность предприятия осуществляется следующим образом.

1) Зарегистрироваться в единой информационной системе (далее ЕИС) и на электронных торговых площадках.

Для этого нужна электронная подпись, которую заказчики получают бесплатно в федеральном казначействе. Казначейство разместит заявку на регистрацию в Единой информационной системе. Владельцу подписи с правами администратора останется зайти в ЕИС и в личном кабинете настроить права доступа остальным сотрудникам. После этого можно публиковать закупки. Оператор ЕИС зарегистрирует заказчика и на 5 федеральных электронных торговых площадках госзакупок.

Тем, кто уже зарегистрирован в системе, до 1 января 2017 года нужно перерегистрироваться (приказ ФК от 30.12.2015 № 27н).

2) Назначить контрактного управляющего или создать контрактную службу.

44-ФЗ разрешает ограничиться одним контрактным управляющим, если объем закупок в год не выше 100 млн. руб. Во всех других случаях нужна контрактная служба минимум из двух сотрудников. Это может быть специальный «закупочный» отдел. Или обязанности контрактной службы можно распределить между сотрудниками разных подразделений.

Например, бухгалтер составляет планы-графики. Главный инженер готовит техзадание, отвечает на запросы разъяснений и принимает качество товара. Секретарь собирает заявки с отделов, готовит и размещает документы в ЕИС. Руководитель контролирует работу, отвечает на претензии ФАС и подписывает контракты.

С 1 января 2017 года все работники контрактной службы должны иметь профильное высшее или дополнительное образование по 44-ФЗ. Если в службе есть «недотягивающие» до требований сотрудники, то до конца года они должны пройти повышение квалификации (108 часов для сотрудников, 40 — для руководителей). Это можно сделать очно или дистанционно в организации, у которой есть лицензия на образовательную деятельность.

3) Разработать и разместить в ЕИС планы и планы-графики закупок.

Заказчики имеют право проводить только запланированные закупки. С 2017 года документов по планированию станет два: помимо плана-графика нужно теперь вести и план закупок. Опубликовать обобщенный план закупок и подробный план-график нужно в течение 10 рабочих дней после утверждения бюджета на год. В план-график включают:

- Название закупки с указанием всех характеристик;
- Количество товара;
- Начальную цену и ее обоснование;
- Способ закупки и его обоснование;

– Дополнительные требования к участникам закупки.

С 2017 года заказчик обязан:

– Включать в план-график срок окончания контракта: сюда входит экспертиза, приемка и оформление документов;

– Указывать дату и причину любых изменений в плане-графике;

– Указывать точные сроки полной оплаты.

4) Учесть нормирование и запреты в сфере госзакупок.

Заказчики должны не только планировать закупки, но нормировать и обосновывать их (ч.1, ст.19, 44-ФЗ).

Расходы на конкретного сотрудника нормированы. Например, врачу полагается 2 хлопчатобумажных халата в год, а руководителю — не больше 2 кресел в год. Чтобы определить нормативы цены, устанавливается среднерыночная стоимость единицы продукции.

Эти требования закреплены в федеральных, региональных и муниципальных нормативных актах. Работники контрактной службы должны их знать.

Нужно следить за качеством закупаемых товаров. Специалисту надо разбираться в свойствах товара, потому что от этого зависит его пригодность и долговечность.

В некоторых закупках заказчик должен устанавливать преференции поставщикам. Например, на часть товаров распространяется национальный режим. Это значит, что заказчик должен предоставить преференции российским поставщикам.

И, наконец, на закупку некоторых товаров установлены запреты. Например, нельзя закупать иностранное программное обеспечение, если есть его российский аналог.

5) Подготовить и разместить в ЕИС закупочную документацию

Корректно описать закупку. При описании закупки можно использовать только термины, которые предусмотрены в технических регламентах и документах из национальной системы стандартизации. Если это невозможно,

придется обосновать, почему при закупке нужно применять нестандартные требования и терминологию. Смысл стандартизации в том, чтобы минимизировать риск описать закупки «под своих» поставщиков.

В закупке нужно указать функциональные, технические, качественные и эксплуатационные характеристики объекта закупки. При этом техническое задание должно быть нейтральным, не ограничивать конкуренцию. Нельзя устанавливать конкретные параметры товара, только диапазон «не менее» и «не более», или чрезмерные требования к товарам. Исключение из правил: если у товара нет аналога или это запчасти к уже имеющемуся оборудованию.

Соблюсти сроки размещения. При запросе котировок заказчик размещает закупку и проект контракта не меньше чем за 7 дней до окончания срока подачи заявок. Этот срок можно сократить до 4 дней, если сумма меньше 250 000 рублей или закупаются продукты питания, ГСМ, жизненно необходимые лекарства.

При электронном аукционе сроки подачи заявок зависят от цены закупки. Если начальная цена контракта больше 3 млн. рублей, у вас есть не меньше 15 календарных дней. Если начальная цена контракта не превышает 3 млн. рублей, то срок подачи заявок составляет не меньше 7 календарных дней.

Заявку на конкурс нужно разместить за 20 дней до окончания срока приема заявок.

Можно изменить извещение. Сроки в разных процедурах разные:

– Для аукциона — не позже чем за 2 дня до даты окончания срока подачи заявок;

– Для конкурса — не позже чем за 5 дней до даты окончания срока подачи заявок;

– Для запроса котировок — не позже чем за 2 рабочих дня до даты истечения срока подачи заявок.

Заказчик обязан отвечать на запросы на разъяснения от поставщиков и размещать их в ЕИС для доступа всем участникам закупки в течение двух дней.

При проведении запроса котировок заказчик не обязан отвечать на запрос разъяснений.

Еще заказчик вправе отменить любую закупку, кроме запроса предложений:

– если это конкурс или аукцион, не позже чем за пять дней до окончания срока подачи заявок,

– если запрос котировок, не позже чем за два дня до окончания срока подачи заявок.

6) Провести закупку.

Есть 10 видов закупок. Некоторые из них имеют лимиты, которые нужно распределять на весь год.

Например, одну закупку у единственного поставщика можно провести на сумму не выше 100 000 рублей. Годовой объем таких закупок — не больше 5% от всех закупок в год и не больше 50 миллионов (4п. 1ч. 93ст, 44-ФЗ). Организации с бюджетом меньше 40 миллионов рублей могут закупать у единственного поставщика на сумму до 2 миллионов.

Конкурентные способы закупок делятся на 4 основные группы: запросы котировок и предложений, конкурсы и аукционы.

Запрос котировок можно провести, если начальная максимальная цена (НМЦ) не превышает 500 тыс. руб. Годовой объем таких закупок не должен превышать 100 млн. рублей в год и 10% совокупного годового объема закупок.

Запрос предложений можно провести в строго определенных 44-ФЗ случаях (ч. 2, ст. 83, 44-ФЗ).

Самый сложный метод определения поставщика — открытый конкурс. Зато он поможет выбрать поставщика по нескольким критериям: не только по низкой цене, а по качеству товара, квалификации и опыту участников.

Большой объем товаров входят в аукционный перечень. То есть закупать их можно только на электронных торговых площадках. Это, например, канцелярские товары, продукты, бумага, нефть, металлы, строительные работы и ремонт.

7) Подписать контракт.

Если требуется обеспечение закупки, контрактный управляющий должен убедиться, что деньги пришли на счет или проверить подлинность банковской гарантии. На 6 видов услуг уже разработаны типовые контракты, которые госзаказчики должны применять. В остальных случаях проект контракта составляет контрактная служба. Поставщик может лишь предложить протокол разногласий, который заказчик принимает или нет.

8) Внести сведения об уклонившихся от подписания контракта в реестр недобросовестных поставщиков (РНП).

Обязанность заказчиков — направлять в ФАС сведения об участниках:

– Уклонившихся от заключения договора,

– С которыми расторгнуты договоры по решению суда.

Обращаться нужно в письменном или в электронном виде в центральный аппарат ФАС России или территориальные органы ФАС по месту нахождения заказчика.

9) Принять товар и оплатить контракт.

Сейчас в ч. 8 ст. 30 44-ФЗ указан предельный срок оплаты по контрактам с СМП и СОНО. Он составляет не больше 30 дней после того, как заказчик подписал документ о приемке.

Остальные случаи прописываются в контракте. В статьях мы часто просили поставщиков обращать внимание на такие расплывчатые формулировки в описании сроков оплаты, как «работы оплачиваются после получения финансирования от администрации края», «в рамках софинансирования в 2017 году» и т. д. Это значит, что денег придется ждать долго.

Разрабатывается новый законопроект, который установит предельный срок оплаты по любым контрактам по 44-ФЗ. Это сыграет в пользу поставщиков, но при этом поставит заказчиков в жесткие рамки. Денег в бюджет могут просто не перевести, а бюджетной организации их взять негде.

10) Разместить отчетность.

Заказчики по 44-ФЗ обязаны публиковать в ЕИС два отчета:

1) Отчет об исполнении контракта или результатах его отдельного этапа, в который входят:

– Сведения о поставщике, контракте, результатах его полного выполнения или выполнения отдельного этапа.

Если контракт не выполнен, выполнен некачественно, в него внесли изменения или расторгли, это тоже нужно обязательно указать. Отчет размещают за 7 рабочих дней с момента подписания документа о приемке контракта или его расторжения.

В данной работе мы предлагаем разделить этапы осуществления закупки между структурными подразделениями, а службу экономической безопасности представить «последней инстанцией», которая будет осуществлять общий контроль и выносить решения.

Необходимо отметить то, что на предприятиях уже существуют службы, занимающиеся осуществлением закупочной деятельности, такие службы как:

– Отдел материально-технического обеспечения;

– Отдел управления закупками;

– Планово-финансовый отдел;

– Закупочная комиссия.

Основными механизмами контроля, по нашему мнению, являются разделение информации и система жесткого контроля в рамках действующего административного ресурса.

Таким образом система контроля закупочной деятельности должна выглядеть следующим образом.

Отдел экономической безопасности формирует план-график закупок учитывая все технические и юридические нюансы в рамках действующего законодательства. Затем «порционно» выдает информацию руководителем других отделов. Отдел ОМТО готовит и оформляет технические характеристики на конкретный продукт закупки, после чего передаёт для

оформления пакета документов в отдел ОУЗ. Далее отдел ОУЗ готовит полный пакет документов в рамках 44-ФЗ, после чего предаёт всю документацию ПФО. Отдел ПФО устанавливает начальную(максимальную) цену контракта и организует конкурсную процедуру и осуществляет сбор заявок. После чего отдел ОЭБ начинает проверку, этапы которой были описаны в пункте 3.2. После проведения всех этапов проверки вся отчетность передается на заседание закупочной комиссии, которая в свою очередь выносит решение о выборе поставщика.

Более того в процессе, описанном выше активное участие принимает отдел ИТ (DLP), отслеживающий вручную или с помощью автоматизированных систем, движение потоков информации на каждом этапе закупочной деятельности.

Резюмируя, необходимо отметить, то что существует различие в подходах к обеспечению экономической безопасности в коммерческих и государственных организациях. В государственных структурах многие процессы жестко регламентированы, поэтому основные угрозы экономической безопасности связаны с внешними факторами, в основном угрозы внешнего характера связаны с недобросовестными поставщиками. В частных структурах роль внутренних факторов риска гораздо выше, так как основной угрозой является «человеческий фактор», а контроль зачастую может основываться на доверие руководителю структурного подразделения. Но не смотря на преобладающие внутренние риски, также существуют внешние угрозы, связанные с поставщиками.

Ключевую роль в определении размеров и порядка функционирования службы экономической безопасности играет размер и финансовые возможности организации. Здесь прежде всего, речь идет о возможности организации обеспечивать (содержать) отдел экономической безопасности, включая все необходимое для функционирование данного отдела оборудование. Как показывает практика, предприятия, относящиеся к государственным структурам, не могут позволить себе обеспечивать отдел экономической

безопасности, поэтому предпочитают распределять некоторые обязанности и полномочия данного отдела на другие структурные подразделения. В предприятиях, принадлежащих частному сектору, при наличии финансовых ресурсов, способных покрыть все расходы, связанные с организацией и обеспечением службы экономической безопасности, возникает проблема. Проблема выражается в том, что частные предприятия не могут сформировать необходимый перечень процедур и документов, подлежащих контролю, поэтому также, как и государственные компании распределяют обязанности и полномочия между структурными подразделениями.

Более того, опираясь на сегодняшнюю ситуацию, можно заметить, что снизилось качество образования, в следствие чего встает кадровый вопрос с точки зрения профессиональной подготовки. На сегодняшний день большинство предприятий государственного и частного сектора сталкиваются с дефицитом квалифицированных кадров на должности, связанные с экономической безопасностью. Таким образом предприятиям приходится также разделять обязанности между руководителями других подразделений, имеющих опыт работы. Также как минус стоит отметить то, что на всех предприятиях отсутствует система оценки эффективности работы сотрудников, совмещающих должности сотрудников экономической безопасности.

3.4 Экономическое обоснование создания отдела экономической безопасности

По нашему мнению, основными минусами являются финансовые возможности предприятия для организации и обеспечения службы экономической безопасности, а также отсутствие понятийного аппарата в формирование необходимых перечней документов и процедур, подлежащих контролю.

Для более глубокого понимания финансовой проблемы ниже мы приведем расчеты содержания одного сотрудника службы экономической безопасности в год.

На сегодняшний день средняя заработная плата по данным Росстата в России составляет 35,845 тысяч рублей.

Для недопущения конкуренции между сотрудниками внутри отдела экономической безопасности мы предлагаем уровнять заработную плату, а среднемесячную заработную плату сделать окладом для сотрудников.

Таким образом получаем:

35,845 тысяч рублей (месячный оклад, включающий отчисления во внебюджетные фонды) +25 процентов (ежемесячная премия) = 44,806 тысячи рублей (до уплаты НДФЛ)

44,806 + 30 процентов (северный коэффициент) =58,248 тысяч рублей (до уплаты НДФЛ);

58,248 тысяч рублей (до уплаты НДФЛ) -13 процентов (НДФЛ) = 50,676 тысяч рублей в месяц.

50,676*3(минимальное количество сотрудников ОЭБ) = 150,028 тысяч рублей в месяц

150,028*12 =1824,336 тысяч рублей в год.

Как видно из расчетов стоимость содержания троих сотрудников обойдется руководству предприятия в 1824,336 тысяч рублей в год.

Стоит отметить, что это только заработная плата, также нужно учесть ремонт помещения и стоимость необходимого оборудования и программного обеспечения. Ремонт стандартного офисного помещения 62м2 «под ключ» обойдется в среднем в 600,000 тысяч рублей. Оборудование в виде трех компьютеров, технические характеристики которых соответствуют сегодняшнему дню, обойдется в 270,000 тысяч рублей. Таким образом получаем 600,000 + 270,000 = 870,000 тысяч рублей составят общехозяйственные расходы.

Как было отмечено выше, необходимо внедрить автоматизированную систему контроля. Российский рынок систем контроля уже сейчас может предложить довольно достойные, бюджетные системы, такие как «Стахановец» и «Staffcop».

Данные системы предназначены для реализации следующих направлений:

– Контроль доступа и учета рабочего времени;

– Информационная безопасность предприятия и защита данных (DLP);

– Анализатор рисков информационной безопасности;

– Мониторинг эффективности сотрудников, распознавая полезную и вредоносную активность.

Цена данной системы контроля зависит от количества компьютеров в организации. Для примера будем считать, что на предприятии присутствует 200 компьютеров. Цена установки программы составляет 2,243 тысячи рублей на один компьютер. Следовательно, 200*2,243 = 448,600 тысяч рублей – объем ежегодных затрат на программное обеспечение.

Также руководство предприятия может приобрести бессрочную лицензию, цена которой, предоставляется по запросу.

Таким образом получаем: 1824,336 тысяч рублей (заработная плата сотрудникам) + 448,600 тысяч рублей (программа автоматизированного контроля) = 2272,936 тысяч рублей.

Как видно из расчетов, содержание отдела экономической безопасности обойдется в 2272,936 тысяч рублей в год, но также необходимо отметить что расчеты являются приблизительными. Кроме того, для проведения расчетов, мы взяли один из бюджетных вариантов систем контроля. Для создания более сложной системы необходимо также учитывать дополнительные расходы на такие элементы средств защиты информации:

– Антивирус;

– Файервол;

– Пакет от несанкционированного доступа.

Подводя итог, необходимо подчеркнуть, что каждое предприятие самостоятельно для себя решает, сможет ли финансовое состояние организации обеспечивать круглогодично данную сумму. Если исходить из субъективного мнения, то данная сумма весьма внушительна для обеспечения одного отдела и прежде чем руководителю предприятия принять решение, необходимо очень детально изучить всю целесообразность обособления отдела экономической безопасности. Что касается возможности обеспечивать данную сумму каждый год, то здесь стоит отметить, что у частных предприятий в данной ситуации возможностей больше, чем у государственных предприятий. Прежде всего это обосновано тем что работа государственных предприятий довольно жестко регламентирована и особенно перераспределение чистой прибыли. Частное же предприятие может позволить себе немного больше, руководство может единогласным решением перераспределить чистую прибыль внутри организации. Поэтому, как уже было сказано выше, принимая решение необходимо довольно детально изучить все аспекты и нюансы данной процедуры.

Задание социальная ответственность

Студенту

Группа	ФИО
3АМ5Б	Засорину Ивану Александровичу

Институт	ИСГТ	**Кафедра**	Менеджмента
Уровень образования	Магистрант	**Направление/ специальность**	38.04.02 Менеджмент

Исходные данные к разделу «Социальная ответственность»	
1. Описание рабочего места (рабочей зоны, технологического процесса, используемого оборудования) на предмет возникновения: *- вредных проявлений факторов производственной среды (метеоусловия, вредные вещества, освещение, шумы, вибрация, электромагнитные поля, ионизирующие излучения)* *- опасных проявлений факторов производственной среды (механической природы, термического характера, электрической, пожарной природы)* *- негативного воздействия на окружающую природную среду (атмосферу, гидросферу, литосферу)* *- чрезвычайных ситуаций (техногенного, стихийного, экологического и социального характера)*	Рабочим местом является компьютерный, деревянный стол, а также сам компьютер, который в свою очередь является источником электромагнитного воздействия. Плохая освещенность или несоответствие параметров микроклимата могут привести к ухудшению психологического и физического самочувствия сотрудника, как следствие снижению работоспособности. К опасным факторам рабочего места можно отнести повреждение кожных покровов в следствие удара о края компьютерного стола. Для обеспечения экологической безопасности при утилизации оргтехники, обращение в специализированные службы. Воздействие на гидросферу и атмосферу не происходит. Никаких чрезвычайных ситуаций, которые могут произойти на рабочем месте не выявлено.
2. Список законодательных и нормативных документов по теме	Международный стандарт IC CSR-08260008000: 2011 «Социальная ответственность организации» Положение АО «НИИПП» по охране окружающей среды. Положение АО «НИИПП» по промышленной безопасности и охране труда. Годовой отчет АО «НИИПП» за 2016 год
Перечень вопросов, подлежащих исследованию, проектированию и разработке	
1. Анализ факторов внутренней социальной ответственности: *- принципы корпоративной культуры исследуемой организации;* *- системы организации труда и его безопасности;* *- развитие человеческих ресурсов через обучающие программы и программы подготовки и повышения квалификации;* *- системы социальных гарантий организации;* *- оказание помощи работникам в критических*	Внутренняя социальная ответственность АО «НИИПП» направленна на обеспечение социальной поддержки, квалифицированного обучения, безопасности деятельности сотрудников и поддержание для них достойного уровня труда и жизни.

ситуациях.	
2. Анализ факторов внешней социальной ответственности: *- содействие охране окружающей среды;* *- взаимодействие с местным сообществом и местной властью;* *- спонсорство и корпоративная благотворительность;* *- ответственность перед потребителями товаров и услуг (выпуск качественных товаров);* *-готовность участвовать в кризисных ситуациях и т.д.*	Внешняя социальная ответственность АО «НИИПП» направлена на охрану окружающей среды.
3. Правовые и организационные вопросы обеспечения социальной ответственности: *- анализ правовых норм трудового законодательства;* *- анализ специальных (характерные для исследуемой области деятельности) правовых и нормативных законодательных актов;* *- анализ внутренних нормативных документов и регламентов организации в области исследуемой деятельности.*	Регулирование отношения между организацией и сотрудниками происходит при следующих правовых нормах: - трудовой распорядок; - выплата социальных льгот; - коллективных договоров; - оплаты труда; - выплаты районного коэффициента; -особенностей регулирования труда женщин, детей, пенсионеров.
Перечень графического материала:	
При необходимости представить эскизные графические материалы к расчётному заданию (обязательно для специалистов и магистров)	Стейкхолдеры организации АО «НИИПП»; Структура программ АО «НИИПП»; Структура программ АО «НИИПП»; Затраты на мероприятия КСО АО «НИИПП»

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Черепанова Н.В.	к.ф.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
3АМ5Б	Засорин Иван Александрович		

4 Социальная ответственность

АО «НИИПП» проявляет все признаки социально ответственного предприятия. Уделяя внимание таким аспектам как экологическая безопасность, обеспечение гарантированного социального пакета для своих работников, членов их семей и пенсионеров, кроме того ведет активную работу по созданию достойных условий труда на производстве.

Заключаемый коллективный договор обеспечивает работникам: достойную и конкурентоспособную заработную плату, социальные льготы и гарантии, а также льготы и гарантии членам их семей, материальную помощь, выплаты по случаю юбилейной даты рождения, а также предоставление детских путевок в санатории (базы отдыха), более того предоставление абонементов на посещение спортивно-оздоровительных комплексов.

АО «НИИПП» стремится поддерживать своих бывших и действующих работников, поздравляя и даря подарки на общепринятые праздники. Прежде всего это поздравления на день старшего поколения и детей сотрудников на новый год и день защиты детей. Кроме того, АО «НИИПП» осуществляет поддержку ветеранов войны и труда и инвалидов.

По мере загруженности работой АО «НИИПП» принимает участие в городских, областных, мероприятиях различной направленности, неоднократно занимало призовые места.

Кроме всего прочего АО «НИИПП» занимается благотворительностью для Томской области.

Являясь социально ориентированным предприятием, АО «НИИПП» традиционно придаёт большое значение созданию безопасных условий труда для сотрудников, разрабатывая и реализуя комплексы программ по улучшению условий и охраны труда, улучшению санитарных и бытовых условий на производстве.

Основные направления деятельности:

– обеспечение работников сертифицированной спецодеждой, спецобувью и другими СИЗ согласно требованиям законодательства и корпоративных норм;

– приведение зданий и сооружений в соответствие с требованиями строительных норм, требований пожарной безопасности;

– приведение освещения и микроклимата на рабочих местах в соответствие с требованиями санитарно-гигиенических норм;

– обустройство новых и ремонт имеющихся санитарно-бытовых помещений, помещений для обогрева, отдыха и приема пищи;

– организация обучения работников по вопросам охраны труда, промышленной, пожарной, экологической безопасности, реагирования в случае аварийных и чрезвычайных ситуаций;

– проведение первичных и периодических медосмотров работников;

– автоматизация и компьютеризация производственного оборудования и рабочих мест;

– укомплектование производственных объектов средствами малой механизации и современным электроинструментом для снижения доли ручного труда.

–

4.1 Внешняя социальная ответственность компании АО «НИИПП»

Компания АО «НИИПП» в своей деятельности неукоснительно соблюдает требования законодательства, придерживается принципов добросовестной деловой практики и честной конкуренции.

Все действия руководства и сотрудников компании АО «НИИПП» направлены на то, чтобы максимизировать прибыль в рамках закона, требований рынка и с полным учетом затрат, так как именно этот показатель

при соблюдении всех вышеназванных условий свидетельствует о наибольшей эффективности ведения бизнеса.

Руководство и сотрудники компании АО «НИИПП» стремятся к открытости и прозрачности своих бизнес-процессов для заказчиков, партнеров и других социальных групп, чьи интересы пересекаются с деятельностью компании. В то же время, компания гарантирует полное сохранение информации, являющейся конфиденциальной, в том числе, данных о финансовых и других отношениях с клиентами и партнерами.

4.2 Определение стейкхолдеров программы КСО АО «НИИПП»

Определяем главных стейкхолдеров программы КСО, которые представлены в таблице 2.

Таблица 2 – Стейкхолдеры организации АО «НИИПП»

Прямые стейкхолдеры	Косвенные стейкхолдеры
1) Заказчики	-
2) Сотрудники компании	-
3) Государство	-

Так как АО «НИИПП» является государственным предприятием и в основном ориентированно на производство государственной продукции, то из этого следует что произведенная продукция уже изначально ориентирована на конечного потребителя. Но АО «НИИПП» также занимается выпуском гражданской продукцией, для также известных потребителей. Из этого следует вывод, что косвенных стейкхолдеров у АО «НИИПП» нет.

Для АО «НИИПП» одним из самых влиятельных российских стейкхолдеров является государство. С органами государственной власти АО «НИИПП» имеет следующие механизмы взаимодействия, которые регламентированы Федеральным законом № 44-ФЗ от 5 апреля 2013 года «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», а именно: государственным контрактом, отчетами о деятельности в рамках государственных контрактов,

также отчетами в сфере КСО и экологической программы и заключением дополнительных соглашений и протоколов сотрудничества.

АО «НИИПП» как и многие предприятия считает, что одним из важных факторов успеха являются слаженные действия всего коллектива. Стабильность, отсутствие социальной напряженности. АО «НИИПП» создает условия для полной реализации потенциала каждого сотрудника. Для взаимодействия с коллективом компания использует следующие механизмы: коллективный договор, корпоративные встречи.

Не менее важной группе стейкхолдеров относятся заказчики, с данной группой стейкхолдеров АО «НИИПП» взаимодействует через договора поставок продукции, разработанной на базе собственного НИИ.

4.3 Структура программ КСО АО «НИИПП»

В таблице 3 приведем структуру программ КСО, которые были реализованы в 2016 году.

Таблица 3 – Структура программ АО «НИИПП»

Наименование мероприятия	Элемент	Стейкхолдеры	Срок реализации	Ожидаемый результат от реализации мероприятия
Мероприятия, обеспечивающие надежное и безопасное функционирование предприятия				
Программа безопасности	социально-ответственное поведение	государство, сотрудники	2016 год	Обеспечение безопасного функционирования
Программа бережливого производства	социально-ответственное поведение	государство, сотрудники	2016 год	Реализация программы бережливого производства
Комплекс социальных программ, направленных на поддержание предусмотренных в коллективном договоре условий, а также корпоративные программы				
Социальные льготы персоналу и пенсионерам, предусмотренные законодательством и коллективным договором	собственные инвестиции	сотрудники	2016 год	Реализация политики улучшения микроклимата
Реализация	собственные	сотрудники	2016 год	Реализация

корпоративных социальных проектов	инвестиции			политики улучшения микроклимата

Таким образом, как видно из таблицы все описанные мероприятия КСО в основном направленны на эффективность деятельности сотрудников, а также на соблюдение законодательств, предусмотренных государством и соответствию корпоративных норм безопасности.

4.4 Определение затрат на программы КСО АО «НИИПП»

Затраты на реализацию программы КСО на предприятии АО «НИИПП» за 2016 год, представленные в таблице 4.

Таблица 4 – Затраты на мероприятия КСО АО «НИИПП»

Наименование мероприятия	Единица измерения	Цена	Стоимость реализации за год
Мероприятия, обеспечивающие надежное и безопасное функционирование предприятий			
Программа безопасности	тыс. руб.	-	2 000
Программа бережливого производства	тыс. руб.	-	3 000
ИТОГО:	тыс. руб.	-	5 000
Комплекс социальных программ, направленных на поддержание предусмотренных в коллективном договоре условий, а также корпоративные программы			
Социальные льготы персоналу и пенсионерам, предусмотренные законодательством и коллективным договором	тыс. руб.	-	1 000
Реализация корпоративных социальных проектов	тыс. руб.	-	500
ИТОГО:	тыс. руб.	-	1 500
ИТОГО:	тыс. руб.	-	**6 500**

Мероприятия, обеспечивающие надежное и безопасное функционирование предприятия, составили 5,000 тыс. руб.

Комплекс социальных программ, предусмотренных в коллективном договоре, а также корпоративные программы в объеме – 1,500 тыс. руб.

Таким образом описанные выше мероприятия программы КСО составляют 6,500 тыс. руб. в год. Данные мероприятия приносят пользу и повышают эффективность деятельности предприятия.

Общая сумма на реализацию программы КСО составляет 6,500 тыс. руб.

4.5 Оценка эффективности программ и выработка рекомендаций

Говоря об эффективности социальных программ, то важно сказать, что социальные программы напрямую зависят от статуса предприятия, а именно является ли оно государственным или частным.

Как видно из отчета для АО «НИИПП» приоритетным направлением является внутренняя социальная ответственность. Данное высказывание доказывает таблица 3, можно заметить, что во всех программах, которые были реализованы в 2016 году, задействованы сотрудники.

АО «НИИПП» тратит достаточно много усилий и затрат для мотивации персонала, предоставляя им хорошие условие труда, социальные льготы и прочее. Также достаточно много программ нацелены на помощь пенсионерам, ветеранам войны и действующим сотрудникам, и их семьям. Что позволяет вырабатывать у данной группы стейкхолдеров лояльность по отношению к компании.

Кроме того, АО «НИИПП» прикладывает не мало усилий для того, чтобы деятельность самого предприятия соответствовала нормам законодательства, сохраняли долгосрочные отношения с заказчиками и партнерами. Таким образом увеличивая лояльность государственной группы стейкхолдеров.

Подводя итог можно сказать что принципы КСО АО «НИИПП» позволяют добиваться таких конкурентных преимуществ, как: привлечение креативных и компетентных кадров; улучшение микроклимата, умение мотивировать и поощрять сотрудников, увеличение репутации предприятия и как следствие расширение возможностей для увеличения потока государственных субсидий и заказов.

Заключение

Проведя анализ сущности и проблем экономической безопасности на предприятии, можно сделать вывод, что целью экономической безопасности является минимизация внешних и внутренних факторов, угрожающих финансовым, материальным, информационным и кадровым ресурсам. При этом большую роль играет защита информации, так как именно информация является основным нематериальным активом любой организации. Кроме того, необходима работа с персоналом на предмет выявления и предотвращения внутрикорпоративного мошенничества, предоставляя доступ к информации исходя из принципов экономической целесообразности.

Экономическая безопасность предприятия - одно из важнейших свойств предприятия. Проведенный анализ существующих предприятий, позволил сделать о том, что подходы по обеспечению экономической безопасности на частных и государственных предприятиях существенно различаются. Основой этого различия является законодательство и капитализация предприятий. В сегодняшней ситуации частным предприятиям предоставляется больше свободы, но тем самым возрастают риски появления угроз как внешних, так и внутренних. На государственных предприятиях законодательство четко регламентирует все действия, связанные с финансово-хозяйственной деятельностью предприятия, тем самым сводя к минимуму риски, связанные с внутренним мошенничеством.

Кроме всего, что отмечено выше, существует наверно самая большая проблема современных предприятий. Данная проблема является краеугольным камнем всей экономической безопасности, так как связана с «понятийным аппаратом». Ситуация понятийного аппарата на сегодняшний день такова, что большинство книг (учебников) и руководителей предприятий не могут дать четкого определения понятия экономической безопасности. В связи с чем возникают проблемы с организацией функционала службы экономической безопасности.

Кроме того, можно сделать вывод о том, что существует огромное различие между государственным и частным предприятиями, и, прежде всего, это выражается подходами к организации собственной экономической безопасности. Самое большое различие между такими предприятиями выражается в заинтересованности максимизации прибыли и свободе действий на юридическом поле.

На государственном предприятии большинство механизмов и методов работы уже регламентированы законом и подлежат строгому контролю, более того финансирование таких предприятий происходит за счет бюджетных средств, поэтому данные виды предприятий мало заинтересованы в максимизации прибыли. Что касается организации экономической безопасности, то как уже было сказано выше все виды документов, принадлежащих к государственной тайне, служебной тайне, персональных данных прописаны и регламентированы законом, также законом регламентированы способы защиты и борьбы с внутрикорпоративным мошенничеством на государственных предприятиях.

Организации же, принадлежащие к статусу частные, более свободны в юридическом плане, данные предприятия могут использовать законодательство по организации экономической безопасности не более как рекомендации, разрабатывать конкретные механизмы, предназначенные только для одного предприятия они могут сами. Но что касается непосредственно защиты, то частные предприятия более заинтересованы в максимизации прибыли, потому как являются автономными, именно поэтому таким предприятиям сложнее организовать собственную экономическую безопасность. Так если на государственном предприятии финансирование чаще всего стабильное, то на частном все зависит от прибыли и убытков, которые предприятие понесло, но как показывает практика большой процент убытков приходится именно на мошенничество со стороны сотрудников частных компаний.

Список публикаций магистранта

1) Засорин И. А., Данков А. Г. Информационное развитие регионов России // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов Международной научной конференции/ Под ред. О.Г. Берестневой, О.М. Гергет. В 2-х частях, Томск, 29 Апреля-2 Мая 2014. - Томск: Изд-во ТПУ, 2014 - Т. 2 - С. 316-318

2) Засорин И. А., Данков А. Г. Информационные технологии как инструмент управления предприятием // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов Международной научной конференции/ Под ред. О.Г. Берестневой, О.М. Гергет. В 2-х частях, Томск, 29 Апреля-2 Мая 2014. - Томск: Изд-во ТПУ, 2014 - Т. 2 - С. 92-94

3) Засорин И. А., Данков А. Г. Современные методы управления проектами. XII Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых.

4) Засорин И. А., Данков А. Г. Инновационно – инвестиционная деятельность предприятий опк с точки зрения проектного подхода. Межрегиональный сборник научных трудов "проблемы управления рыночной экономикой", Выпуск 16, ТОМ 2. Томск 2015. ТПУ.

5) Засорин И. А., Данков А. Г. Управления проектами оборонно-промышленного комплекса. XII Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых. 17-21 ноября 2015 г., г. Томск, НИ ТПУ.

6) Засорин И. А., Данков А. Г. Российско – китайское инновационное сотрудничество в XXI веке, как проводник мягкой силы КНР. Международная молодежная конференция «КНР – Роль и место в международной системе научно – технологического сотрудничества» Томск, 19 – 21 Ноября 2015. ТГУ.

7) Засорин И. А., Данков А. Г. Обеспечение экономической безопасности при развитии деловых контактов с компаниями КНР.

Международная молодежная конференция «Российско – китайские отношения: сибирский аспект.» Томск, 01 – 02 Декабря 2016. ТГУ.

Список используемых источников

1) Балкова К.М. Особенности формирования службы экономической безопасности предприятия / К.М. Балкова // Экономика и предпринимательство. - 2014. - № 11. - С. 812-814.

2) Бекряшев А. К., Белозеров И. П., Бекряшева Н. С., Леонов И. В. эл.учеб. Теневая экономика и экономическая преступность / Омск – 2012, www.osi.ru

3) Белокур, В.В. Угрозы экономической безопасности предприятия [Текст]: учебник / под ред. В.В. Белокура - М.: 2012. - 290 с.

4) Бурыкин А.Д., Наседкин А.Л. Финансовый анализ предприятия - основа его экономической безопасности // Бухгалтерский учет. 2012. N 10.

5) В.А. Гадышев, О.Г. Поскочинова классификация угроз экономической безопасности предприятия [электронный ресурс] — Режим доступа. — URL: http://vestnik.igps.ru/wp-content/uploads/V32/6.pdf

6) Васильев Г.А., Халикова Э.А. экономическая безопасность предприятия в современных условиях // Экономика и современный менеджмент: VIII международная научно – практическая конференция – Новосибирск: СибАК, 2012. [электронный ресурс] — Режим доступа. — URL: https://sibac.info/conf/econom/viii/25849

7) Волкова, М.Н. Функциональные направления службы безопасности предприятия / М.Н. Волкова, Д.С. Иванников // Социально-экономические науки и гуманитарные исследования. - 2015. - № 4. - С. 144-147.

8) Гапоненко В.Ф. Экономическая безопасность предприятия: подходы и принципы. М: «Ось-89», 2012. - 208 с.

9) Горбачев, Д.В. Комплексный подход к организации деятельности службы экономической безопасности предприятия / Д.В. Горбачев, М.В. Кононова // Интеллект. Инновации. Инвестиции. - 2014. - № 1. - С. 165-170.

10) Доценко, Д.В. Экономическая безопасность: методологические аспекты и составляющие / Д.В. Доценко // Аудит финансовый анализ. - 2012. - № 4. - С.45-50.

11) Забродский В., Капустин Н. Теоретические основы оценки экономической безопасности отрасли и фирмы // Бизнес-информ. – 2012. – №24

12) Ильяшенко С.Н. Составляющие экономической безопасности кооператива и подходы к их оценке // Актуальные проблемы экономики. – 2013. - № 3. – с. 12-19

13) Кабанов А. А., Бончук Г. И. Внутренние и внешние угрозы экономической безопасности предприятия // Вестник Санкт-Петербургского университета МВД России. 2012. №1. URL: http://cyberleninka.ru/article/n/vnutrennie-i-vneshnie-ugrozy-ekonomicheskoy-bezopasnosti-predpriyatiya (дата обращения: 06.04.2017).

14) Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения / А.В. Козаченко, В.П. Пономарев, А.Н. Ляшенко. Киев: Издательство: Либра, 2013. — 280 с.

15) Козаченко А.В., Пономарев В.П. Методические основы оценки уровня экономической безопасности предприятия //Региональные перспективы -2012, №3.

16) Колпаков П.А. Система экономической безопасности фирмы // Экономика и менеджмент инновационных технологий. 2013. № 1 [Электронный ресурс]. URL: http://ekonomika.snauka.ru/2013/01/1567 (дата обращения: 19.11.2016).

17) Корелин Владимир Владимирович, Инструменты обеспечения экономической безопасности промышленного предприятия // Известия Санкт-Петербургского государственного экономического университета. 2016. №4 (100). URL: http://cyberleninka.ru/article/n/instrumenty-obespecheniya-ekonomicheskoy-bezopasnosti-promyshlennogo-predpriyatiya (дата обращения: 06.04.2017).

18) Лошаков А. П. Предпосылки формирования и сущность экономической безопасности предприятия // Вопросы экономических наук. – 2014. - № 5. – с. 87-89

19) Мак-Мак В.П. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности. – М.: Мир безопасности, 2016

20) Меркулова Е. Ю. Формирование индивидуальной финансовой нормативной модели управления экономической надежностью производственных систем // Социально-экономические явления и процессы. Тамбов, 2012. № 12.

21) Мусатаева М. О. Источники, виды и факторы угроз экономической безопасности, создание службы экономической безопасности // Научно-методический электронный журнал «Концепт». – 2015. – Т. 23. – С. 26–30. – URL: http://e-koncept.ru/2015/95250.htm.

22) П.Э. Шлендер. Безопасность жизнедеятельности предприятий: Учеб. пособие. 2-е изд., перераб. и доп. — М.: Вузовский учебник, - 304 с. 2012

23) Парамонов П.Ф. Экономика предприятий. 4.II: Учебное пособие. 2012

24) Понятие экономической безопасности [электронный ресурс] — Режим доступа. — URL: http://www.superinf.ru/view_helpstud.php?id=543

25) Российский обзор экономических преступлений за 2016 год // – [Электронный ресурс]. – Режим доступа: URL: http://www.pwc.ru/ru/forensic-services/publications/resc-2016.html (Дата обращения 06.01.2016 г.).

26) Саламова С.С. Теоретические подходы к обеспечению экономической безопасности предприятия / Т.А. Волкова, М.Н. Волкова, Н.В. Плужникова, С.С. Саламова // ФЭС: Финансы. Экономика. Стратегия – 2015. - №3. – С.29-32.

27) Светлаков А.Г. Журнал «Экономическая безопасность России» № 5 2015 г. с.150

28) Светлаков А.Г. Стратегия развития предприятий в условиях непредсказуемости внешней среды, Перм, 2016, с. 164

29) Светлаков А.Г. Экономическая безопасность АПК, Учебное пособие, Пермь, 2014, с. 218

30) Современные тенденции управления развитием организационно-экономических систем под редакцией проф. Тимиргалеевой Р.Р. - Симферополь, 2014.

31) Суглобов, А. Е. Экономическая безопасность предприятия: учебное пособие / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. - М.: ЮНИТИ, 2013. - 271 с.

32) Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура проблемы // Вестник Московского гос. ун-та. Сер. «Экономика». – 2012. – №5.

33) Терехов. Экономическая безопасность предприятия как успешная составляющая современного бизнеса [электронный ресурс] — Режим доступа. — URL: http://bre.ru/security/22999.html.

34) Трофимова Л.Н. Экономическая безопасность эффективности деятельности организаций торговли: ситуационно-характеристические параметры. Российское предпринимательство, № 11 (209) /июнь 2012.

35) Фокина Н.П. Экономика предпринимательства – важнейшая составляющая финансовой устойчивости // Актуальные проблемы экономики. – 2012.-№ 8.

36) Шаваев А.Г. Безопасность корпораций. Криминологические, уголовно-правовые и организационные проблемы. – М.: «Банковский Деловой Центр», 2012, с. 42

37) Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. – СПб: «Алетейя», 2015, с. 59

38) Шумпетер Й. Теория экономического развития. – М., 2016. С.159

Приложение А (обязательное)

Part 1

Theoretical basis of economic security in the enterprise

Студент:

Группа	ФИО	Подпись	Дата
3АМ5Б	Засорин Иван Александрович		

Консультант кафедры менеджмента:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Данков Артем Георгиевич	к.и.н.		

Консультант – лингвист кафедры иностранных языков ИСГТ:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ст. преподаватель	Гаспарян Гаянэ Арамаисовна			

1 Theoretical basis of economic security in the enterprise

1.1 Economic security, basic definitions

Strange as it may seem, official documents of the Russian Federation lack the concept of economic security of an enterprise (organization, legal entity). Therefore, we give several opinions of the authors of books on the economic security of enterprises.

According to E.A. Oleynikov, "the economic security of an enterprise is the state of the most effective use of corporate resources to prevent threats and to ensure the stable functioning of the enterprise now and in the future." In another work, The Business Strategy, prepared for publication by the Institute for Strategic Analysis and Enterprise Development, it is said that "the economic security of an enterprise is a state of the economic entity in which the vital components of the structure and activity of the enterprise are characterized by a high degree of protection from undesirable Changes "[3,2].

N.V. Matveyev suggests the following definition of the economic security of the enterprise: "this is the state of the enterprise, which ensures the stability of its functioning, the financial balance and regular extraction of profits, the ability to fulfill the set goals and objectives, the ability to further development and improvement."

In the literature, there are other very close to the quoted definitions of the economic security of the enterprise. For example, "economic security is the state of the most effective use of all types of resources in order to prevent (neutralize, eliminate) threats and ensure the stable operation of an enterprise in a market economy".

In the opinion of O.V. Klimochkina, the economic security of the enterprise (firm, corporation) is "a state of protection of its vital interests in the financial-economic, industrial-economic, technological spheres from various kinds of threats, primarily the social and economic plan that comes due to the management and staff

System of legal, organizational, socio-economic and engineering-technical measures "[2].

Analyzing the conceptual apparatus, in our view, most fully reflects and reveals the essence of the interpretation of "economic security" the following definition: "the economic security of an enterprise is to ensure the protection of the vital interests of the enterprise from internal and external threats, organized by the administration and the collective of the enterprise through the implementation of a system of legal measures , Economic, organizational, engineering, technical and socio-psychological nature ".

The goal of ensuring the economic security of an enterprise is to protect its property and employees from sources of external and internal security threats, to prevent the causes and conditions that give rise to them [11].

1.3 Threats to economic security

For each enterprise, economic threats are purely individual and depend on a number of factors (industry, enterprise scale, scope of activities, etc.), all threats are divided into two categories "external" and "internal". At the same time, in our opinion, these categories include separate elements that are acceptable to almost any business entity. For a more convenient perception of external and internal threats, we combined them into a table [5].

Table 1 – external and internal threats to the economic security of the enterprise

Externalthreats	**Internalthreats**
Active participation of representatives of government and management in commercial activities.	Actions or omissions (including intentional and unintentional) of employees of the enterprise, contrary to the interests of its commercial activities, the consequence of which may be causing economic damage to the Enterprise.
Use of criminal structures to influence competitors.	Leakage or loss of information resources (including information constituting commercial secrets and / or confidential information).
Absence of laws that allow counteracting unfair competition in full.	Undermining business image in business circles.

The absence in the country of favorable conditions for scientific and technical research.	The emergence of problems in the relationship with real and potential partners (up to the loss of important contracts).
Lack of detailed and objective information about business entities and their financial situation.	Conflict situations with representatives of the criminal environment, competitors, controlling and law enforcement agencies, occupational traumatism or death of personnel, etc.
Lack of culture of doing business in an entrepreneurial environment.	

As a positive influence of the external environment, it is necessary to consider technical and managerial innovations that have a complex impact on the activities of the whole enterprise. An enterprise can accept these innovations for implementation, or may ignore them, but the need to take into account innovations is dictated by a number of objective reasons. As a result of innovative processes, new ways and means of production are emerging. This objectively determines the need for active intervention of enterprises in innovative processes, a critical analysis of the possible means and methods of manufacturing the same type of products. But this is only one side of the matter. The second is the variety of forms of organization of production and labor, ways to improve production efficiency. The need to take into account the emerging innovations in the field of production technology and in the organization of production and management is due, for at least two reasons, namely: the ability to reduce production costs and thereby increase profits and gain competitive advantages in the market; expand the occupied market segment or enter new markets. In the end, both the first and the second directions should lead to an increase in the company's profit, strengthening its competitive positions in the market and increasing the level of economic security [5].

It should be noted that today not all managers of enterprises are ready to fully appreciate the need to create a reliable system of economic security. Especially it is difficult to determine the specific actions necessary to protect certain vital resources. Consequently, many managers are limited to creating security structures at the enterprise, almost completely, excluding organizational, technical and legal methods, means and methods of protecting information from the arsenal.

Measures to ensure the safety of information in a separate enterprise can be different in scale and form and depend on the production, financial and other capabilities of the enterprise, on the number and quality of protected secrets. In this case, the choice of such measures must be carried out on the basis of the principle of reasonable sufficiency, adhering to the "golden mean" in financial calculations, because excessive information closure, as well as negligent attitude to its preservation, can cause loss of a certain share of profit or lead to serious losses.

The procedure for protecting the vital resources of an enterprise implies, first, that it is necessary to classify all the risk factors that may occur during the activity of the enterprise. Thus, all risk factors, hazards and threats can be grouped according to the following classification criteria:

1) Whenever possible, forecast:

– Projected - arising under certain circumstances, identified from past experience and summarized by industry science and enshrined in laws, standards, guidance technical materials and other regulatory documents;

– Unpredictable - force majeure circumstances, technological achievements and discoveries, and other, inevitable, in essence.

2) By source of origin:

– objective arise without participation and in addition to the will of the subjects of the system - the state of the market situation, technological achievements and discoveries, force majeure circumstances, etc .;

– Subjective - deliberate or unintentional actions of people, authorities and state organizations, competition, crime and others, affecting the economic relations of an enterprise in the market.

3) If possible, prevent:

– Unforeseen is characterized by the insurmountability of the impact (natural disasters, technogenic catastrophes, wars, epidemics that force to decide and act contrary to intentions) and represent a particular complexity of prevention by budgetary means;

– Preventable can be envisaged at the planning stage of business, processes and technologies to minimize or completely prevent possible damage in case of risk factor implementation.

4) On the probability of an offensive:

– Obvious, conditioned by market (economic and legal) laws;

– Latent - implicit, temporarily hidden and difficult to detect. Their manifestation or non-manifestation may be due to economic conjuncture, the effect of macroeconomic phenomena, as well as competition and ways of conducting it. The suddenness of their manifestation can be subjective and difficult to predict even with a certain probability of occurrence.

5) By the nature of their occurrence:

– Economic - market (market) changes;

– Political - the change of power, the imposition of embargoes;

– Legal - legislative regulation of activities, licensing, customs;

– Technogenic - accidents and disasters, depletion of resources;

– Environmental - depletion of resources, climate change;

– Competitive - "black" PR, unfair competition;

– Counterparties - default, fraud;

6) Significance or significance of the damage:

– Insignificant - do not affect the market state of companies;

– Significant - loss of a significant part of the material and financial resources;

– Significant - loss of competitive advantages, possibly bankruptcy;

– Catastrophic - it is impossible to continue economic activities, inevitable bankruptcy.

7) By probability:

– Incredible - with extremely low probability of coincidence of the circumstances of the threat;

– Unlikely - do not require the planning of preventive measures as a form of force majeure;

– Probable - poorly projected, requiring planning depending on the significance of the damage;

– Very likely - projected, planned and secured by the budget;

– Inevitable - easily predictable, nature-related occurrences planned and provided by the budget.

8) On the basis of their implementation in time:

– direct - with a certain probability of implementation;

– close (up to 1 year) - projected and planned;

– far (over 1 year) - is not provided for by the current budget.

9) On the basis of their implementation in space:

– On the territory of the enterprise;

– On the territory adjacent to the enterprise;

– On the territory of the region;

– On the territory of the country;

– On foreign territory.

10) By the methods of implementation:

– Industrial espionage;

– Theft;

– Recruitment and bribery of personnel;

– Psychological impact on staff;

– Technological access;

– Others.

11) On the sphere of origin:

– Internal factors are related to the economic activities of the enterprise and its personnel. They are conditioned by business processes and affecting the results of economic activity - the form and quality of enterprise management,

compliance with technology, the organization of labor and the social sphere of personnel, and many others;

– External arise outside the enterprise, related to the market situation and the environment of the enterprise, the change of which can lead to damage - socio-economic, political, legal, technological, forensic and others [7].

Actions, defined as threats, are deliberately aimed at obtaining some benefit from the economic destabilization of the enterprise, from encroachments on its economic security.

The activities of the company's management, in spite of the risky nature, generally correspond to the current legislation. Threats, as a rule, involve violation of legislative norms (in this or that branch of law - civil, administrative, criminal) and presume a certain responsibility of the persons who implement them. Threats to the economic security of entrepreneurial activity are characterized by three characteristics:

– A conscious and self-serving nature;

– The direction of actions to inflict damage on the business entity;

– Illegal nature.

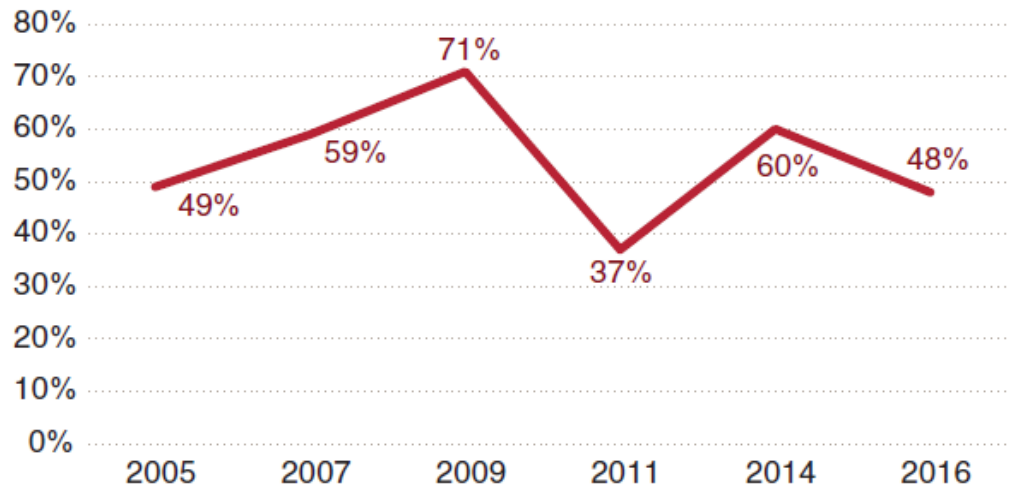
As already mentioned above, all threats can be divided into external and internal ones. It follows that actions considered as threats can also be divided into internal and external. External may include, for example, embezzlement of material assets and values by persons who do not work at a given enterprise, industrial espionage, illegal actions of competitors, and extortion from criminal structures. Internal threats include the disclosure of confidential information by own employees, low qualification of specialists who develop business documents (contracts), ineffective work of the economic security service and those responsible for checking counterparties. The greatest danger, as a rule, is external threats, since internal threats are often the implementation of external "orders".

According to statistics, 81.7 percent of threats are committed either by the personnel of the enterprise itself, or by direct or indirect involvement (internal

threats); 17.3 percent are external threats or criminal actions; 1 percent - threats from random persons [4].

But despite the difficult economic environment both on the external and internal markets of Russia, according to the Ministry of Internal Affairs (MVD) in 2016, compared to January-December 2015, the number of economic crimes identified by law enforcement agencies decreased by 3.3 percent Bodies. In total, 108.8 thousand crimes of this category were identified; the share of these crimes in the total number of registered crimes was 5.0 percent. The material damage from these crimes (on completed and suspended criminal cases) amounted to 397.98 billion rubles. Grave and especially serious crimes, in the total number of identified economic crimes, accounted for 59.9 percent. Departments of internal affairs bodies revealed 93.5 thousand crimes of economic orientation, their share in the general array of economic crimes amounted to 86.0 percent.

It should also be noted that according to the Russian Economic Crime Survey for 2016, almost half of all companies and organizations (48 percent) have faced economic crimes in the last two years. However, this is significantly lower than the result in 2014, when the corresponding figure was 60 percent. Nevertheless, the level of economic crime in Russia remains higher than the world average (36 percent), as well as above the results for the "big seven of the developing countries" (29 percent) and the countries of Eastern Europe (33 percent). It should be noted that of those who faced economic crimes in the last two years, 33 percent recorded more than 10 cases of fraud. [39].



Drawing 1 – The level of economic crime in Russia

The decline in the level of economic crime in Russia can be explained by several reasons. First, many enterprise managers testify to the strengthening of the role of the internal audit function, as well as the improvement of other fraud detection mechanisms. Practice shows that enterprises that have developed mechanisms for identifying illegal actions and implemented fraud risk management programs are better prepared to identify and prevent fraud. Secondly, recently in Russia there have been major changes in the field of combating corruption, including legislative initiatives aimed at applying international best practices.

In Russia, the most common type of economic crime is the misappropriation of assets. For example, 72 percent of managers in Russia whose enterprises are facing economic crimes have become victims of misappropriation of assets. It is not surprising that the misappropriation of assets prevails over other types of economic crimes. As a rule, it is easier to identify, because this type of fraud is not as complex as bribery and corruption or cybercrime.

Fraud in the procurement of goods and services was noted by 33 percent of executives, which puts him in second place among the economic crimes most often faced by enterprises in Russia. It is worth noting that the number of leaders in Russia, who indicated this type of economic crime among the most common, is 10% more than the average value all over the world. In our opinion, this type of fraud is a

double threat, since it has a negative impact on both the commercial and public sectors.

In Russia, the number of executives who noted bribery and corruption is more than the average worldwide (30 percent and 24 percent respectively). However, compared to two years earlier, the number of responses that indicated bribery and corruption was significantly reduced from 58 percent in 2014 to 30 percent in 2016.

Cybercrime was indicated in 32 percent of responses. As a result, they ranked second among the types of fraud most often encountered by enterprises. At the same time, the number of leaders in Russia who reported cybercrime in their responses was less (23 percent), and compared to 2014, the situation changed insignificantly - two years ago, such managers were 25 percent. It must be remembered that a significant percentage of those who did not indicate in their cybercrime responses may have suffered from this type of fraud even without knowing it. [39].

It should be understood that any economic crime, regardless of the severity of the commission, can have a negative impact on the enterprise both in the short and long term.

The long - term results of the operation are significantly affected by indirect damage, which includes a wide range of consequences: suspension of activities, investigative and preventive measures, measures to eliminate the causes of violations and, most importantly, damage to the moral and psychological climate in the enterprise and its business reputation. In Russia, 50 percent of enterprises that faced economic crimes in the last two years noted that unlawful actions had a significant negative impact on the moral and psychological climate in the enterprise. At the same time, managers in Russia are less concerned about the negative impact of economic crimes on relations with business partners (35 percent) and on reputation / image (34 percent).

There are many motives for committing economic crimes. Most often, the three most common factors that cause fraud (the so-called "Triangle of fraud"): the possibility or ability to commit an economic crime; A certain motivation or external pressure; and the ability to justify a perfect economic crime self-justification.

In Russia, the ability or ability to commit a crime remains the most significant factor in the opinion of leaders (84 percent). Its significance has increased by 8 percent compared to 2014. Motivation or external pressure, as well as the ability to justify a committed economic crime / self-justification, are at the same level of importance (8 percent) [39].

The tendency to increase the share of this factor is worrying. This means that companies should minimize such "loopholes". To do this, a proactive approach must be used to ensure effective management of the significant risks of fraud, using mechanisms to detect and prevent illegal actions.

Continuing to analyze statistical data, it can be noted that most often internal threats are committed by people who are well aware of all the intricacies and nuances of the enterprise, as well as having access to information about financial transactions of the enterprise. As practice shows such people almost always turn out to be the heads of internal structural units and their closest deputies.

When performing any actions that are threatening, such as:

- Misuse of material values;
- Theft, theft;
- Intra-firm fraud.

First of all there is a psychological factor of what is not because it needs to be done, but simply because it can be done, as well as lobbying for one's own interests, the purpose of which is "dishonest" enrichment.

1.4 Tools for economic security.

One of the most significant elements of the economic security of an enterprise its support tools, which are a set of legislative acts, legal norms, incentives and incentives, methods, measures, forces and means that help to achieve security objectives and accomplish the tasks. It should also be noted that for each individual enterprise providing its economic safety the list of tools would be highly individual.

As practice shows, the majority of Russian enterprises use those tools and methods that have proved themselves in the international practice of intracorporate fraud.

Turning to the statistics for the last two years, that the internal audit services and security services of companies are the first to identify the majority of economic crimes (20 percent and 15 percent respectively) [37].

The management of the enterprise, determining the nature of measures and instruments, ensuring economic security must proceed from the specifics of the scope and scope of the enterprise's activities, the objects to be protected, take into account the possibilities of material and technical and financial security measures, thus forming the system. All units of the system are fully created only by large enterprises. Small businesses are limited to internal security groups, consisting of security guards and personnel involved in setting up and repairing technical protection equipment.

A systematic approach to the formation and provision of economic security of the enterprise assumes that it is necessary to take into account all the real conditions of its activity, and the system itself must have clearly delineated elements, a scheme of their action and interaction. The system of economic security of the enterprise consists of several blocks, the simultaneous operation of which is designed to provide a sufficient profit for the expanded reproduction of the enterprise's capital, obtained as a result of observing the interests of the enterprise, i.e. As a result of the interaction of the enterprise with the subjects of the external environment. The system of ensuring the economic security of an enterprise can have a different degree of structuring and formalization.

The system of ensuring the economic security of the enterprise is designed to organize the organizational interaction of the enterprise with the subjects of the external and internal environment. The result of the functioning of this system is the receipt of resources and information necessary for the organization of production in accordance with the system of priority interests of the enterprise, minimizing the costs of acquiring resources in the required quantity and of proper quality.

The main purpose of the enterprise's economic security system is to create and implement conditions that ensure the economic security of the enterprise. These conditions are determined based on the criterion of economic security and its level. The operation of the system should be aimed at ensuring economic security in the activities of the enterprise, both now and in the future.

The conditions for ensuring the economic security of an enterprise can not be viewed in isolation, they are closely interrelated. Realization of conditions for ensuring the economic security of an enterprise is possible either with the use of measures of an organizational nature, which, as a rule, do not need investment support (either it is insignificant) or with attraction of a certain volume of investments. In the first case, it is not a capital-intensive creation of conditions for ensuring the economic security of an enterprise; in the second case, the creation of conditions should be considered capital-intensive.

It is clear that in the event of a lack of profit, enterprises should first of all implement those conditions for ensuring their economic security, which do not require investment support. And only after the completion of non-capital-intensive measures to ensure economic security, enterprises must begin to implement conditions that require investment support.

The system of economic security of the enterprise and the mechanism for ensuring that the tasks of economic security are solved not only by a specially created subdivision, but with the active participation of all departments and services of the enterprise within the responsibility for security issues assigned to the heads of structural divisions.

Thus, the main role in ensuring the economic security of the enterprise belongs to its personnel, the human resources or resource is the main resource of the enterprise. Only it can make a profit, but at the same time, personnel is the source of all internal threats to economic security, and, ultimately, the success of any managerial innovation is the loyalty and motivation of employees.

Carrying out work to ensure the economic security of the enterprise, it is necessary to establish the correlation of threats from competitors, intruders and risks

arising in the course of the enterprise activity in time and in the space of threats. The threat space covers the object of protection - the personnel of the enterprise, property, financial resources, and information constituting a trade secret. Each threat entails a certain damage - moral or material, and opposition is designed to reduce its magnitude. Proceeding from this, when creating a system of economic security,it is necessary to rely on such a tool as a legal framework.

The legal basis for creating the Security Council is the Law of the Russian Federation "On Private Detective and Security Activities in the Russian Federation" of March 11, 1992, No. 2487-1, which provides that enterprises located on the territory of the Russian Federation, regardless of their organizational and legal forms, the right to establish detached units - security services for the implementation of security and detective activities in the interests of their own security.

The enterprise security service can perform the following functions:

1) Collection of information on civil cases on a contractual basis with the participants of the process;

2) Market research, information gathering for business negotiations, identification of non-creditworthy or unreliable business partners;

3) Establishment of the circumstances of unlawful use in business activities of brand names and names, unfair competition, as well as disclosure of information constituting commercial secret;

4) Identification of biographical and other personal data about individual citizens (with their written consent) when they conclude employment contracts;

5) Search for missing citizens;

6) Search for property lost by citizens or enterprises, institutions, organizations;

7) Collection of information on criminal cases on a contractual basis with the participants in the process;

8) Protection of life and health of citizens;

9) Protection of property of owners, including during its transportation;

10) Design, installation and maintenance of fire alarm systems;

11) Consulting and preparation of recommendations to clients on issues of lawful protection against unlawful attacks;

12) Armed protection of property owners, as well as the use of technical and other means that do not harm the life and health of citizens, and the environment, the means of operational radio and telephone communication [13, 16].

To ensure the protection of economic security of business activities, it is important to establish its own economic security service (hereinafter - SEB), which in turn will also be one of the tools to ensure economic security in the enterprise. It is possible to recommend a number of stages when creating the SEB:

1) Decision-making on the need for the establishment of the SEB. The question of creating a system of economic security should arise at the time of making a decision on the organization of the enterprise depending on the type of activity chosen by it, the volume of production expected to be produced, the amount of annual turnover and profit, the use of production secrets, the number of employees, etc. The founders must anticipate in advance the need to create a system of economic security.

2) After the state registration, the leaders make a final decision on the creation of the SEB. In case of a positive decision of the issue, the responsible person (group of persons) who will directly engage in the organization of the SEB is identified;

3) Definition of common tasks of SEB - threat prevention, response to emerging threats and identification of specific protection objects (personnel, information, computer systems, buildings and premises);

4) Development of the SEE regulation, definition of the structure and approval of the states;

5) Recruitment. Employees of the SEB may be people who are specially and permanently engaged in this activity as the main one, and attracted specialists (for example, chief accountant, lawyer, etc.).

6) Direct organization and functioning of the SEB.

When selecting permanent workers, the most important requirement is vocational training. In this regard, preference should be given to former law enforcement officials (the Ministry of Internal Affairs, the FSB, the prosecutor's office, the tax police), who have experience and are suitable for moral and business qualities for this activity. For the service of physical protection, it is more expedient to invite persons who have served in Special Forces, who possess professional skills in possession of weapons and hand-to-hand combat.

Thus, summing up a general result concerning instruments that ensure economic security, we can say that the system of economic security should be based on the following principles:

- Complexity and consistency;
- Timeliness;
- Legality;
- Economy;
- Continuity;
- Smoothness;
- Interactions.

The tools for ensuring the economic security of an enterprise should, in our opinion, encompass all the principles presented above. Proceeding from these principles,it is possible to single out the instruments of economic security, which are classified as follows:

1) Risk management (diversification, insurance, hedging, etc.)
2) Technical protection (security, information security, personnel policy);
3) Financial protection (financial monitoring, management accounting and control, budgeting).

Based on these principles and tools to ensure the economic security of the enterprise, it is possible to analyze the correspondence of already existing tools to theoretically justified principles. Based on the threats that the company identifies as

the most important, appropriate security tools are selected. In our opinion, it is inadvisable to use tools that cover only one or several principles [21].