ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РФ»
ВОЛГОГРАДСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ

**А. М. Цыбулин, В. М. Запрягайло,
И. И. Кулагина**

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ ПРОВЕРКИ БЕЗОПАСНОСТИ БИЗНЕСА

Учебно-методическое пособие

Волгоград 2017

УДК 004.056.5:338.22(075.8)
ББК 65.290.4я73
Ц 93

Рецензенты:

кандидат техн. наук ***С. А. Македонский***,
Главный специалист по информационной безопасности службы безопасности Волгоградского филиала «Акционерного банка «Россия»

кандидат техн. наук, доцент ***О. А. Астафурова***,
Волгоградского института управления – филиала ФГБОУ ВО РАНХиГС

Цыбулин А. М., Запрягайло В. М., Кулагина И. И.

Ц 93 Обеспечение комплексной проверки безопасности бизнеса: учебно-методическое пособие / А. М. Цыбулин, В. М. Запрягайло, И. И. Кулагина; Волгоградский институт управления – филиал ФГБОУ ВО РАНХиГС. – Волгоград: Издательство Волгоградского института управления – филиала РАНХиГС, 2017. – 1 электрон. опт. диск (CD-ROM). – Систем. требования: IBM PC с процессором 486; ОЗУ 64 Мб; CD-ROM дисковод; Adobe Reader 6.0. – Загл. с экрана.

Пособие содержит основные сведения по теоретическим и практическим аспектам обеспечения комплексной проверки безопасности бизнеса. В пособии изложены положения для формирования практических навыков по оценке рисков экономической и информационной безопасности, по работе с системами профессионального анализа контрагентов «СПАРК-Интерфакс», «Контур-Фокус», «СПАРК-Маркетинг», «1СПАРК-Риски».

Для студентов и слушателей высших учебных заведений экономических специальностей.

ISBN 978-5-7786-0683-8

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Дисциплина Б1.Б.32 «Обеспечение комплексной проверки безопасности бизнеса» обеспечивает овладение студентами по специальности 38.05.01 «Экономическая безопасность» общей профессиональной компетенцией «Способность применять инструменты и механизмы нейтрализации и предотвращения экономических угроз в деятельности хозяйствующих субъектов».

Профессиональный стандарт «Специалист по управлению рисками», утв. приказом Министерства труда и социальной защиты РФ от 07 сентября 2015 г. N 591н, требует от специалиста обеспечение эффективной работы системы управления рисками/ разработка системы управления рисками.

Для достижения этой цели у обучающихся должны быть сформированы соответствующие знания, умения и навыки.

На уровне знаний:

дать определение следующим понятиям: аудит безопасности фирмы, разведывательный цикл, аналитические методы деловой разведки, контрразведовательный цикл в сфере конкуренции, этап предотвращения, этап обнаружения, этап “наказания” разведки, система профессионального анализа рынков и компаний (СПАРК), СПАРК-Маркетинг, Web-сервис Контур.Фокус – быстрая проверка контрагента, ИАС «Seldon.Basis».

На уровне умений:

уметь реализовать этапы предотвращения, обнаружения и нейтрализации экономических угроз;

уметь организовать быструю проверку контрагента.

На уровне навыков:

владеть навыками практической работы в системе СПАРК, Web-сервис Контур.Фокус.

Учебная дисциплина Б1.Б.32 «Обеспечение комплексной проверки безопасности бизнеса» входит в Блок 1 «Базовая часть», обязательные дисциплины

учебного плана. Дисциплина общим объемом 108 часов (3 ЗЕТ) изучается в течение одного семестра. На очной форме дисциплина осваивается в 6 семестре, на заочной форме – на 5 курсе.

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний в области информационных систем в экономике, а также на приобретенные ранее умения и навыки в сфере экономической безопасности.

Для успешного овладения дисциплиной студенту необходимо использовать знания и навыки, полученные им при изучении дисциплины Б1.Б.23 «Экономическая безопасность».

Знания, полученные в ходе изучения дисциплины «Обеспечение комплексной проверки безопасности бизнеса» могут быть полезны при изучении такой дисциплины, как Б1.Б.37 «Диагностика финансовой безопасности экономического субъекта».

Настоящее учебно-методическое пособие имеет практическую направленность: одновременно с усвоением теоретического материала студентам будет предоставлен доступ к информационно-аналитическим ресурсам, в рамках практических занятий они смогут самостоятельно оценить возможности и преимущества указанных информационных массивов, получить навыки работы с этими системами.

Для успешного освоения учебного материала занятия построены по следующей схеме:

- Изучение теоретических вопросов;
- Практическая работа – решение проблемы с использованием общедоступных интернет-источников информации;
- Практическая работа – решение проблемы с использованием информационно-аналитических систем «СПАРК-Интерфакс», «Контур-Фокус», «СКАН-Интерфакс» и «СПАРК-Маркетинг».

1. О СТРАТЕГИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Президент Путин утвердил стратегию экономической безопасности РФ до 2030 года, в которой фактически впервые говорится о суверенизации российской экономики как о стратегической цели.

Документ включает 5 глав, каждая глава содержит несколько статей. Всего в стратегии 38 статей.

Предполагается, что реализация Стратегии будет осуществляться в два этапа: на I-м этапе (до 2019 года) – разработка и реализация мер организационного, нормативно-правового и методического характера в целях, обеспечения экономической безопасности, совершенствования механизмов мониторинга и оценки ее состояния; на II-м этапе (до 2030 года) – выполнение мер по нейтрализации вызовов и угроз экономической безопасности.

Согласно указу, правительству поручено разработать в течение трех месяцев меры по реализации стратегии, которая направлена на:

— обеспечение противодействия вызовам и угрозам экономической безопасности;

— предотвращение кризисных явлений в ресурсно-сырьевой, производственной, научно-технологической и финансовой сферах;

— недопущение снижения качества жизни населения.

1.1. В настоящей Стратегии используются следующие основные понятия:

— «экономическая безопасность» – состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условий для реализации стратегических национальных приоритетов РФ;

— «экономический суверенитет РФ» – объективно существующая независимость государства в проведении внутренней и внешней экономической политики с учетом международных обязательств;

— «национальные интересы» РФ в экономической сфере- объективно значимые экономические потребности страны, удовлетворение которых обеспечивает реализацию стратегических национальных приоритетов РФ;

—«угроза экономической безопасности» – совокупность условий и факторов, создающих прямую или косвенную возможность нанесение ущерба национальным интересам РФ в экономической сфере;

—«вызовы экономической безопасности» – совокупность факторов, способных при определенных условиях привести возникновению угрозы экономической безопасности;

—«риск в области экономической безопасности» – возможность нанесения ущерба национальным интересам РФ в экономической сфере в связи с реализацией угрозы экономической безопасности;

—«обеспечение экономической безопасности» – реализация органами государственной власти, органами местного самоуправления и Центрального банка РФ во взаимодействии с институтами гражданского общества комплекса политических, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие вызовам и угрозам экономической безопасности и защиту национальных интересов РФ в экономической сфере.

1.2. Основные угрозы экономической безопасности

Документ определяет основные угрозы экономической безопасности, к которым относятся:

— стремление развитых государств использовать свои преимущества, в том числе информационные технологии, в качестве инструмента глобальной конкуренции;

— рост частной и суверенной задолженности, разрыв между стоимостной оценкой реальных активов и производственных ценных бумаг;

— ограничения доступа к международным финансовым ресурсам и современным технологиям;

— колебания на мировых товарных и финансовых рынках;

— изменения структуры мирового спроса на энергоресурсы и развитие «зеленых» технологий;

— создание межгосударственных экономических объединений без участия РФ;

— уязвимость финансово-банковской системы;

— исчерпание экспортно-сырьевой модели экономического развития;

— отсутствие российских несырьевых компаний среди глобальных лидеров мировой экономики;

— недостаточный объем инвестиций в реальный сектор экономики;

— отставание в сфере передовых технологий;

— исчерпание действующих месторождений;

— низкая конкурентоспособность российского несырьевого экспорта;

— недостаточное развитие транспортной и энергетической инфраструктуры;

— несбалансированность национальной бюджетной системы;

— сохранение значительной доли теневой экономики;

— недостаточно эффективное госуправление;

— высокий уровень криминализации и коррупция в экономической сфере;

— недостаточность трудовых ресурсов и т.д.

1.3. Основные направления государственной политики в сфере обеспечения экономической безопасности.

Определены основные направления государственной политики в сфере обеспечения экономической безопасности:

— развитие системы госуправления, прогнозирования и стратегического планирования

— обеспечение устойчивого роста реального сектора экономики

— разработка и внедрение современных технологий, стимулирование инновационного развития

— развитие национальной финансовой системы

— укрепление единства экономического пространства РФ

— повышение эффективности внешнеэкономического сотрудничества

— обеспечение безопасности экономической деятельности

— развитие человеческого потенциала.

1.4. Этапы реализации экономической стратегии

Стратегия будет реализовываться в два этапа:

— первый этап (до 2019 года). Разработка и реализация мер в целях обеспечения экономической безопасности, совершенствование механизмов мониторинга

— второй этап (до 2030 года). Выполнение мер по нейтрализации вызовов и угроз экономической безопасности.

Вопросы для самоподготовки

1. Основные понятия, которые используются в настоящей Стратегии.
2. Основные угрозы экономической безопасности.
3. Цели, основные направления и задачи государственной политики в сфере обеспечения экономической безопасности.
4. Основные задачи по реализации направления, обеспечения безопасности экономической деятельности.
5. Оценка состояния экономической безопасности.
6. Основные задачи системы управления рисками.
7. Показатели состояния экономической безопасности.
8. Основные направления государственной политики в сфере обеспечения экономической безопасности
9. Функции и полномочия по осуществлению мониторинга и оценки состояния экономической безопасности.

Литература

1. Указ Президента РФ от 13 мая 2017 г. № 208 “О Стратегии экономической безопасности Российской Федерации на период до 2030 года”. ГАРАНТ.РУ: http://www.garant.ru/products/ipo/prime/doc/71572608/ #ixzz4wuKM9Lm3

2. АНАЛИЗ ПОЛОЖЕНИЙ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Анализ положений Доктрины информационной безопасности Российской Федерации, введенной Указом Президента РФ от 05.12.2016 № 646.

Доктрина отражает национальные интересы, официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности в Российской Федерации.

2.1. Определения и общие положения

В первый раздел новой Доктрины вошли основные понятия, применяемые в документе, которые в новой редакции стали полнее, шире и приобрели более структурированный вид. Доктрина основана на Конституции, федеральных законах и нормативных правовых актах, что подтверждают используемые в документах формулировки и термины.

а) «национальные интересы Российской Федерации в информационной сфере (далее – национальные интересы в информационной сфере) – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) угроза информационной безопасности Российской Федерации (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности».

2.2. Основные информационные угрозы и состояние информационной безопасности.

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, крими-

нальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

2.3. Состояние ИБ в экономической сфере.

Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

Стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

Вопросы для самоподготовки

1. Основные понятия, используемые в Доктрине;
2. Национальные интересы в информационной сфере;
3. Основные информационные угрозы и состояние информационной безопасности;
4. Стратегические цели и основные направления для обеспечения информационной безопасности;
5. Организационные основы обеспечения информационной безопасности.

Литература

1. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". Система ГАРАНТ: http://base.garant.ru/71556224/#friends#ixzz4x0uCVEwN

2. http://www.securitylab.ru/analytics/485289.php

---

3. ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БИЗНЕСА

3.1. Безопасность бизнеса – это набор мероприятий и мер, направленных на всестороннюю защиту предпринимательской деятельности от различных видов угроз (информационных, юридических, физических, экономических и организационно-кадровых). Все решения, касающиеся всесторонней охраны бизнеса и принимаемых мер, возлагаются на службу безопасности, руководителей соответствующих отделов и директора организации.

3.2. Виды проблем в безопасности бизнеса и пути их решения. В любом виде бизнеса всегда есть место для риска. При этом хороший руководитель не будет ждать проблем – он своевременно примет меры для защиты от наиболее вероятных проблем в сфере бизнеса. К таким можно отнести:

- корпоративные неурядицы – споры и конфликтные ситуации между акционерами компании, конфликты между топ менеджерами или сложности взаимоотношений между владельцами компании и руководителями подразделений;
- внешние опасности – угрозы со стороны криминальных структур, конфликты с правоохранительными и государственными структурами, рейдерские налеты и так далее;

● финансовые потери – мошеннические действия персонала (клиентов), кража, недобросовестные посредники или поставщики, нецелесообразное применение ресурсов компании, получение взяток за определенную деятельность против интересов компании;

● информационные опасности – утечка секретной информации компании (ее сокрытие или уничтожение), получение несанкционированного доступа к конфиденциальным данным, разглашение коммерческой тайны и тому подобное;

● охранные «прорехи» – кражи материально-технических ценностей посторонними лицами, несанкционированное проникновение на территорию компании, нарушение трудовой дисциплины;

● проблемы с репутацией – наличие в структуре работников, имеющих плохую репутацию, сотрудничество с людьми (контрагентами), имеющими плохую репутацию.

3.3. Информационная безопасность бизнеса. По статистики больше половины всех проблем бизнеса возникают по причине «пробелов» в информационной безопасности. Утечка информации к конкурентам, потеря данных, передача в чужие руки секретной информации компании – все это несет большой риск для бизнеса. В такой ситуации IT-менеджеры компании идут на ряд эффективных мер, обеспечивающих комплексную защиту компании.

На первом месте находится защита финансовых данных, на втором – защита от утечек, а на третьем – защита от DdoS-атак. И если первые два пункта уже давно в тройке лидеров, то проблема с атаками появилась лишь недавно. Причина такого интереса – возросшее число DdoS-атак на компании малого и среднего сегмента.

3.4. Основные методы информационной защиты бизнеса следующие:

Защита от вторжений – установка программ или оборудования, необходимого для контроля трафика в сети. При появлении первой же опасности

(вторжения) система реагирует и блокирует доступ. Одновременно с этим происходит оповещение ответственного сотрудника.

Защита от утечек – набор мер, позволяющих предотвратить попадание конфиденциальной информации в посторонние руки.

Защита файлов подразумевает сохранность всей наиболее важной информации, которая хранится на компьютерах и серверах внутри компании.

3.5. Экономическая безопасность бизнеса. Для обеспечения экономической безопасности необходимо выполнение следующих мер:

— Проверка компании-контрагента. В законе РФ нет пункта, который бы обязывал проводить проверку будущего партнера. С другой стороны, организация должна проявлять осмотрительность в этом вопросе и не совершать сделок с подозрительными структурами.

— Оптимизация налогов позволяет снизить затраты предприятия и возможные проблемы с органами налоговой инспекции. Лучшим решением может стать аутсорсинг.

— Защита компьютера с установленной системой «клиент-банка».

3.6. Организация физической безопасности бизнеса. Одна из наиболее важных задач для любой компании – защита от проникновения посторонних лиц на территорию объекта, контроль всех основных помещений предприятия, защита и обеспечение спокойствия работников организации, обеспечение защиты от пожара.

3.7. Правовая безопасность бизнеса. Обеспечение правовой безопасности – это один из способов защиты компании (фирмы, предприятия) от грубых юридических ошибок, которые могут повлечь за собой серьезные репутационные и финансовые потери.

3.8. Организационно-кадровая безопасность бизнеса. Обеспечение организационно-кадровой безопасности – это задача любого руководителя. Суть таких мероприятий – защита деятельности от вероятных угроз, вызванных человеческим фактором. Основные задачи – выявление и предупреждение мошеннических действий работников.

Вопросы для самоподготовки

1. Виды проблем в безопасности бизнеса и пути их решения.
2. Информационная безопасность бизнеса.
3. Основные методы информационной защиты бизнеса.
4. Экономическая безопасность бизнеса.
5. Организация физической безопасности бизнеса.
6. Правовая безопасность бизнеса.
7. Организационно-кадровая безопасность бизнеса.

Литература

1. Кузнецов И.Н., Бизнес-безопасность, 3-е изд. М.: ИТК «Дашков и К°», 2012, 416 с.

2. Электронное учебно-методическое пособие. Обеспечение безопасности персональных данных. ООО «Издательский Дом «Афина», 194017, Санкт-Петербург, пр. Мориса Тореза, д. 98, корп. 1.

3. Варфоломеев А.А. Основы информационной безопасности: Учеб. пособие. – М.: РУДН, 2008. – 412 с.: ил.

4. КОМПЛЕКСНАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИНИМАТЕЛЬСТВА

4.1. Объектом системы обеспечения экономической безопасности выступает стабильное экономическое состояние субъекта предпринимательской деятельности в текущем и перспективном периоде. Именно от объекта защиты во многом зависят основные характеристики системы обеспечения экономической безопасности. Комплексный подход предполагает учет в управлении объектом всех основных его аспектов и все элементы управляемой системы рассматриваются только в совокупности, целостности, единстве.

Комплексная система обеспечения экономической безопасности предпринимательства – это совокупность взаимосвязанных мероприятий организационно-правового характера, осуществляемых в целях защиты предпринимательской деятельности от реальных или потенциальных действий физических или юридических лиц, которые могут привести к существенным экономическим потерям.

4.2. Концепция комплексной системы обеспечения экономической безопасности предпринимательства. Концепция включает цель комплексной системы обеспечения безопасности, ее задачи, принципы деятельности, объект и субъект, стратегию и тактику.

Цель данной системы – минимизация внешних и внутренних угроз экономическому состоянию субъекта предпринимательства, в том числе его финансовым, материальным, информационным, кадровым ресурсам, на основе разработанного и реализуемого комплекса мероприятий экономико-правового и организационного характера. В процессе достижения поставленной цели осуществляется решение конкретных задач, объединяющих все направления обеспечения безопасности.

Задачи, решаемые системой обеспечения безопасности:

— прогнозирование возможных угроз экономической безопасности;

— организация деятельности по предупреждению возможных угроз (превентивные меры);

— выявление, анализ и оценка возникших реальных угроз экономической безопасности;

— принятие решений и организация деятельности по реагированию на возникшие угрозы;

— постоянное совершенствование системы обеспечения экономической безопасности предпринимательства.

Организация и функционирование комплексной системы обеспечения экономической безопасности предпринимательской деятельности в целях максимальной эффективности должны основываться на ряде следующих принципов:

— принцип законности. Вся деятельность фирмы, в том числе ее службы безопасности должна носить безусловно законный характер, иначе система обеспечения безопасности может быть разрушена по вине самого субъекта предпринимательства. В качестве негативных последствий могут быть различного рода санкции правоохранительных органов, привлечение в качестве ответчика в суд, шантаж со стороны криминальных структур;

— принцип экономической целесообразности. Следует организовывать защиту только тех объектов, затраты на защиту которых меньше, чем потери от реализации угроз этим объектам. Здесь также должны учитываться финансовые возможности фирмы по организации системы экономической безопасности;

— сочетание превентивных и реактивных мер. Превентивные – меры предупредительного характера, позволяющие не допустить возникновения или реализации угроз экономической безопасности. Реактивные – меры, которые предпринимаются в случае реального возникновения угроз или необходимости минимизации их негативных последствий;

— принцип непрерывности – предполагает, что функционирование комплексной системы обеспечения экономической безопасности предпринимательства должно осуществляться постоянно;

— принцип дифференцированности. Выбор мер по преодолению возникших угроз происходит в зависимости от характера угрозы и степени тяжести последствий ее реализации;

— координация. Для достижения поставленных задач необходимо постоянное согласование деятельности различных подразделений службы безопасности, самой фирмы и сочетание организационных, экономико-правовых и прочих способов защиты;

— полная подконтрольность системы обеспечения экономической безопасности руководству субъекта предпринимательской деятельности. Это необходимо, во-первых, для того, чтобы система безопасности не превратилась в замкнутое образование, ориентированное на решение узких задач, без учета интересов фирмы в целом, а во-вторых, для оценки эффективности деятельности системы и ее возможного совершенствования.

Объект и субъект системы обеспечения экономической безопасности предпринимательства тесно взаимосвязаны. Объектом системы в целом, как уже говорилось, выступает стабильное экономическое состояние субъекта предпринимательской деятельности в текущем и перспективном периоде. Конкретными же объектами защиты выступают ресурсы: финансовые, материальные, информационные, кадровые. Субъект системы обеспечения экономической безопасности предпринимательства носит более сложный характер, поскольку его деятельность обусловливается не только особенностями и характеристиками объекта, но и специфическими условиями внешней среды, которая окружает субъект предпринимательской деятельности. Исходя из этого, можно выделить две группы субъектов, обеспечивающих экономическую безопасность предпринимательства: внешние субъекты; внутренние субъекты.

К внешним субъектам относятся органы законодательной, исполнительной и судебной власти призванные обеспечивать безопасность всех без исклю-

чения законопослушных участников предпринимательских отношений; причем деятельность этих органов не может контролироваться самими предпринимателями. Эти органы формируют законодательную основу функционирования и защиты предпринимательской деятельности в различных ее аспектах и обеспечивают ее исполнение.

К внутренним субъектам относятся лица, непосредственно осуществляющие деятельность по защите экономической безопасности данного конкретного субъекта предпринимательства.

Субъекты, обеспечивающие экономическую безопасность предпринимательства, осуществляют свою деятельность на основе определенной стратегии и тактики.

Стратегия – это долгосрочный подход к достижению цели. Стратегия экономической безопасности включает, прежде всего, систему превентивных мер, реализуемая через регулярную, непрерывную, работу всех подразделений субъекта предпринимательской деятельности по проверке контрагентов, анализу предполагаемых сделок, экспертизе документов, выполнению правил работы с конфиденциальной информацией и т.п. Служба безопасности в этом случае выполняет роль контролера.

Тактика обеспечения безопасности предполагает применение конкретных процедур и выполнение конкретных действий в целях обеспечения экономической безопасности субъекта предпринимательства.

Основными функциями службы экономической безопасности фирмы являются следующие:

— организация и осуществление совместно с подразделениями фирмы защиты конфиденциальной информации;

— проверка сведений о попытках шантажа, провокаций и иных акций в отношении персонала, преследующих цель получения конфиденциальной информации о деятельности фирмы;

— организация сбора, накопления, автоматизированного учета и анализа информации по вопросам безопасности;

— проведение проверок в подразделениях фирмы и оказание им практической помощи по вопросам безопасности их деятельности;

— разработка и внедрение положения о коммерческой тайне;

— проверка правил ведения закрытого делопроизводства;

— проверка работников на предмет соблюдения правил обеспечения экономической, информационной и физической безопасности;

— оказание содействия отделу кадров по работе с персоналом в вопросах подбора, расстановки, служебного перемещения и обучения персонала;

— сбор, обработка, хранение, анализ информации о контрагентах с целью предотвращения сделок с недобросовестными партнерами;

— выполнение поручений руководства фирмы, входящих в компетенцию службы;

— взаимодействие с правоохранительными органами, проведение мероприятий по выявлению и предупреждению различного рода финансово-хозяйственных правонарушений;

— проведение служебных расследований по фактам разглашения конфиденциальной информации, потери служебных документов работниками фирмы и действий угрожающих экономической безопасности фирмы.

Вопросы для самоподготовки

1. Цель комплексной системы обеспечения экономической безопасности предпринимательства.
2. Задачи, решаемые системой обеспечения безопасности.
3. Организация и функционирование комплексной системы обеспечения.
4. Объект и субъект системы обеспечения экономической безопасности предпринимательства.
5. Стратегия экономической безопасности.
6. Тактика обеспечения безопасности.
7. Основные функции службы экономической безопасности фирмы.
8. Правовые основы создания службы безопасности.

9. Перечислить виды деятельности службы безопасности предпринимательской фирмы.

Литература

1. Уразгалиев В.Ш. Экономическая безопасность. Учебник и практикум для вузов. СПб.: Издательство «Юрайт», 2017.-374с.

2. Гапоненко В.Ф., Беспалько А.Л., Власов А.С. Экономическая безопасность предприятия. Подходы и принципы. М.: Издательство «Ось-89», 2007.-208с. www.zahvat.ru 33743.pdf

3. Суглобов А.В., Хмелев С.А., Орлова Е.А. Экономическая безопасность предприятия. М.: Издательство: Юнти-Дана, 2012.- 272с.

4. Экономическая безопасность предприятия. http://schooled.ru/economic/safety/index.htm

---

5. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ И ИНСТРУМЕНТАРИЙ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

5.1. Экономическая безопасность предприятия рассматривается с различных точек зрения:

– наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры предприятия его стратегическим целям и задачам;

– состояние наиболее эффективного использования корпоративных ресурсов для предотвращения угроз и для обеспечения стабильного функционирования предприятия в настоящее время и в будущем;

– 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;

– 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;

– состояние наиболее эффективного использования всех видов ресурсов в целях предотвращения (нейтрализации, ликвидации) угроз и обеспечения стабильного функционирования предприятия в условиях рыночной экономики ;

– состояние, при котором обеспечивается ее устойчивость при воздействии различного рода угроз, а также гарантируется ее развитие и способность к самосохранению и естественному воспроизводству;

– защищённость его научно-технического, технологического, производственного и кадрового потенциала от прямых (активных) или косвенных (пассивных) экономических угроз.

Однако, ввиду комплексности, многоуровневости и многогранности содержания данного понятия, к нему следует применять термин «система экономической безопасности» предприятия. Чаще всего ученые рассматривают систему экономической безопасности предприятия как «…совокупность таких структурных элементов, как: научная теория безопасности, политика и стратегия безопасности, средства и методы обеспечения безопасности, концепция безопасности», как «организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз» или как «комплекс организационно-управленческих, режимных, технических, профилактических и пропагандистских мер, направленных на ка-

чественную реализацию защиты интересов предприятия от внешних и внутренних угроз».

5.2. Система экономической безопасности представляет собой совокупность взаимосвязанных и взаимно обусловливающих подсистем: оценочной, инструментальной, подсистемы детерминантов, объектов воздействия и субъектов обеспечения, представлена на рисунке 1.

Уровень экономической безопасности предприятия – это величина, характеризующая процесс взаимодействия подсистем детерминантов и инструментального обеспечения и формируемая в оценочной подсистеме. (здесь и далее, детерминант – основной фактор, оказывающий доминирующее влияние).

Содержание детерминантов на микроуровне – финансовая, интеллектуально-кадровая, технико-технологическая, информационная, ресурсно-производственная, управленческая, сбытовая (характеризующие наличие ресурсов у предприятия для обеспечения собственной безопасности).

Содержание детерминантов на мезоуровне – характеристики сферы деятельности и характеристики развития территории.

Содержание детерминантов на макроуровне – политические, макроэкономические, социальные; технологические, институциональные; природно-экологические (выступающие факторами либо повышающие, либо снижающими уровень экономической безопасности предприятия).

Комплексная методика оценки уровня экономической безопасности предприятия, включает:

— определение соответствия необходимого объема имеющихся ресурсов потребностям предприятия; выявление характера и силы воздействия детерминант мезо- и макро-уровней хозяйствования;

— расчет интегрального показателя, характеризующего уровень экономической безопасности предприятия на основе оценки имеющихся ресурсов и учета характера и силы воздействия внешней среды.

Рис. 1. Система экономической безопасности предприятия и ее структурные составляющие

5.3. Проведенный анализ классификаций угроз экономической безопасности предприятия, а также составляющих внешней среды (наиболее полно учитываемых в стратегическом менеджменте) позволил представить состав детерминант макро- и мезо- уровней в системе экономической безопасности в виде таблицы 1.

Таблица 1

Состав ключевых детерминант
в системе экономической безопасности предприятия

№ п/п	Уровень воздействия	Ключевые детерминанты	Характеристика ключевых детерминант
1	Микро-уровень	финансовая	достаточность собственных и заемных финансовых ресурсов
		интеллектуально-кадровая	достаточность трудовых ресурсов и уровень их квалификации
		технико-технологическая	соответствие технической оснащенности и технологического обеспечения потребностям развития
		информационная	адекватность и надежность информационного обеспечения
		сырьевая	достаточность ресурсного обеспечения для бесперебойного функционирования
		управленческая	адекватность и компетентность органов управления
		сбытовая	непрерывность основного вида деятельности, результативность сбытовой деятельности
2	Мезо-уровень	характеристики сферы деятельности	характеристика контрагентов, особенности развития сферы деятельности
		характеристики территории	ресурсное обеспечение территории; инфраструктурное обеспечение территории; привлекательность региона
3	Макро-уровень	политические	характер воздействия конкретных изменений в политической сфере
		экономические	характеристика макроэкономической ситуации, воздействие изменения макроэкономических характеристик
		социальные	характер воздействия на экономическую деятельность изменений социального характера
		технологические	динамика нововведений, темпы научно-технического прогресса
		институциональные	характер влияния на предприятие конкретных изменений в законодательстве
		природно-экологические	характер влияния изменений природных условий, изменение экологической обстановки

5.4. Комплексная оценка экономической безопасности предприятия. Оценки детерминант микроуровня и проведена адаптация методов определения ключевых параметров экспертной оценки детерминант мезо- и макро- уровней экономической безопасности (таблица 1).

Для оценки уровня экономической безопасности необходимо:

1) определить соответствие необходимого объема имеющихся ресурсов задаче безопасного функционирования предприятия.

Порядок определения соответствия необходимого объема имеющихся ресурсов выступает одним из элементов комплексной методики оценки экономической безопасности. Для оценки соответствия рекомендован расчет величины $\overline{d_{mi}}$ – усредненная величина, характеризующая достаточность имеющихся ресурсов по составляющим предприятия;

d_{mi} – величина, характеризующая достаточность имеющихся ресурсов по составляющим предприятия;

$$d_{mi} = \frac{x_{ij}}{m_{ij}} ,$$

где x_{ij} – текущее значение j-го показателя в i-ой детерминанте (финансовая, интеллектуально-кадровая, технико-технологическая, информационная, сырьевая, управленческая или сбытовая);

m_{ij} – пороговое значение j-го показателя в i-ой детерминанте.

Величина $\overline{d_{mi}}$ рассчитывается по каждой составляющей ресурсов (детерминант микроуровня в системе экономической безопасности) как средняя геометрическая стандартизированных значений показателя для каждой характеристики. Система данных показателей представлена в таблице 2.

Объем ресурсов следует считать соответствующим задаче безопасного функционирования, если усредненная величина, характеризующая достаточность имеющихся ресурсов по составляющим предприятия ($\overline{d_{mi}}$) по каждой составляющей превышает единицу.

Таблица 2

Состав показателей для оценки уровня экономической безопасности предприятия по составляющим

№ п\п	Составляющая детерминант	Показатели, характеризующие составляющие	Порядок расчета показателей	m[1]
1	финансовая	коэффициент текущей ликвидности	$К_{ТЛ}$ = ОбА / КДО	2
		коэффициент финансовой независимости	$К_{ФН}$ = ВБ / СК	0,5
		коэффициент обеспеченности СОС	$К_{ОБ.СОС}$ = СОС \ ОбС	0,1

[1] Пороговое значение (m) может варьироваться в зависимости от специфики сферы деятельности и особенностей предпринимательской структуры.

Окончание табл. 2

№ п\п	Составляющая детерминант	Показатели, характеризующие составляющие	Порядок расчета показателей	m^1
		вероятность получения займа или инвестиций при подаче заявки	экспертная оценка	100%
2	интеллектуально-кадровая	профессионально-квалификационный уровень кадров	экспертная оценка доли соответствующих требованиям предприятия	100%
		доля персонала, не имеющая нарушений трудовой дисциплин	$К_{ПН} = ЧП_{НН}/ЧП$	0,9
		коэффициент постоянства кадров	$К_{ПК} = К_{ПОСТ} \setminus К_{СП}$	0,8
3	технико-технологическая	доля технологического процесса, охваченного инновациями	$К_{ИО} = ТП_{И}/ТП$	0,8
		технический и технологический уровень производства	экспертная оценка в баллах (от 1 до 3)	3
4	информационная	вероятность сохранения коммерческой тайны	экспертная оценка	100%
		уровень надежности компьютерной техники	экспертная оценка в баллах (от 1 до 3)	3
5	сырьевая	коэффициент годности основных средств	$К_{ГОС} = О_{СТ}Ст / П_{ОЛН}Ст$	0,7
		коэффициент ресурсного обеспечения	$К_{РО} = РО_{ФАКТ} / РО_{НОРМ}$	1
		коэффициент автоматизации труда	$К_{АТ} = К_{ОЛ\text{-}ВОАВ} \setminus К_{ОЛ\text{-}ВОАВ}+К_{ОЛ\text{-}ВО\ РУЧ}$	0,7
6	управленческая	профессиональный уровень руководителей	экспертная оценка в баллах (от 1 до 3)	3
		репутация предприятия	экспертная оценка в баллах (от 1 до 3)	3
		разрыв в оплате труда аппарата управления и основной категории работников	$Кр = ВОТ_{Р} / ВОТ_{У}$	0,5
7	сбытовая	уровень развития сбытовой деятельности	доля реализованной продукции от планируемого объема	0,9
		качество продукции	доля продукции, соответствующей мировым стандартам, в общем объеме	0,7

Это свидетельствует о том, что при неизменности воздействия факторов макро- и мезо-уровней у предприятия имеются необходимые ресурсы для безопасного функционирования. Если же по какой-либо составляющей значение не превышает единицы – это свидетельствует о нехватке определенного типа ресурсов и обусловливает необходимость соответствующей корректировки реализуемой стратегии развития.

2) выявить характер и силу воздействия детерминант мезо- и макроуровней хозяйствования на функционирование предприятия.

Определение характера и силы воздействия детерминант мезо- и макроуровней хозяйствования производится только на основе экспертных оценок. Важными составляющими в системе оценки уровня экономической безопасности являются детерминанты макро- и мезо- уровней. При комплексной оценке их учет производится в виде применения уточняющих коэффициентов $\overline{k_{ma}}, \overline{k_{me}}$.

$\overline{k_{ma}}$ – коэффициент влияния детерминант макроуровня в системе экономической безопасности предприятия, полученный как усредненное значение параметров, полученных в результате экспертной оценки;

$\overline{k_{me}}$ – коэффициент влияния детерминант мезо-уровня в системе экономической безопасности предприятия, полученный как усредненное значение параметров, полученных в результате экспертной оценки.

Оценка детерминант макроуровня. В данном случае для целей оценки детерминант системы экономической безопасности макроуровня целесообразно адаптировать применяемый в стратегическом управлении ПЭСТ-анализ (ПЭСТ анализ является аббревиатурой следующих показателей отрасли: политические (П), экономические (Э), социально-культурные (С) и технологические (Т)). Составом детерминант (политическая составляющая исследуется как внешняя среда предпринимательской структуры, определяющая возможности получения ресурсов; экономические детерминанты представляют интерес с точки зрения условий для стабильного функционирования; социальный аспект интересен с точки зрения потребления; технологическая составляющая имеет значение как возможность осуществления предпринимательской структуры), однако, для целей оценки детерминант системы экономической безопасности эти составляющие требуют дополнения. В состав ПЭСТ-анализа включают правовые и природные факторы, согласимся с данным положением, поскольку правовая, или институциональная составляющая (ее несовершенство) может выступать довольно сильным ограничителем в предпринимательской сфере (таблице 3).

Таблица 3

Параметры экспертной оценки детерминант макроуровня в системе экономической безопасности предприятия[2]

Ключевые детерминанты	Характеристика ключевых детерминант	Параметр экспертной оценки
политические	содержание воздействия изменений политической ситуации на функционирование предприятия	– возможности изменения объемов поставок зарубежным потребителям в случае изменения политической ситуации; – возможности изменения объемов сырья и ресурсов, получаемых из-за рубежа
экономические	содержание воздействия макроэкономических параметров на функционирование предприятия	– инфляция; – фаза экономического цикла; – валютный курс
социальные	содержание воздействия на функционирование предприятия изменений в потребительской среде	– уровень жизни населения; – объемы потребления; – потребительские предпочтения
технологические	динамика нововведений, темпы научно-технического прогресса	– появление инновационных технологий; – соответствие этапу технологического развития страны
институциональные	характер влияния на предприятие конкретных изменений в законодательстве	– изменения в налоговом законодательстве; – изменение ставки рефинансирования; – изменения в приоритетах государственной политики (поддержка предпринимательской деятельности)
природно-экологические	характер влияния изменений природных условий, изменение экологической обстановки	– изменения климатических условий; – изменения в параметрах экологического контроля

Оценка детерминант мезо-уровня системы экономической безопасности. В данном случае следует учитывать, что мезо-уровень хозяйствования можно понимать как в отраслевом, так и в территориальном аспекте. Если мы обращаемся к отраслевому аспекту, то в качестве фактора, выступающего либо угрозой, либо благоприятным условием, исследуются характеристики сферы функционирования предпринимательской структуры. В данном аспекте интересной будет адаптация методик проведения отраслевого среза.

[2] Совокупность параметров для экспертной оценки воздействия детерминант макроуровня на безопасное функционирование предприятия может быть изменено в зависимости от специфики предпринимательской деятельности и сферы деятельности.

Если же рассматривать мезо-уровень с позиций территории, то детерминантами будут выступать характеристики определенного региона. Параметрами экспертной оценки характера воздействия детерминант мезоуровня будут выступать следующие параметры, приведенные в таблице 4:

Таблица 4

Параметры экспертной оценки детерминант мезоуровня в системе экономической безопасности предприятия [3]

Ключевые детерминанты	Характеристика ключевых детерминант	Параметр экспертной оценки
характеристики сферы деятельности	характеристика контрагентов; особенности развития сферы деятельности	– надежность партнеров; – надежность инвесторов; – объем и перспективность развития рынка; – характер конкуренции на рынке; – сезонные колебания; – инновационное развитие конкурентов; – привлекательность бизнеса
характеристики территории	ресурсное обеспечение территории; инфраструктурное обеспечение территории; привлекательность региона	– уровень безработицы в регионе; – уровень жизни населения в регионе; – инвестиционная привлекательность территории; – границы рынка сбыта; – наличие местных ресурсов; – транспортно-логистическая инфраструктура

Для оценки уровня экономической безопасности значение имеет не только сила, но и характер воздействия. В данном случае предлагается экспертам оценку детерминант системы экономической безопасности макроуровня проводить в следующем порядке:

– определение содержания воздействующего фактора на систему экономической безопасности;

– определение характера воздействия (в данном случае возможен выбор одного из двух вариантов: угроза для бизнеса или благоприятное условие для бизнеса);

– определение силы воздействия (предполагается, что сила воздействия определяется исходя из следующих вариантов: полная независимость, слабое

[3] Совокупность параметров для экспертной оценки воздействия детерминант мезоуровня на безопасное функционирование предприятия может быть изменено в зависимости от специфики предпринимательской деятельности и сферы деятельности.

воздействие, чувствительное воздействие, сильное воздействие, очень сильное воздействие);

– выбор оценки для характеристики силы и характера воздействия каждого фактора в составе детерминант макро- и мезо- уровней (табл.5);

– расчет среднего уточняющего коэффициента по макро- и мезо- экономическим детерминантам (расчет коэффициента осуществляется по средней геометрической).

– по средней геометрической).

Таблица 5

Значения оценок факторов в составе детерминант мезо- и макро- уровней в соответствии с экспертной оценкой их силы и характера воздействия

№ п/п	Сила воздействия	Характер воздействия	Оценка, используемая при расчетах
1	полная независимость	угроза для бизнеса	1
		благоприятные условия для бизнеса	1
2	слабое воздействие	угроза для бизнеса	0,9
		благоприятные условия для бизнеса	1,1
3	чувствительное воздействие	угроза для бизнеса	0,8
		благоприятные условия для бизнеса	1,2
4	сильное воздействие	угроза для бизнеса	0,7
		благоприятные условия для бизнеса	1,3
5	очень сильное воздействие	угроза для бизнеса	0,6
		благоприятные условия для бизнеса	1,4

3) дать комплексную оценку экономической безопасности предприятия по формуле (1).

Интегральный показатель уровня экономической безопасности представлен $Э$ в мультипликативном виде:

$$Э = \overline{d_m} * \overline{k_{ma}} * \overline{k_{me}} \qquad (1)$$

Пороговым значением для оценки данного показателя выступает единица. Если $Э$ больше или равно единице, то уровень экономической безопасности не просто высокий, а у предприятия достаточно собственных ресурсов для успешного нивелирования угроз экономической безопасности, возникающих во внешней среде. Если значение $Э$ меньше единицы, то необходим детальный анализ детерминант в системе экономической безопасности.

Вопросы для самоподготовки

1. Дайте определение «система экономической безопасности предприятия».

2. Состав детерминант в системе экономической безопасности предприятия. Раскрыть их содержание.

3. Раскройте содержание комплексной оценки уровня экономической безопасности предприятия.

4. Содержание оценки детерминант микроуровня в системе экономической безопасности предприятия.

5. Структура системы экономической безопасности предприятия.

6. Уровень экономической безопасности предприятия.

7. Классификации угроз экономической безопасности.

8. Состав ключевых детерминант микроуровня в системе экономической безопасности предприятия.

9. Состав ключевых детерминант мезоуровня в системе экономической безопасности предприятия

10. Состав ключевых детерминант макроуровня в системе экономической безопасности предприятия

Литература

1. Гильфанов, М.Т. Организационно-методический инструментарий оценки детерминант обеспечения экономической безопасности предприятия / М.Т. Гильфанов // Социально-экономические явления и процессы. – 2013. – №8. – 1,0 п.л.

2. Гильфанов, М.Т. Дифференцированный инструментарий обеспечения экономической безопасности предприятия / М.Т. Гильфанов // Социально-экономические явления и процессы. – 2013. – №10. – 0,4 п.л.

3. Колесниченко, Е.А. Методические аспекты оценки и обеспечения экономической безопасности предприятия / Е.А. Колесниченко, М.Т. Гильфанов // Вестник Тамбовского университета. Серия: гуманитарные науки. – 2013. – Вып.11. – 0,8 п.л.

6. ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ. ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

6.1. Общее определение: экономическая безопасность предприятия – это наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры предприятия его стратегическим целям и задачам.

Данное определение подчеркивает тот факт, что экономическая безопасность находится на стыке экономики и безопасности предприятия. Исходя из данного выше определения, следует выделить основные функциональные блоки системы экономической безопасности предприятия, обеспечивающие максимальное соответствие менеджмента предприятия и его ресурсного потенциала: имущество (активы) предприятия; финансы предприятия; кадры предприятия; технологии и инновации; информационная система предприятия; организационная структура предприятия.

Данная структура функциональных составляющих соответствует структуре механизма обеспечения экономической безопасности предприятия и затрагивает все функциональные области деятельности предприятия: инновационную, ресурсную, инвестиционную, маркетинговую), их цели должны корреспондироваться со стратегическими интересами предприятия в рассматриваемой функциональной области деятельности, а показатели, характеризующие цели стратегии, должны соответствовать количественной оценке стратегических интересов предприятия. Установление такого соответствия является очень важным, поскольку именно с его помощью обеспечивается единство методиче-

ской базы организации управления предприятием.

Создание и функционирование любого предприятия представляет собой процесс инвестирования финансовых ресурсов на долгосрочной основе с целью извлечения прибыли. Процесс управления активами (имущественным потенциалом) также направлен на возрастание прибыли и характеризуется понятием операционно-финансового рычага (производственного и финансового левериджа), для которого характерна взаимосвязь экономических показателей: выручки, расходов производственного и финансового характера и чистой прибыли. Оптимальность этой связи обеспечивает запас финансовой прочности и является фактором экономической безопасности предприятия.

Бизнес-процесс предприятия связан с операционной деятельностью, бухгалтерским учетом, управлением финансами и кадрами, существенная роль в которых принадлежит информационным технологиям (совокупность вычислительных и информационных систем, средств связи, программ и т. п.), позволяющим решить эту задачу оптимальным способом, но требующим материальных и временных затрат на ее внедрение. Таким образом бизнес-процесс предприятия зависит от работоспособности информационной системы, а для потребителя безопасность внедряемых информационных технологий – это проблема, связанная с обеспечением их правильного и бесперебойного функционирования.

6.2. Информационная система предприятия, как правило, охватывает все сферы его деятельности: административную, производственную, финансовую, выступает как связующее звено при выработке стратегии бизнеса и качества управления предприятием и персоналом. В ней содержатся сведения, касающиеся планов, состояния материальных и финансовых потоков, договорной деятельности, данные финансового и управленческого учета. Такого рода коммерческая информация носит сугубо конфиденциальный характер, а ее утрата может оказаться критичной для работы всего предприятия, поэтому организация работы пользователей с содержащейся в системе информацией требует специальных мер защиты, обеспечивающих конфиденциальность, целостность и доступность данных.

Помимо самой информации к объектам правовой защиты следует отнести все элементы информационной системы предприятия, которые по своей стоимости и значимости являются нематериальными активами, т. е. долгосрочными активами, не обладающими материальной сущностью (формой) и способные приносить доход.

6.3. Информационная безопасность – один из главных приоритетов современного бизнеса, поскольку нарушения в этой сфере приводят к гибельным последствиям для бизнеса любой компании. Применение высоких информационных технологий XXI в., с одной стороны, дает значительные преимущества в деятельности предприятий и организаций, а с другой – потенциально создает предпосылки для утечки, хищения, утраты, искажения, подделки, уничтожения, копирования и блокирования информации и, как следствие, нанесение экономического, социального или других видов ущерба, т. е. проблема информационных рисков и нахождения путей снижения ущерба становится с каждым годом все острее.

Цель информационной безопасности – выявить возможные угрозы безопасности информации, определить их последствия и возможный ущерб, обеспечить необходимые меры и средства защиты, и оценить их эффективность.

Поскольку анализ всей информационной инфраструктуры далеко не всегда оправдан с экономической точки зрения, целесообразно сосредоточиться на наиболее важных, одновременно выявляя не только сами угрозы, вероятность из осуществления, размер потенциального ущерба, но и их источники.

6.4. Анализ рисков информационной безопасности. Анализ информационных рисков – это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. Стандарт ISO 27001 определяет информационную безопасность как: «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность».

Конфиденциальность – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).

Целостность – обеспечение точности и полноты информации, а также методов ее обработки.

Доступность – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

При этом риск – это вероятный ущерб, который зависит от защищенности системы. Итак, из определения следует, что на выходе алгоритма анализа риска можно получить либо количественную оценку рисков (риск измеряется в деньгах), либо – качественную (уровни риска; обычно: высокий, средний, низкий).

Оценка рисков производится с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящие потенциальную угрозу в разряд опасных и потому требующих принятия дополнительных защитных мер. Как правило, для каждой подобной угрозы существует несколько решений по ее нейтрализации. При оценке их стоимости и эффективности следует учитывать не только расходы на закупку оборудования и программных средств, но и такие обстоятельства, как стоимость обучения персонала для работы с ним, совместимость с программным обеспечением и т. д.

В настоящее время не существует единой методики количественного расчета величин рисков, измеряемой в стоимостной оценке. Это связано в первую очередь с отсутствием достаточного объема статистических данных о вероятности реализации той или иной угрозы. В настоящее время идет активное накопление данных, на основании которых можно было бы с приемлемой точностью определить вероятность реализации той или иной угрозы. К сожалению, имеющиеся справочники опираются на зарубежный опыт и потому с трудом применимы к российским реалиям. К тому же определение величины стоимости информационного ресурса (будь то физический сервер или файлы и записи СУБД) тоже зачастую затруднено. К примеру, если владелец ресурса (в предположении, что таковой идентифицирован) может назвать стоимость оборудо-

вания и носителей, то указать точную стоимость находящихся в его ведении данных он практически не в состоянии.

Поэтому наиболее распространенной остается качественная оценка информационных рисков. Его главная задача – определить факторы риска, установить потенциальные области риска и оценить воздействие каждого вида. Анализ рисков проводится экспертным путем.

В расчетах информационных рисков учитываются следующие факторы:

1. Стоимость ресурса (СР), указанная величина характеризует ценность ресурса. При качественной оценке рисков стоимость ресурса чаще всего ранжируется в диапазоне от 1 до 3, где 1 – минимальная стоимость ресурса, 2 – средняя стоимость ресурса и 3 – максимальная стоимость ресурса. К примеру, сервер автоматизированной банковской системы имеет СР = 3, тогда как отдельный информационный киоск, предназначенный для обслуживания клиента, имеет СР = 1 по отношению к информационной банковской системе;

2. Мера уязвимости ресурса к угрозе (УР). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе. Например, с точки зрения банка ресурс автоматизированной банковской системы имеет наибольшие риски, переводящие потенциальную угрозу в разряд опасных и потому требующих принятия дополнительных защитных мер. Как правило, для каждой подобной угрозы существует несколько решений по ее нейтрализации. При оценке их стоимости и эффективности следует учитывать не только расходы на закупку оборудования и программных средств, но и такие обстоятельства, как стоимость обучения персонала для работы с ним, совместимость с программным обеспечением и т. д.

Оценка вероятности реализации угрозы (ВРУ) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая).

На основании полученных данных выводится оценка ожидаемых потерь от конкретной угрозы за определенный период времени (ОПВ), которая харак-

теризует величину риска и рассчитывается по формуле:

$$ОПВ = (СР \times УР \times ВРУ). \quad (2)$$

После проведения первичной оценки рисков полученные значения следует систематизировать по степени важности для выявления низких, средних и высоких уровней рисков. Методика управления рисками подразумевает несколько способов действий. Риск может быть:

принят, т. е. пользователь согласен на риск и связанные с ним потери. В этом случае работа информационной системы продолжается в обычном режиме;

снижен – с целью уменьшения величины риска будут приняты определенные меры;

передан – компенсацию потенциального ущерба возложат на страховую компанию, либо риск трансформируют в другой риск – с более низким значением – путем внедрения специальных механизмов.

Некоторые методики дополнительно предусматривают еще один способ управления – «упразднение». Он подразумевает принятие мер по ликвидации источника риска.

Далее проводится ранжирование рисков, а затем определяются те, которые требуют первоочередного внимания. Основным методом управления такими рисками является снижение, реже – передача. Риски среднего ранга могут передаваться или снижаться наравне с высокими рисками. Риски низшего ранга, как правило, принимаются и исключаются из дальнейшего анализа.

Диапазон ранжирования рисков принимается исходя из проведенного расчета их качественных величин. Так, например, если величины рассчитанных рисков лежат в диапазоне от 1 до 18, то низкие риски находятся в диапазоне от 1 до 7, средние – в диапазоне от 8 до 13, высокие – в диапазоне от 14 до 18.Таким образом, управление рисками сводится к снижению величин высоких и средних рисков до характерных для низких рисков значений, при которых возможно их принятие. Снижение величины риска достигается за счет

уменьшения одной или нескольких составляющих (СР, УР, ВРУ) путем принятия определенных мер. В основном это возможно применительно к УР и ВРУ, так как СР (стоимость ресурса) – достаточно фиксированный параметр. Однако возможно и его снижение, например, если хранящаяся на сервере информация относится к конфиденциальной, но проверка выявила, что гриф «конфиденциально» в силу каких-либо причин может быть снят. В результате стоимость ресурса автоматически уменьшается. В системе Internet-банкинга, например, параметр УР можно уменьшить путем фиксации ответственности сторон в договорном порядке. В этом случае считается, что стороны предупреждены об ответственности, которую может повлечь за собой нарушение правил эксплуатации системы, и, таким образом, фактор уязвимости снижается.

Снижение параметра ВРУ, т. е. вероятности реализации угрозы, может быть достигнуто за счет технических мер. Например, при наличии угрозы кратковременного отключения электропитания установка источника бесперебойного питания снижает вероятность ее реализации.

Возникшие (оставшиеся) после применения методики управления риски называются остаточными, и именно они применяются для обоснования инвестиций в информационную безопасность.

Перерасчет рисков производится в отношении всех рисков, если они оценены как высокие и средние.

Вопросы для самоподготовки

1. Роль и цель информационной безопасности в бизнес-процессах предприятия.

2. Риск информационной безопасности и подходы к его оценке.

3. Основные факторы, которые учитываются при расчетах информационных рисков.

4. Систематизация оценок рисков по степени важности.

5. Подходы к снижению информационных рисков.

Литература

1. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.

2. ГОСТ Р 51897-2002, Менеджмент риска. Термины и определения.

3. ГОСТ Р 51898-2002, Аспекты безопасности. Правила включения в стандарты.

4. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

5. ГОСТ Р ИСО/МЭК 27001-2013 Системы менеджмента информационной безопасности

---

7. ОЦЕНКА РИСКОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

7.1. Система обеспечения экономической безопасности предприятия обеспечивает защиту его деятельности от существующих либо прогнозируемых угроз. При этом возможно возникновение угроз экономической безопасности предприятия, которые не могли быть заранее и обоснованно спрогнозированы. Не поддающиеся обоснованному прогнозированию угрозы экономической безопасности предприятия представляют собой риски.

Риск – это экономическая категория, которая отражает характерные особенности восприятия заинтересованными субъектами экономических отношений, объективно существующих неопределенности и конфликтности, присущих процессам целеполагания, управления, принятия решений, оценки, обремененные возможными угрозами и неиспользованными возможностями.

Особенностью экономического риска в современных условиях является его тотальность (всеобщность)

Риск – это величина, характеризующая потенциальные убытки (потери), связанные с принятием неправильных управленческих решений, вырабатываемых в результате изучения экономической, политической и социальной ситуации, в которой протекает деятельность компании.

Несмотря на то, что в современной экономической литературе существует множество взглядов на проблему риска, что порождает разнообразие определений понятия «риск», предложенных различными авторами, можно сформулировать три типа определения данной категории:

- риск – это вероятность отклонения от запланированных результатов (потери или дополнительные прибыли);
- риск – это неопределенность, поддающаяся качественной и/или количественной оценке;
- риск – это действие наудачу в ситуации неопределенности в надежде на положительный результат.

Применительно к производственной сфере риск определяется как возможность потери части ресурсов и/или недополучения доходов по сравнению с уровнями и значениями, рассчитанными исходя из предпосылок о наиболее рациональном использовании ресурсов и принятого сценария развития рыночной конъюнктуры.

Промышленный риск – это риск, возникающий при любых видах деятельности, связанных с производством продукции, ее реализации, товарно-денежными и финансовыми операциями, маркетингом, коммерцией, осуществлением социально-экономических и научно-технических проектов.

Составление системы классификационных признаков риска дает понимание его природы, позволяет установить структурные характеристики, и разрабатывать мероприятия, позволяющие снижать уровень риска по результатам его оценки.

Выделяются следующие группы рисков экономической безопасности предприятия:

– непредвиденные изменения окружающей предприятие среды (социально-политические сдвиги и изменение спроса, девальвация, инфляция, обвалы на фондовых биржах, изменение налоговых ставок, недобросовестность хозяйственных партнеров и т.д.);

– появление более выгодных для предприятия предложений (новых покупателей или поставщиков), которые потенциально угрожают потерей дополнительной выгоды;

– появление новых технических и организационных решений, в особенности возникших вне предприятия и угрожающих конкурентоспособности продукции;

– техногенные катастрофы, аварии, остановки;

– изменение транспортных, финансовых и других условий взаимоотношений с покупателями и поставщиками.

Как правило, причина негативных отклонений фактического развития предприятия от предусмотренных стратегическим планом является наступление одной из вышеперечисленных ситуаций. Поэтому риск – это непредсказуемая угроза экономической безопасности предприятия и устойчивости его функционирования.

Таким образом, задача системы обеспечения экономической безопасности предприятия состоит в анализе рисков экономической безопасности предприятия, а также в оценке степени их влияния на деятельность предприятия и недопущении перехода за допустимые пределы.

7.2. Подходы к оценке рисков предприятий.

Для оценки рисков используется алгоритм, приведенный на рисунке 2.

На первом этапе осуществляется выбор факторов риска, влияние которых на хозяйственную деятельность необходимо уменьшить. Основная цель оценки риска определить максимально допустимый риск для конкретного вида случаев. Далее необходимо провести оценку и анализ отобранных факторов.

Сравнительный анализ используемых методов оценки рисков позволил выделить два подхода: качественный и количественный.

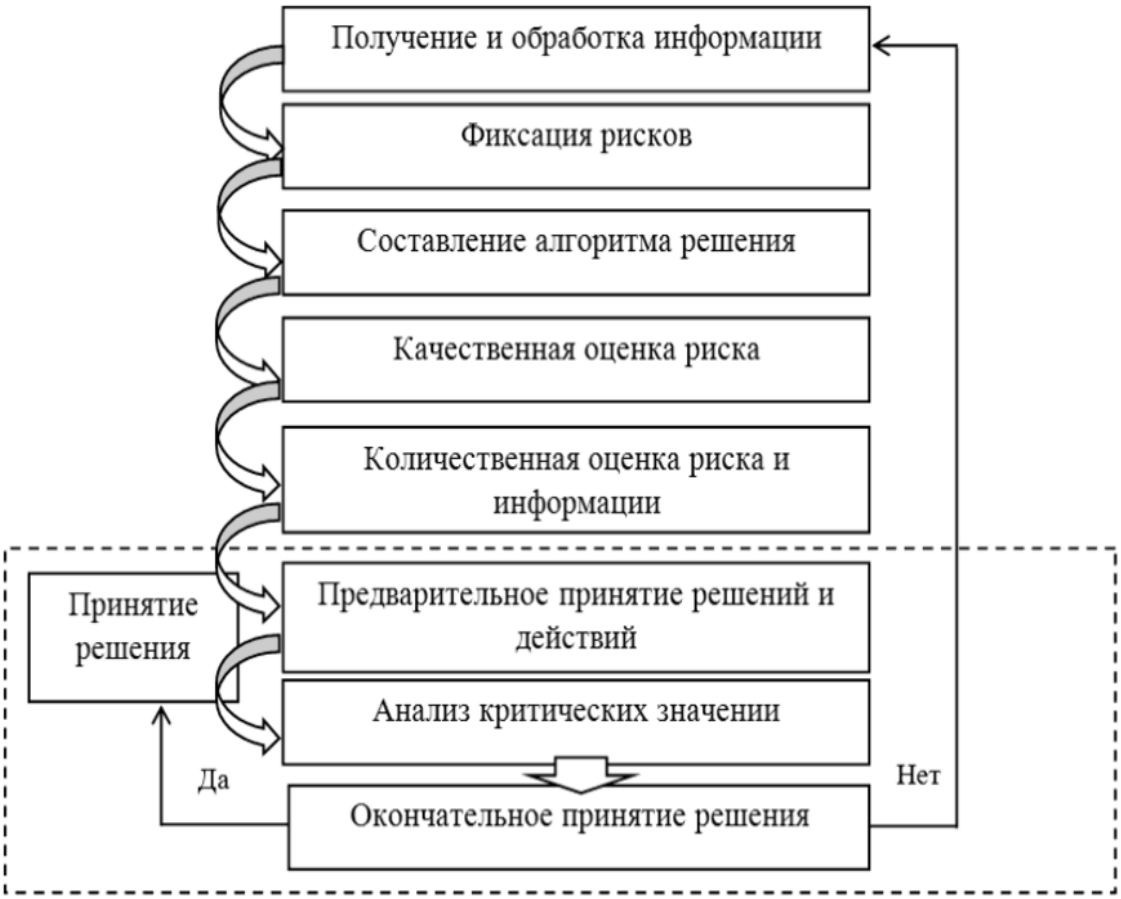


Рис. 2. Алгоритм комплексной оценки рисков

Основная специфическая особенность качественного подхода в исследовании рисков состоит в том, что сначала проводится идентификация рисков проекта, а затем стоимостная оценка последствий риска и разработанных мероприятий по борьбе с ними.

Качественный анализ проводиться на стадии планирования деятельности.

Количественный анализ, базирующийся на инструментарии теории вероятности и математической статистики, состоит, в числовом измерении, влияния изменений рисковых факторов проекта на изменение эффективности проекта и опирается на базисный вариант бизнес-плана проекта и проведенный качественный анализ.

За идентификацию всех возможных рисков отвечает качественный анализ, который определяет факторы риска, последовательность работ, при выполнении которых возникает риск и т.д.

За выявление размера ущерба от различных подвидов риска отвечает количественный анализ, который выявляет причины, источники риска и величину вероятных последствий. На рисунке 3 обозначены процедуры, применяемые для анализа рисков. Алгоритм экспертного оценивания рисков, приведен на рисунке 4. Методы количественной оценки рисков – это статистические методы оценки, метод аналогий, логико-вероятностные методы, группа аналитических методов (рисунок 5).

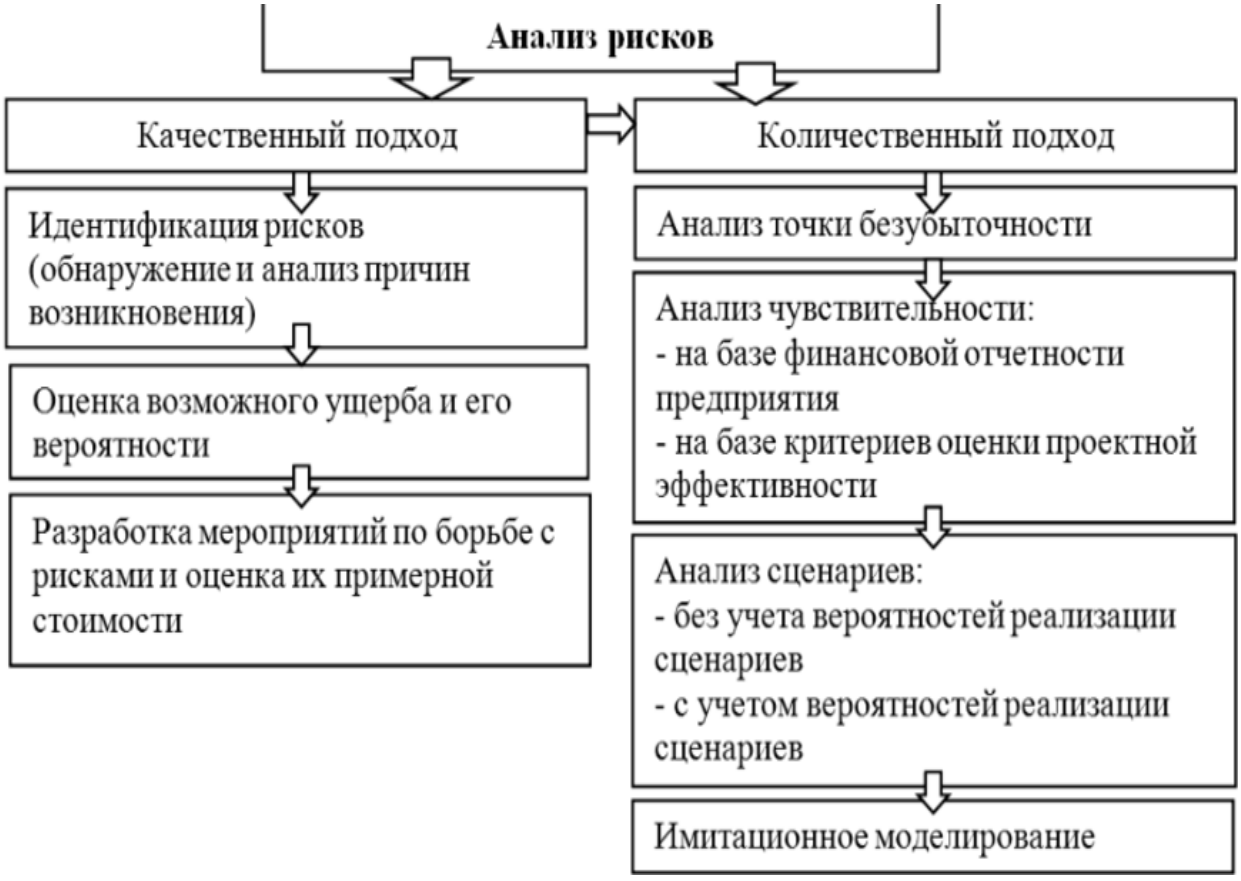


Рис. 3. Процедура анализа рисков

Рис. 4. Алгоритм экспертного оценивания рисков

Рис. 5. Алгоритм количественного оценивания рисков

Особый интерес в последнее время проявляется к аналитическим методам оценки рисков, а именно методам, учитывающим распределение вероятностей. Данные методы применяются, как правило, для оценки рисков инвестиционных / инновационных проектов.

7.3. Для решения задачи прогнозирования рисков используются все известные методы статистики и экономики, которые позволяют оценить параметры объекта вперед на некоторый интервал времени.

Уровень риска может оцениваться по формуле:

$$У_Р = В_Р * Р_П, \quad (3)$$

где $У_Р$ – уровень соответствующего риска;

$В_Р$ – вероятность возникновения данного риска;

$Р_П$ – размер возможных финансовых потерь при реализации данного риска.

Таким образом, существует совокупность методов определения вероятности потерь, которые позволяют произвести приблизительную оценку общего объема рисков для промышленного предприятия.

Предприятие, осуществляя свою деятельность может отказаться от реализации того или иного решения, связанного с рисками, причем данные методы применимы в отношении значительных рисков как на стадии предварительной проработки решения, так и в процессе деятельности, как корректирующее воздействие в случае не санкционированного роста рисков.

7.4. На сегодняшний день существует большое количество методов минимизации риска, представленные различными учеными.

К основным способам минимизации рисков относят: распределение риска по разным агентам, страхование риска, осуществление самострахования рисков, организация диверсификации производства, лимитирование, осуществление альтернативного планирования, создание гибкой структуры производства, создание резервных фондов, мониторинг информации, обучение и тренировка персонала, применение гибких технологий, уклонение от риска.

Способы снижения риска в управлении предприятием, приведены в таблице 6.

Таблица 6

Способы снижения риска

Виды риска	Способы снижения риска
В сфере производства	
Технический риск	Проведение профилактических мероприятий, формирование резервных фондов, страхование
Технологический риск	Контроль качества, мониторинг ситуации
Риск организации производства	Разработка перспективных направлений развития, построение рациональной производственной структуры, проведение эффективной инновационной и инвестиционной политики
Риск обеспечения трудовыми ресурсами	Повышение квалификации, обучение персонала, аттестация, страхование от несчастных случаев
Исполнительский риск	Методы мотивации работников, способствующие достижению целей предприятия (объединения)
Риск стихийных бедствий	Страхование, самострахование - формирование резервных фондов
В сфере снабжения и сбыта	
Рыночный риск	Проведение интеграционных процессов (заключение долгосрочных договоров, соглашений), диверсификация производства
Транспортный риск	Самострахование, введение штрафных санкций, неустоек
Складской риск	Внедрение ресурсосберегающих, энергосберегающих технологий
Риск закупки сырья	Внедрение методов научного управления запасами
Маркетинговый риск	Проведение маркетинговых исследований, диверсификация рынков сбыта, создание и продвижение торговой марки (брэнда)

На предприятиях создают системы управления риском (рисунок 6), в которых реализуются методы управления, приведенные на рисунке 7.

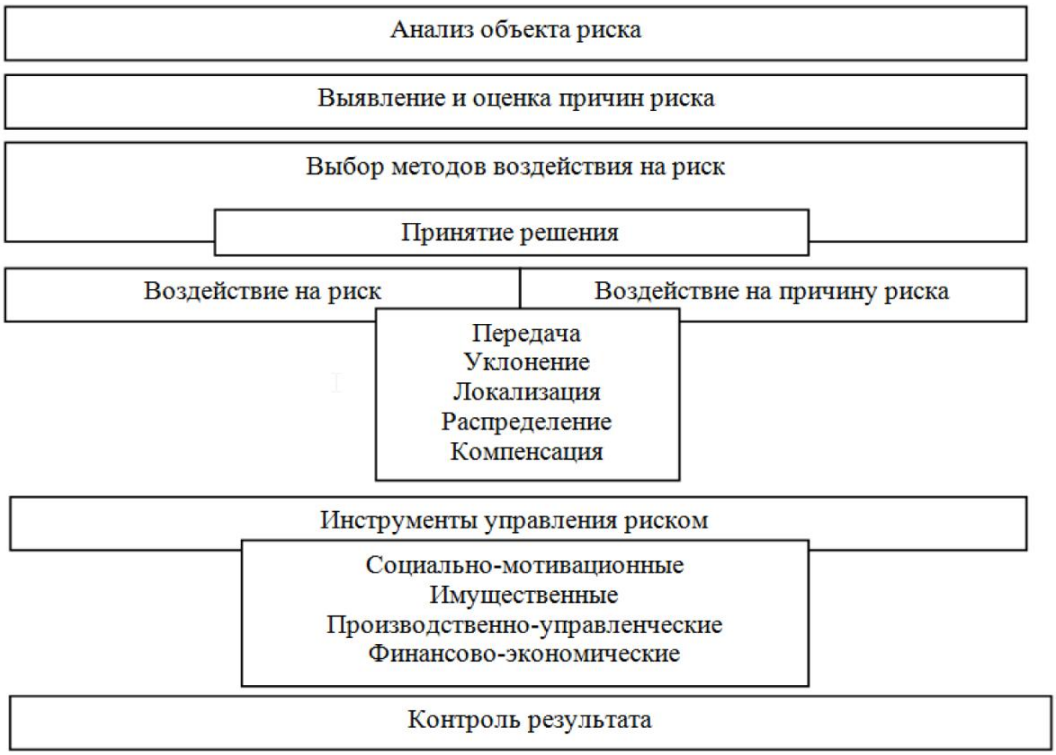


Рис. 6. Общая схема системы управления риском предприятий

Рис. 7. Методы управления риском

Угрозы и ограничения внешней среды также представляют серьезную опасность, порождая множество рисков. Внешние угрозы – это организованная преступность, рэкет, преступные действия и мошенничества отдельных лиц, недобросовестная конкуренция и т.д. Ограничения внешней среды в ряде случаев затрудняют рыночную деятельность предприятий (фирм). К ним относятся, например, факторы политического, демографического, экономического окружения. Так, политические факторы порождаются действиями государственных органов и выражаются в увеличении налогов, акцизов, таможенных ставок, изменении договорных условий, трансформации форм в отношении собственности, законодательном ограничении предпринимательства и др.

Вопросы для самоподготовки

1. Риск как экономическая категория. Определения рисков.
2. Группы рисков экономической безопасности предприятия.
3. Алгоритм оценки рисков.

4. Анализ рисков качественный и количественный подходы. Общая характеристика.

5. Алгоритм экспертного оценивания рисков.

6. Алгоритм количественного оценивания рисков.

7. Математическая модель оценки уровня риска.

8. Способы минимизации рисков.

9. Общая схема системы управления риском предприятия.

10. Модель вероятных потерь от снижения намеченных объемов производства и реализации продукции вследствие проявления рисков.

11. Схема зон риска в зависимости от величины потерь и характеристики рисков.

12. Анализ зависимости вероятностей возможных потерь прибыли от уровня потерь по графику.

Литература

1. Уразгалиев, В.Ш. Экономическая безопасность. Учебник и практикум для вузов. – СПб.: Издательство «Юрайт», 2017. – 374 с.

2. Гапоненко, В.Ф., Беспалько, А.Л., Власов, А.С. Экономическая безопасность предприятия. Подходы и принципы. – М.: Издательство «Ось-89», 2007.-208с. www.zahvat.ru 33743.pdf

3. Суглобов, А.В., Хмелев, С.А., Орлова, Е.А. Экономическая безопасность предприятия. – М.: Издательство: Юнти-Дана, 2012. – 272 с.

4. Ланкина, С.А., Флегонтов, В.И. Классификация и проблемы оценки рисков промышленного предприятия. http://schooled.ru/economic/safety/index.htmИнтернет-журнал «НАУКОВЕДЕНИЕ», http://naukovedenie.ru, Том 7, № 3 (май – июнь 2015) publishing@naukovedenie.ru

8. СИСТЕМА МОНИТОРИНГА И АУДИТА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

8.1. Государственная деятельность по обеспечению экономической безопасности страны включает в себя следующие элементы:

- мониторинг экономики и общества в целях выявления и прогнозирования внутренних и внешних угроз жизненно важным интересам;
- разработка мер по предупреждению и нейтрализации внутренних и внешних угроз;
- организация мер по обеспечению экономической безопасности.

Ряд вопросов по обеспечению экономической безопасности осуществляется в процессе разработки проектов прогноза социально-экономического развития России и государственного бюджета на следующий год.

Для обеспечения стратегии экономической безопасности формируется система государственного воздействия на экономику. Эта система позволяет регулировать важнейшие экономические преобразования, включая взаимодействие между ними, а также берет на себя функции регулирования и поддержания экономики страны на безопасном уровне. Для этого должны быть: определены границы и условия государственного вмешательства в экономику; границы государственного сектора; обеспечено развитие эффективных методов государственного регулирования.

Важнейшими элементами механизма обеспечения экономической безопасности Российской Федерации являются мониторинг и прогнозирование.

Мониторинг как оперативная информационно-аналитическая система показателей играет важную роль в условиях наличия межотраслевых диспропорций и острой недостаточности ресурсов (прежде всего финансовых), изменчивости и неустойчивости социально-экономических индикаторов.

Это определяет возрастание требований к государственной статистике, глубине форм охвата объектов статистического наблюдения, качества и оперативности информации.

Для проведения мониторинга факторов, определяющих угрозы экономическим интересам личности, общества и государства, важнейшей задачей является создание организационно-информационной базы.

8.2. Мониторинг является механизмом контроля экономической безопасности, главные цели которого:

● создание государственной системы мониторинга состояния обеспечения экономической безопасности РФ;

● оперативное обеспечение органов государственной власти информацией о состоянии угроз экономической безопасности, их характере, возможным последствиям, а так же прогнозам в этой области;

● обеспечение информационного взаимодействия всех органов власти;

● контроль за состоянием угроз экономической безопасности страны.

Для достижения целей организации мониторинга необходимо решение следующих задач:

● разработка организационно-методического обеспечения проведения мониторинга;

● разработка механизма сбора информации о состоянии угроз;

● оперативный анализ информации в целях предупреждения угроз экономической безопасности.

Для реализации стратегии показатели (пороговые значения) состояния экономики, выход за пределы которых вызывает угрозу экономической безопасности страны, характеризующие:

● динамику и структуру валового внутреннего продукта, показатели объемов и темпов промышленного производства, отраслевую и региональную структуру, динамику отдельных отраслей, капитальные вложения и тому подобное;

● состояние ресурсного, производственного и научно-технического по-

тенциала;

● способность адаптироваться к внутренним и внешним факторам (темпы инфляции, дефицит государственного бюджета, воздействие внешнеэкономических факторов, стабильность национальной валюты, внутренняя и внешняя задолженность и тому подобное);

● состояние финансово-бюджетной и кредитной систем;

● качество жизни населения (валовой внутренний продукт на душу населения), уровень безработицы и дифференциации доходов, обеспеченность основных групп населения материальными благами и услугами, состояние окружающей среды и тому подобное.

8.3. Анализ и прогнозирование социально-экономического развития является началом работ по планированию регионального развития. На основе прогноза определяются цели, уточняются программные мероприятия и приоритеты в развитии региона.

Прогнозирование – составная часть государственного регулирования экономики, призванная определять направления развития региона и его структурных составляющих. Результаты прогнозных расчетов используются государственными органами для обоснования целей и задач социально-экономического развития, выработки и обоснования социально-экономической политики правительства, способов рационализации использования ограниченных производственных ресурсов.

В состав прогноза развития региона входят набор частных прогнозов и комплексный экономический прогноз, отражающий в обобщенной форме развитие экономики и социальной сферы региона.

В частных прогнозах оцениваются:

● демографическая ситуация;

● состояние природной среды;

● состояние научно-технических достижений;

● основные факторы производства (капитал, труд, инвестиции);

● спрос населения на товары и услуги;

● платежеспособность населения;

● темпы развития отдельных отраслей народного хозяйства, территорий и других общественно значимых сфер деятельности.

В комплексном экономическом прогнозе отражается будущее развитие экономики региона как целостного образования. Разработка комплексного прогноза базируется на научных основах, которые объясняют функционирование и развитие региона.

По временному горизонту комплексные прогнозы экономического развития регионов можно подразделить на: долго-, средне- и краткосрочный.

В качестве рабочих инструментов комплексного прогноза используются: экстраполяция тенденций; эконометрические расчеты на базе данных системы национального счетоводства; система макроструктурных моделей, включающая модифицированную модель межотраслевого баланса; модель динамики капитала и инвестиций в реальный сектор экономики

Разработка комплексного экономического прогноза региона преследует следующие цели: он должен обеспечить правительство региона информацией для принятия решений; его показатели служат основой для разработки показателей проекта бюджета региона.

Для эффективного решения задач экономического развития необходимо объективно оценивать ситуацию в региональной экономике и научно-технический потенциал, с учетом наличных ресурсов, выявить сильные и слабые стороны региона и принять обоснованное управленческое решение. Это невозможно без достоверной и систематизированной информации, которую в значительной степени призван обеспечить мониторинг показателей развития региона. Мониторинг является не только инструментом контроля реализации принятых планов и программ комплексного инновационного развития региона, но и выступает инструментом формирования информационной базы для их разработки.

Мониторинг экономической безопасности следует осуществлять, используя весьма широкий круг показателей, который нужно свести к необходимому и достаточному количеству, сгруппировав их по видам деятельности.

В перечень показателей для мониторинга могут быть включены показатели характеризующие:

● общий экономический потенциал: показатели призваны определить нижнюю границу, экономического развития, выход за пределы которой угрожает стабильности, экономической самостоятельности и устойчивому развитию.

● способность экономики региона к самодостаточному развитию группа показателей обеспечивает комплексную оценку способности экономики функционировать в режиме расширенного воспроизводства; группа включает в себя показатели технического уровня производства и продукции, развития научно-производственного и кадрового потенциала, структуры производства и т. д.

● уровень жизни населения: показатели призванные определить границы, выход за которые угрожает общественному спокойствию и политической стабильности, создает угрозы возникновения социальных и трудовых конфликтов в регионе;

● безопасность финансовой системы: отражают вероятность наступления кризисных ситуаций в бюджетной и денежно - кредитной сферах;

● показатели, характеризующие внешнеэкономическую безопасность: группа отражает устойчивость экономики региона к изменениям внешних условий и функционирования, способность компенсировать возможные воздействия внешней среды на внутреннее экономическое состояние;

● качество управления: экономическим развитием, контролируемость экономических процессов, эффективностью регулирования экономики.

Мониторинг экономической безопасности должен представлять собой интерактивный процесс. Проведение предварительного анализа по заранее определенному перечню показателей неизбежно выявит необходимость осуществления дополнительного анализа и не должен ограничиваться анализом

фактических данных за прошедший период, т.к. не менее (а может быть и более) важен анализ данных прогноза социально-экономического развития на предстоящий год и на среднесрочную перспективу.

Для проведения диагностики социально-экономической безопасности региона рекомендуются следующие показатели:

- отношение средней заработной платы (с учетом выплат социального характера) к прожиточному уровню в регионе;
- уровень преступности (число зарегистрированных преступлений на 100 тысяч человек населения);
- просроченная дебиторская, кредиторская задолженность предприятий и организаций на душу населения;
- задолженность по заработной плате на душу населения;
- уровень безработицы;
- соотношение числа безработных с числом вакансий.

Эти показатели позволяют осуществлять сравнительный анализ социально-экономического положения в регионах, а регулярный сбор информации обеспечивает возможность организации оперативного мониторинга.

В ходе мониторинга факторов, вызывающих угрозы экономической безопасности, недостаточно осуществление мониторинга изменения указанных выше индикаторов по годам за отчетный или прогнозируемый период, так как такой мониторинг не показывает насколько ситуация критична, каков уровень угрозы экономической безопасности. Для этого необходимо сравнение фактических и прогнозных данных с пороговыми значениями, четко определяющими параметры кризисной ситуации.

Для обеспечения региональной социально-экономической безопасности необходима система ее оценки: система индикаторов экономической безопасности региона и муниципального уровня, которая может осуществляться по следующим сферам деятельности (таблица 7).

Каждая из сфер включает определенный набор индикативных показателей (обычно от 3 до 7) для каждого уровня.

Нужно отметить, что в целом индикаторы экономической безопасности региона существенно не отличаются от индикаторов экономической безопасности территорий муниципального уровня.

Проведение мониторинга факторов, учитывая пороговые значения, позволят выявить вероятность наступления кризисных ситуаций в экономике, а также оценить возможный ущерб от этого. За пределами пороговых значений экономика региона будет функционировать в экстремальных режимах. При этом необходимо оценивать по скольким показателям есть угроза выйти за пределы пороговых значений, так как угрожающей становится ситуация, когда нарушается сразу несколько пороговых значений.

Таблица 7

Набор индикативных показателей по различным сферам

На региональном уровне	**На муниципальном уровне**
1. Способность экономики территории к устойчивому росту	
1.1.Инвестиционная безопасность	1.1.Инвестиционная безопасность
1.2.Производственная безопасность	1.2.Производственная безопасность
1.3. Научно-техническая безопасность	1.3.Безопасность собственности
1.4.Внешнеэкономическая безопасность	1.4. Финансовая безопасность
1.5. Финансовая безопасность	1.4. Финансовая безопасность
1.6. Энергетическая безопасность	1.5. Энергетическая безопасность
2. Обеспечение приемлемого уровня существования на территории	
2.1. Уровень жизни населения	2.1 Социальный уровень жизни населения
2.2. Рынок труда	2.2. Рынок труда и оплата труда
2.3. Демографическая безопасность	2.3. Демографическая безопасность
2.4. Правопорядок	2.4. Правопорядок
2.5. Продовольственная безопасность	2.5. Продовольственная безопасность
3. Экологическая безопасность	
3.1. Экологическая защита	3.1. Выбросы вредных веществ

Выход за пределы пороговых значений экономической безопасности не всегда влечет наступление острого кризиса. Это может свидетельствовать лишь о необходимости принятия мер по недопущению или преодолению угроз эко-

номической безопасности.

Необходимо учитывать, что многие показатели должны анализироваться не только в стоимостном, но и в "физическом" измерении, т.е. в постоянных ценах. В этих случаях требуется привязка некоторых количественных параметров пороговых значений экономической безопасности к ценам определенного года.

Типичным случаем является ситуация, когда у региона не хватает финансовых ресурсов для преодоления или недопущения кризисных ситуаций, а также для компенсации возможных ущербов, что потребует определения очередности и приоритетности преодоления наиболее острых угроз экономической безопасности, т. е. необходимости их ранжирования.

Ранжирование (приоритетности) необходимо в случаях, когда финансовых ресурсов недостаточно, а распыление недостаточных ресурсов на преодоление всех угроз одновременно может привести к тому, что в результате не будет устранена в требуемые сроки ни одна угроза. Необходимо ранжирование (приоритетности) устранения тех или иных угроз во времени.

Для проведения ранжирования угроз по очередности (приоритетности), необходимо:

- определить по каждой угрозе уровень агрегированности;
- перечень мер по их устранению;
- определить объем финансирования, необходимого для осуществления мер по устранению каждой угрозы в целом по всем угрозам.

Такие расчеты нужны как примерный ориентир для оценки возможных масштабов разрыва между возможными к использованию для устранения угроз и требуемыми финансовыми ресурсами.

Необходимо иметь механизм выбора приоритетности, так как имеются различные угрозы экономической безопасности: с быстрым сроком наступления и сравнительно небольшими негативными последствиями; с достаточно далекими сроками наступления, но крайне тяжелыми негативными последствиями. Кроме этого имеются и другие проблемы ранжирования угроз экономиче-

ской безопасности, связанные с масштабом негативных последствий и сроками их наступления: особо крупные, крупные и некрупные. Для этого можно ориентироваться на следующие критерии:

- особо крупные: следует считать такие, которые приводят к невозможности нормального функционирования экономики региона.
- крупные: экономика региона сохраняет возможность функционирования, но теряет устойчивость;
- некрупные: при сохранении и возможности функционирования и устойчивости приводят к угрозе невыполнения каких-либо отдельных параметров.

При ранжировании угрозы экономической безопасности следует также учитывать период, необходимый для проведения соответствующих мероприятий. Диагностика кризисных ситуаций включает в себя: мониторинг факторов, вызывающих угрозу экономической безопасности; определение наиболее вероятных угроз экономической безопасности; определение масштабов негативных последствий от действия этих угроз; ранжирование по степени очередности и приоритетности их предотвращения или преодоления. Следующим этапом является обоснование комплексной системы мер обеспечения экономической политики региона.

Таким образом, мониторинг экономической безопасности представляет собой: систему сбора, обработки и анализа информации; оценку и прогнозирование социально-экономической ситуации в регионе; подготовка объективной и достоверной информации о состоянии объектов и территорий региона, оказывающих существенное влияние на безопасность региона в целом, и о возможных отклонениях этого состояния от допустимых значений. Речь идет в первую очередь об отслеживании соблюдении границ показателей (так называемых "порогов безопасности"), нарушение которых может обернуться катастрофическими последствиями, с тем, чтобы принять меры по их недопущению. Система мониторинга регионального развития выступает механизмом выявления и

предотвращения возможных угроз, а информация, полученная в процессе мониторинга, позволяет доступными методами воздействовать на ситуацию.

К числу приоритетных направлений организационно-методических работ в области мониторинга можно отнести:

- определение состава, содержания и периодичности работ по мониторингу с разработкой необходимой нормативно-методической базы и инструментальных средств;
- создание государственной системы информационного обеспечения мониторинга;
- формирование организационных структур по управлению мониторингом и их правовое и финансовое обеспечение.

Различные структуры государственной власти должны выполнять свои функции по обеспечению жесткую регламентации этапов разработки, корректировки и реализации политики государства. Одной из центральных процедур в этом процессе должен стать мониторинг нормативно-правовых документов, выражающих экономическую политику с точки зрения воздействия их на показатели экономического роста, достижения социально значимых результатов благополучия общества и экономической безопасности.

Организация мониторинга соответствующих уровней, разработка показателей по объектам мониторинга должны быть возложены на органы, создаваемые в рамках управления системой экономической безопасности. На рисунке 8 приведена схема проведения работ по диагностике и прогнозированию экономической безопасности. Видно, что цепочка «оценка состояния региона – диагноз – прогноз – стратегия управления» замкнута. Это дает возможность: рассмотрения динамики региона; исследование процессов развития при различных исходных данных и стратегиях управления; создание потенциально возможных сценариев его развития.

Стратегический мониторинг оценивает ход реализации стратегии, возможность и целесообразность ее дальнейшего развития. Оперативный мониторинг дает оценку правильности отдельных функций и работ, отслеживает те-

кущую деятельность по фактическим значениям показателей, сравнивая их с плановыми, нормативными, средними показателями и пороговыми значениями. Стратегический мониторинг направлен на развитие, а оперативный мониторинг – на конкретный результат.

Рис. 8. Схема проведения работ по диагностике и прогнозированию

Основные этапы мониторинга:

1. Определение целей и объектов мониторинга, разработка показателей, выбор средств и методов сбора информации.

2. Сбор, изучение и обобщение информации, формирование информации для анализа.

3. Анализ информации, сравнение фактических данных с пороговыми значениями показателей и оценка перспектив развития.

4. Систематизация и подготовка информации для принятия управленческих решений.

5. Контроль над результатами управленческих воздействий. Разработка мероприятий по устранению негативных последствий в случае их возникновения.

6. Анализ необходимости дальнейшего проведения мониторинга, корректировка системы мониторинга.

7. Выработка прогнозных направлений деятельности региона или корректировка стратегии деятельности в случае необходимости.

Сущность первого этапа заключается в определении целей и объектов мониторинга в соответствии с особенностями и задачами, стоящими перед регионом.

На втором этапе выполняется сбор и регистрация информации, осуществляется оперативный контроль поступления и свода информации.

На третьем этапе анализируется информация, выполняется сравнение данных с пороговыми значениями показателей, изучается динамика показателей. Таким образом, основой системы мониторинга является управление по отклонениям, определяются факторы, вызвавшие эти отклонения.

На четвертом этапе разрабатываются альтернативные управленческие решения, по устранению "узких мест" или определению точек роста приоритетных направлений развития региона.

На пятом этапе оценивается эффективность разработанных управленческих решений, причины, виновники негативных явлений, разрабатываются новые решения.

На последних этапах уточняется методика мониторинга, принимается решение о дальнейшем проведении мониторинга, уточняются цели и направления деятельности региона.

Таким образом, мониторинг является механизмом, обеспечивающим развитие региона. На основе системного наблюдения за ходом и характером количественных и качественных изменений, происходящих в регионе. Мониторинг нацелен в первую очередь на раннее выявление различных сбоев и угроз, потенциально опасных с точки зрения вероятности ухудшения состояния региона и обеспечивает распознавание надвигающегося кризиса, для того, чтобы опера-

тивно отреагировать на него, уменьшить степень риска и избежать катастрофических последствий.

Объективная информация об изменениях, происходящих в регионе, является необходимым условием его развития. Мониторинг дает органам регионального управления оперативную информацию для принятия эффективных управленческих решений в различных ситуациях для обеспечения выбора необходимой стратегии развития.

Вопросы для самоподготовки

1. Какие элементы включает государственная деятельность по обеспечению экономической безопасности страны.

2. Цели мониторинг экономической безопасности.

3. Задачи, которые необходимо решить для достижения целей организации мониторинга.

4. Перечень показателей (пороговые значения) состояния экономики, выход за пределы которых вызывает угрозу экономической безопасности страны.

5. Что оценивается в частных прогнозах.

6. Перечень показателей для мониторинга.

7. Показатели для проведения диагностики социально-экономической безопасности.

8. Набор индикативных показателей по различным сферам.

9. Схема проведения работ по диагностике и прогнозированию.

10. Основные этапы мониторинга.

Литература

1. Павленков, М.Н. Экономическая безопасность: учебное пособие: НГ. Изд-во НГГУ им. Н.И. Лобачевского. 2015 г. – 151 с.

2. Уразгалиев, В.Ш. Экономическая безопасность: учебник и практикум для вузов. – СПб.: Издательство «Юрайт», 2017. – 374 с.

3. Гапоненко, В.Ф., Беспалько, А.Л., Власов, А.С. Экономическая безопасность предприятия. Подходы и принципы. – М.: Издательство «Ось-89», 2007. – 208 с. www.zahvat.ru 33743.pdf.

9. КОНКУРЕНТНАЯ РАЗВЕДКА И КОНТРРАЗВЕДКА В СИСТЕМЕ БЕЗОПАСНОСТИ БИЗНЕСА

9.1. Для снижения ситуационных рисков в процессе развития любого тактического цикла, в том числе для преодоления неожиданных угроз, диссонансов, стрессов и неудач, субъекты предпринимательского бизнеса охотно прибегают к использованию таких специфических инструментов деловой деятельности, как конкурентная разведка и конкурентная контрразведка.

В любой конкурентной ситуации независимо от ее вида перед субъектами бизнеса возникает задача упреждающего выявления источников внутренних и внешних угроз безопасности бизнеса, как и резервов конкурентоспособности, которые порой оказываются гораздо лучше известными соперникам, чем собственному менеджменту. Именно поэтому в арсенале оперативного и ситуационного управления конкурентным поведением компаний так много похожего на инструментарии тайных спецслужб.

Конкурентная разведка (КР) нацелена на всё в мире бизнеса, что сказывается на способности конкурировать. Это – не только конкуренты, прямые, косвенные и потенциальные. Это – и конкуренты, и клиенты, и поставщики, и дилеры, и дистрибьюторы, и технологии и продукция, а также, сама деловая среда. КР должна фокусироваться не только на конкурентах, но и на клиентах, рынках, участниках рынка и деловом окружении, на всем том, где ваша компания желает быть заметной, играть важную роль, быть конкурентноспособной, получать прибыль. Фактически, в КР делается не конкурентный анализ, как таковой, а анализ всего рынка. Целью КР должно быть глубокое понимание не только отдельных его частей, но и всего целого.

9.2. Возможности конкурентной разведки

В настоящее время правильно организованная конкурентная разведка не ограничивается изучением конкурентов. В нее входит, например, изучение по-

литической обстановки, законодательства, кадровых перемещений людей, чья деятельность может оказать влияние на компанию, новых технологий, собственных клиентов и поставщиков компании.

При постоянном использовании конкурентная разведка может дать владельцам бизнеса гораздо больше, чем они предполагают. Вот лишь основные ее возможности:[4]

— прогнозирование изменений на рынке;

— предсказание действий конкурентов и поставщиков;

— выявление новых или потенциальных конкурентов;

— возможность учиться на успехах и ошибках других компаний;

— отслеживание информации, связанной с патентами и лицензиями;

— оценка целесообразности приобретения нового бизнеса;

— изучение новых технологий, продуктов и процессов, которые могут повлиять на конкретный бизнес;

— изучение политических, законодательных или регуляторных изменений, которые могут повлиять на конкретный бизнес;

— оценка соответствия методов ведения бизнеса рыночным реалиям;

— снижение рисков промышленного шпионажа через внутренние каналы;

— использование слабостей конкурента в своей рекламе;

— сбор информации о партнерах и клиентах.

КР помогает выяснить, какие направления деятельности конкурентов отражены в публикациях, но не защищены патентами. Если компания не смогла либо не захотела защитить созданное ею изобретение в соответствии с законом, она не может жаловаться на то, что кто-то воспроизвел изделие или технологию, подобные ее образцам.

КР позволяет быстро выявить признаки искусственного «накачивания» стоимости компании в целях более выгодной продажи.

Помимо информации о наличии криминальных связей и методах решения проблем, принятых у контрагентов, КР позволяет установить источники их фи-

[4] Larry Kahaner «Competitive Intelligence», Simon & Shuster, 1997.

нансирования и, соответственно, снизить риски возможных обвинений в соучастии в отмывании преступных доходов.

Любой специалист КР в области аудита присутствия компании в сети Интернет, обнаруживает сообщения, содержащие адрес для корпоративной электронной почты: приглашение изучить, анкеты, предложения купить услуги или товары. Иногда попадаются старые объявления о уже бывших сотрудниках компании или даже сводки существующих сотрудников.

Такая информация может быть очень интересна недобросовестным конкурентам, которые с удовольствием воспользуются ею для найма сотрудника в качестве информатора.

Блокировка каналов утечки информации не входит в компетенцию КР, однако данные о потенциальных источниках утечки среди сотрудников службы безопасности могут оказаться полезными.

Разнообразным разведывательным действиям (легальным и нелегальным) соперников субъекты предпринимательского бизнеса должны противопоставить активную контрразведывательную деятельность. Под конкурентной контрразведкой понимается профессиональная деятельность компании:

- по затруднению и предотвращению наблюдения за своими действиями извне, а также сбора, обработки и распространению актуальной информации о своих сильных и слабых сторонах;
- по массовому или адресному сокрытию информации об опасных ситуациях, либо по намеренному распространению ее в целях своевременного ознакомления своего окружения с подлинным положением дел или отвлечения внимания конкурентов от наиболее важных аспектов конъюнктуры своего положения;
- по утаиванию и камуфлированию своих истинных намерений, приготовлений и осуществляемых действий; по изготовлению и распространению массовой или адресной дезинформации о действиях фирмы; по производству ситуационного блефа, имеющего характер пропаганды или контрпропаганды;

● по выявлению подготовительных действий соперников, направленных на обострение конкурентных ситуаций, предотвращению навязываемых casus belli;

● по прекращению несанкционированного доступа соперников к сведениям, не подлежащим разглашению;

● по изобличению агентуры, осведомителей, а также сотрудников компании, допускающих халатность в процессе хранения и обработки секретной информации, а также – недобросовестных партнеров и криминалитета;

● по профилактической проверке лояльности сотрудников компании в сочетании с применением мер по прикрытию сотрудников.

Выполнение вышеперечисленных действий способствует снижению угроз и превращению деловой деятельности в менее опасное занятие. При этом ставятся под сомнение и способности соперников по эффективному управлению данной конкурентной ситуацией.

В процессе осуществления контрразведывательной деятельности следует четко представлять, что противник может использовать различные каналы утечки конфиденциальной информации. К основным категориям источников, обладающих конфиденциальной информацией относятся:

● люди, способные выступать не только источниками информации, но субъектами злонамеренных действий противника; таковыми, в частности, являются сотрудники филиалов и региональных представительств компании, от которых обычно легче получить секретную информацию, чем от работников головного офиса;

● документы, размещенные на различных материальных носителях информации;

● публикации, в которых разглашаются (умышленно или необдуманно) конфиденциальные сведения и коммерческие секреты;

● технические носители информации, а именно видео, кино и фотоматериалы, магнитные носители (ленты, диски, дискеты, стриммеры), компакт-диски, распечатки данных и программ, информация на мониторах персо-

нальных компьютеров и табло индивидуального или коллективного пользования;

● технические средства обеспечения бизнеса, такие как телефоны и телефонная связь, телевизоры и промышленные телевизионные установки, радиоприемники, радиотрансляционные системы, системы громкоговорящей связи, усилительные системы и другие, которые по своим параметрам могут быть источниками утечки конфиденциальной информации, а также автоматизированные системы обработки информации;

● производственные отходы так называемый бросовый материал, который может многое рассказать о характере бизнеса компании и ее продукции; тем более, что он получается почти безопасным путем на свалках, помойках, местах сбора металлолома, в мусорных корзинах офисов.

Обезвреживание таких источников становится главной задачей контрразведывательной деятельности субъектов бизнеса в целях обеспечения мер по управлению конкурентными ситуациями. Конкурентные ситуации окажутся вполне управляемыми, если разведка и контрразведка превратятся на фирме в целостный комплекс мотивированных действий.

Разведку и контрразведку нельзя считать самостоятельными конкурентными действиями или приемами конкурентного поведения, они лишь создают информационную базу для быстрого конъюнктурного выбора и последующего тактического поведения субъектов предпринимательского бизнеса.

10. НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

В нынешних очень сложных условиях для бизнеса актуальными становятся вопросы управления рисками: в первую очередь – прогнозирование наиболее значимых рисков и разработка системы для минимизации любого потенциального ущерба в случае неблагоприятных последствий. Это относится ко всем областям деятельности компании, но особую значимость приобретает управление рисками при работе с контрагентами.

Принимая решение о возможности сотрудничества с конкретным контрагентом, компания должна составить более полную картину потенциального делового партнера. И рекомендуется не только получать информацию о том, какой является компания-контрагент на данный момент, но и какова деловая репутация компании, ее основателей и лидеров. При решении вопросов управления рисками необходимо прогнозировать не только риск мошеннического присвоения активов вашей компании, но и значительные риски, которые возникают в отношениях вашей компании с налоговыми органами в случае неоправданного усердия при работе с компаниями-контрагентами.

10.1. «СПАРК-Интерфакс» (система профессионального анализа рынков и компаний) – крупнейшая база данных по компаниям России, Украины и Казахстана с аналитическими функциями.

Основные базовые возможности системы СПАРК в области экономической безопасности обеспечивают решение следующих задач:

- проверка компаний и осуществление оперативного мониторинга контрагентов;
- эффективное выявление фирм-однодневок;
- анализ корпоративных связей;
- поиск, проверка и мониторинг компаний;
- создание различных видов отчетов из данных системы;
- работа со списками и выгрузками по предприятиям и многое другое.

Для решения перечисленных задач в СПАРКе реализуются следующие функции: поиск компаний и предпринимателей по реквизитам; получение выписок из ЕГРЮЛ; выборка предприятий по финансовым показателям; определение взаимосвязей среди руководства, учредителей, дочерних компаний; расчет финансовых показателей на основе собственных формул и отчетов; оценка регионов и отраслей по экономическим, трудовым и статистическим показателям; ранжирование предприятий, страховых компаний и банков; анализ ценных бумаг и многое другое

Аналитические возможности СПАРКа обеспечиваются следующими инструментами и функциями: инструменты для проведения экспресс и комплексной оценки финансового состояния компаний, отраслей и регионов; возможность создания своих собственных методик оценки бизнеса или создания своего собственного представления информации в системе; анализ кредитных рисков; поиск основных производителей и потребителей товаров или услуг и выявление их доли рынка; построение рэнкингов предприятий, банков, страховых компаний по различным финансовым показателям и расчетным коэффициентам; поиск взаимосвязей между компаниями по совладельцам, руководству или аффилированным лицам, возможность визуализации всех прямых и косвенных связей; оценка места компании в отрасли и/или регионе и сравнение с другими аналогичными компаниями.

Основные партнеры СПАРКа: федеральная налоговая служба; периодичность обновления: ежедневно, ежемесячно; федеральная служба государственной статистики; периодичность обновления: ежемесячно, ежеквартально, бух-

галтерские балансы – ежегодно; федеральная служба по финансовым рынкам; периодичность обновления: ежемесячно; центральный Банк России; периодичность обновления: ежемесячно; высший арбитражный суд; периодичность обновления: ежедневно; федеральное агентство по управлению государственным имуществом; периодичность обновления: ежемесячно; федеральное Казначейство (Казначейство России);периодичность обновления: ежемесячно; вестник Государственной Регистрации; периодичность обновления: еженедельно; депозитарий финансовой отчетности Республики Казахстан; периодичность обновления: ежедневно, по мере обновления; роспатент; периодичность обновления данных: ежемесячно, по мере поступления; международная корпорация Dun & Bradstreet; единый федеральный реестр сведений о банкротстве; периодичность обновления данных: ежедневно.

Пользователями СПАРКа являются: департаменты рисков банков и компаний; аналитические подразделения холдингов, банков, инвестиционных компаний; службы безопасности; маркетинговые службы, отвечающие за оценку рыночного окружения своих компаний, выявление потенциала рынков, поиск новых направлений деятельности; отделы материально-технического снабжения, подразделения, занимающиеся организацией сбыта; кредитные и лимитные подразделения банков; страховые, консалтинговые, аудиторские компании; оценщики и арбитражные управляющие; информационные и мониторинговые агентства, СМИ; подразделения министерств и государственных ведомств, отвечающие за мониторинг предприятий отрасли или региона; высшие учебные заведения.

СПАРК для своей работы использует следующие источники информации: Росстат РФ и Агентство Республики Казахстан по статистике; собственные источники по Украине; ФСФР РФ; Федеральная налоговая служба РФ; Росимущество; Высший Арбитражный Суд РФ (Банк решений арбитражных судов); «Российская газета» и Коммерсантъ; сообщения о банкротствах с 1999 года; информация непосредственно от организаций и банков; Интернет – Яндекс, Google, Headhunter.ru, moikrug.ru; СМИ: федеральная и региональная пресса,

отраслевые издания, транксрипты ТВ и радио; собственный колл-центр Интерфакса; Российские и зарубежные биржи.

Базовый состав информации, который берется из источников: реквизиты компании, сведения о регистрации в регистрирующих органах, лицензии; структура компании, совладельцы, дочерние компании, филиальная сеть, состав руководства; статистическая и финансовая отчетность компаний, адаптированная для фундаментального анализа, финансовые и расчетные коэффициенты, в том числе и отраслевые, сведения об аудиторских проверках; финансовая отчетность банков и страховых компаний; скоринговые оценки, в том числе и кредитных рисков; описание деятельности компании, планов ее развития, существенные события, анонсы корпоративных событий; информация о выпусках ценных бумаг, календарь событий по акциям и облигациям, котировки, сведения о регистраторе; рекомендации аналитиков, аналитические обзоры и комментарии; база данных по банкротствам и решениям арбитражных судов; сообщения СМИ, различная публичная информация; сведения об обязательствах компании, информация об участии в гостендерах.

10.2. Проверка контрагентов в системе СПАРК

Минфин напомнил, как налоговики рекомендуют налогоплательщикам проверять контрагентов (от 17.12.2014 № 03-02-07/1/65228).

На сайте ФНС размещаются сведения об адресах, указанных при госрегистрации в качестве места нахождения несколькими юрлицами (адреса "массовой регистрации", характерные для "фирм-однодневок"), и наименования юрлиц, в состав исполнительных органов которых входят дисквалифицированные лица.

Ссылаясь на анализ судебной практики, Минфин перечислил признаки "фирмы-однодневки": наличие "массового" учредителя (участника); "массового" руководителя; отсутствие организации по адресу регистрации; отсутствие персонала; отсутствие налоговой отчетности либо ее представление с минимальными показателями; наличие численности организации в составе 1 челове-

ка; отсутствие собственных либо арендованных основных средств, транспортных средств.

Представляется, что выводы о проявлении налогоплательщиком должной осмотрительности и осторожности при выборе контрагентов можно делать, исследуя конкретные обстоятельства, заключил Минфин.

Для того чтобы оценить уровень благонадежности компании-партнера, снизить риски ведения бизнеса и проявить тем самым должную осмотрительность, Интерфакс предлагает воспользоваться готовым скорингом в СПАРКе.

Доступны следующие скоринги системы СПАРК: индекс должной осмотрительности; индекс финансового риска; индекс платежной дисциплины.

10.3. Web-сервис Контур.Фокус – быстрая проверка контрагента.

«Контур.Фокус» – онлайн-сервис оперативной проверки контрагентов. С «Контур.Фокусом» открытая информация о миллионах юридических лиц и индивидуальных предпринимателях России становится доступной.

Вся информация получается только из основных открытых источников:

- ЕГРЮЛ/ЕГРИП ФНС России;
- Информация Росстата (годовая бухгалтерская отчетность компаний);
- Реестр госконтрактов Федерального казначейства;
- Картотека арбитражных дел Высшего арбитражного суда.

С помощью сервиса становится возможным оперативно проверить:

- Реквизиты организаций
- Финансовую информацию о предприятиях, основанную на годовых бухгалтерских отчетах
- Связи между компаниями
- «Массовость» руководителей и учредителей организаций
- Номера выданных лицензий, свидетельств, филиалы и представительства
- Сведения о государственных контрактах
- Арбитражные дела компании

Вся информацию об интересующей компании может быть получена в течение нескольких секунд:

- Единая строка поиска «как в Яндексе»
- Автоматическое исправление опечаток
- Возможность фильтровать запросы по регионам и отраслям
- Информация о компании из всех источников сосредоточена в одном месте
- Возможность в один клик выявить связи между организациями по различным параметрам: по адресу, руководителям и учредителям

В Контур.Фокусе появилась возможность анализировать компании массово. Для этого достаточно загрузить список организаций и построить по нему сводку, и можно применять знакомые инструменты анализа списка связанных компаний, но только для произвольного списка.

В Контур.Фокусе есть три основных ингредиента: связи, маркеры и списки. С помощью их сочетания можно решать разные практические задачи. Например, сейчас появилась возможность массово проверять организации за счет комбинации списков и маркеров.

Где это может быть применимо?

1. При стартовой проверке своих контрагентов, когда контрагенты никогда ранее не проверялись. Достаточно импортировать организации в список и провести массовую проверку.

2. При проверке группы компаний, когда группа собирается вручную.

10.4. Система анализа медиасреды «СКАН-Интерфакс»

Поисковая база данных для анализа информации и медиамониторинга «СКАН-Интерфакс» является эффективным инструментом для мониторинга СМИ, обработки деловой информации и графического анализа.

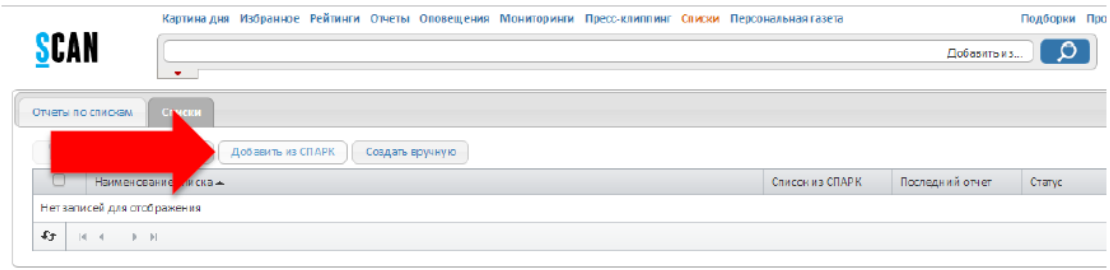
Для оценки уровня благонадежности компании-партнера и снижения риска ведения бизнеса в системе СКАН доступен скоринг Индекс Репутационного Риска (ИРР). Индекс Репутационного Риска (ИРР) рассчитывается по 30 000 юридических лиц и помогает оценить целесообразность работы с тем или иным контрагентом.

Он делится на 3 зоны: зеленую – негатива почти не было или его доля незначительна среди общего объема публикаций, желтую – система зафиксировала негативные сообщения, контрагент требует дополнительной проверки, а СКАН позволяет заказать детальный отчет; и красную – количество негативных сообщений критично, работа с этим контрагентом может нанести урон репутации вашей компании.

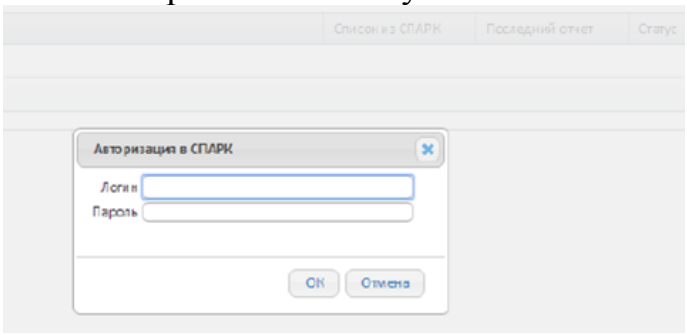
Алгоритм расчета ИРР построен таким образом, что учитывает размер компании и количество сообщений за последние 12 месяцев. Если сообщений по компании было меньше 100, то индекс не рассчитывается.

Постановка контрагентов из списка на мониторинг для определения Индекса Репутационного Риска

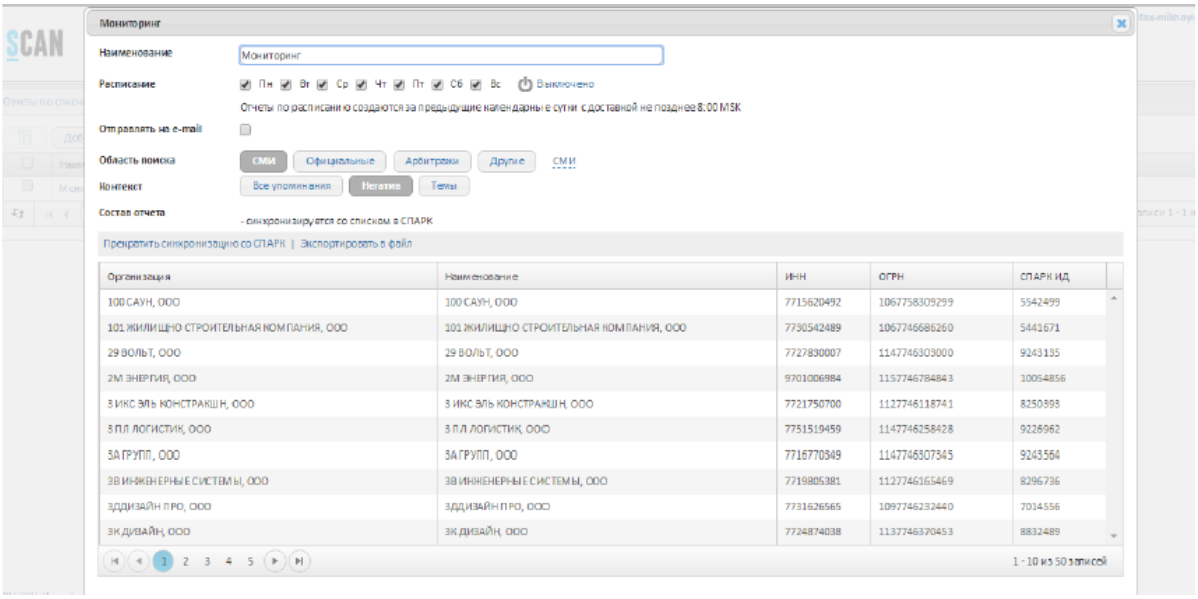
Для клиентов системы СПАРК, поставивших списки своих контрагентов на мониторинг в СПАРКе, возможно поставить их на мониторинг репутационных рисков в СКАНе автоматически. Для этого необходимо выполнить следующие действия (см. рисунки, представленные ниже).



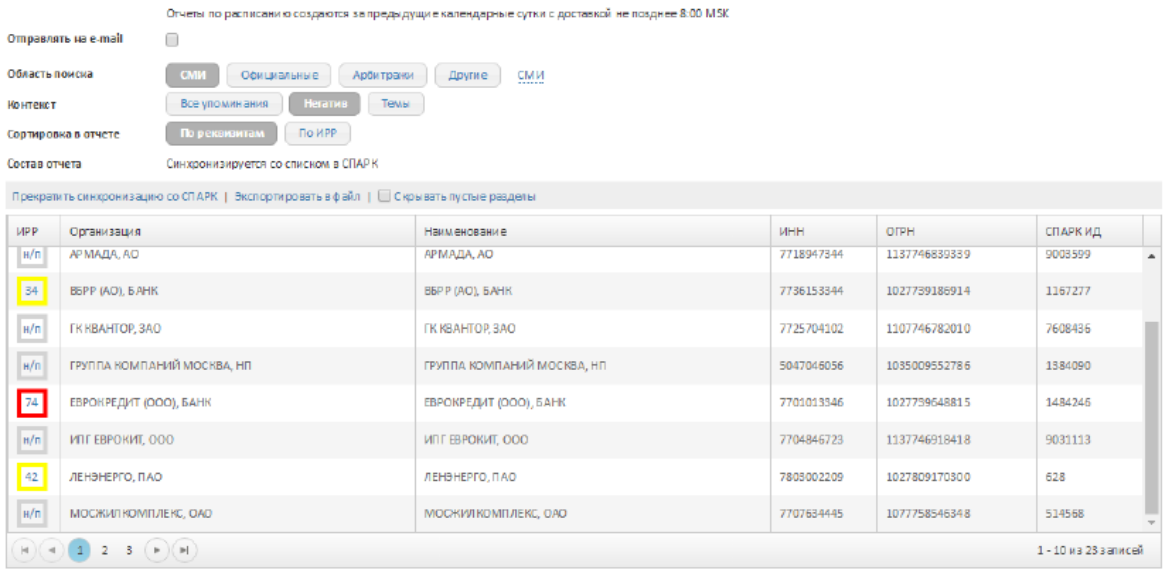
Ввести свой логин и пароль к СПАРКу:



В результате будет получен список из СПАРКа в интерфейсе СКАНа, чтобы осуществлять контроль за репутационными рисками организаций, с которыми работаете.



Если предварительно настроены списки мониторинга контрагентов, то напротив каждого, по которому рассчитывается ИРР, появится соответствующее значение:



10.5. Возможности Спарк – Маркетинга

СПАРК-Маркетинг содержит публичные данные по государственным и коммерческим закупкам и продажам по всей стране, которые обновляются в онлайн режиме.

Используя эти сведения, возможно изучение истории аналогичных закупок, понять, насколько конкурентен рынок товара/услуги, не пропустить интересующий тендер, спрогнозировать действия конкурента, оценить вероятность победы на торгах.

Система интересна широкому и разностороннему кругу пользователей за счет большого объема информации, сервисов и отчетов, разработанных с применением уникальных технологий обработки данных.

Индикаторы контроля в «СПАРК-Маркетинге» позволяют выявлять 4 вида рисков: процедурные нарушения; ограничение конкуренции; неэффективное расходование бюджетных средств; некачественное исполнение контрактов. В общей сложности это почти три десятка признаков, и список индикаторов постоянно пополняется. В итоге пользователь получает таблицу, из которой видно, какие индикаторы контроля «сработали» в интересующих его закупках. Здесь же показана вся цепочка – от объявления торговой процедуры до заключения контракта.

Для сужения поиска можно использовать фильтры: покупатель, продавец, регион поставки, сфера деятельности, размер начальной (максимальной) цены контракта (НМЦК) и т.д.

Ни один индикатор не является, конечно, прямым указанием на нарушение. Это лишь признаки, позволяющие ориентироваться в типологии возможных злоупотреблений, информация для дальнейшей детальной работы контролеров.

Вопросы для самоподготовки

1. Основные задачи, решаемые в системе СПАРК, в области экономической безопасности.
2. Основные функции СПАРКа.
3. Аналитические возможности СПАРКа.
4. Основные партнеры СПАРКа.
5. Пользователи СПАРКа.
6. Источники информации для СПАРКа.
7. Базовый состав информации для СПАРКа.
8. Возможности СПАРК для проверки контрагентов.
9. Скоринги системы СПАРК.
10. Возможности Web-сервиса «Контур.Фокус» для проверки контрагентов.
11. Система анализа медиасреды «СКАН-Интерфакс».

12. Скоринг Индекс Репутационного Риска (ИРР).

13. Возможности Спарк – Маркетинга.

Литература

1. http://www.spark-interfax.ru/ru/articles/obnovleniye-spark-release-3-08

---

11. КОМПЛЕКСНАЯ ОЦЕНКА БЛАГОНАДЕЖНОСТИ КОНТРАГЕНТОВ И УПРАВЛЕНИЕ НАЛОГОВЫМИ РИСКАМИ С ИСПОЛЬЗОВАНИЕМ ИАС «1СПАРК-РИСКИ»

11.1. Современные предприятия в своей деятельности помимо ежедневного риска столкнуться с некачественным выполнением работ поставщиком, отказом заказчика от оплаты предоставленной услуги, с фирмами-однодневками, должны нести ответственность за работу с недобросовестными контрагентами, через которые выполняются не вполне законные операции (например, всевозможные виды обналичивания денег).

Максимально удобную и недорогую возможность снизить возможные финансовые потери при работе с другими предприятиями и организациями дает использование системы интеллектуального анализа данных.

Сервис «1СПАРК-Риски», совместный проект фирмы «1С» и информационной группы «Интерфакс», позволит пользователям программ системы «1С: Бухгалтерия 8» комплексно оценивать благонадежность контрагентов, управлять налоговыми рисками и принимать управленческие и финансовые решения.

Сотрудничество фирм «Инферфакс» и «1С» призвано вывести систему СПАРК на рынок малого и среднего бизнеса через партнерскую сеть. Сервис

«1СПАРК-Риски» представляется в виде встроенной опции в деловых приложениях системы «1С» (например, «1С: Бухгалтерия 8» (ред. 3.0)).

Для руководителей предприятий и лиц, принимающих бизнес-решения, бухгалтеров, специалистов финансовых служб и др. сервис окажет неоценимую услугу. Возможность получения оперативной информации о благонадежности контрагентов в виде набора пользующихся доверием на рынке скоринг-индексов системы СПАРК станет хорошим подспорьем бизнес-пользователям. При желании пользователи смогут получать развернутую информацию о своих поставщиках и покупателях в виде справки из системы СПАРК, заверенной электронной подписью «Интерфакса» (эти документы уже несколько лет применяются в судебной практике) и будут оперативно оповещаться о важнейших изменениях в статусе своих контрагентов: банкротство, изменения в руководстве, присоединение к другой компании и т. д.

В основе данного решения лежит база данных юридических лиц СПАРК-Интерфакс, в которой собраны сведения о финансовом состоянии практически всех компаний в стране. 150 из «ТОП-200» крупнейших компаний по версии Forbes используют СПАРК-Интерфакс для проверки контрагентов, управления кредитными и налоговыми рисками, маркетинга и инвестиционного анализа. Теперь эффективные аналитические инструменты оценки контрагентов становятся доступными для предприятий среднего и малого бизнеса.

Сервис «1СПАРК-Риски» позволяет вычислить с помощью имеющихся данных коэффициенты, характеризующие платежеспособность компании, и в последующем на их основе вывести индексный показатель, который позволяет принять решение о целесообразности сотрудничества с той или иной компанией. Это позволит снизить риск не получить оплату по выставленным счетам от предприятия с низкой платежеспособностью.

«1СПАРК-Риски» встроен в программы 1С и предоставляет пользователям информацию для принятия обоснованных решений:

- оценка контрагентов на основе индексов системы СПАРК позволяет принять взвешенное решение о целесообразности сделки с контрагентом,

предотвратив возможность сделки с недобросовестным поставщиком или неплатежеспособным покупателем.

- мониторинг информации о контрагентах по данным СПАРКа помогает вовремя отреагировать на действия контрагента, в связи с планами контрагента по реорганизации, ликвидации и т.д.
- заверенная бизнес-справка системы «1СПАРК-Риски», содержит развернутую информацию об основных существенных индикаторах деятельности контрагента, таких как выявленные факторы риска, финансовые показатели, проверки государственными органами и др. Документом, подтверждающим проявление должной осмотрительности контрагента, является бизнес-справка.

Кроме того, «1СПАРК-Риски»:

- помогает проявить должную осмотрительность и снизить налоговые риски;
- помогает выиграть споры при возмещении НДС;
- принимать решение на этапе выбора поставщика;
- принимать решение о том, стоит ли давать кредит;
- помогает контролировать дебиторскую задолженность;
- снижает прямые финансовые риски в случае попытки мошеннических действий контрагентов.

11.2. Оценка контрагентов на основе индексов системы СПАРК:

- *Индекс должной осмотрительности (ИДО)* - скоринговая модель, позволяющая оценить на основе всего комплекса имеющейся информации вероятность того, что та или иная компания является однодневкой, транзитной компанией, брошенным активом.

ИДО представляет собой значение от 1 до 99, где более высокое значение отражает большую вероятность того, что компания создана не для уставных целей, а в качестве "транзакционной единицы", не имеющей существенных собственных активов и операций, или является "брошенным" активом.

Индекс рассчитывается с помощью таких аналитических методов, как модель логистической регрессии, модель классифицирующих и регрессионных деревьев, а также моделей, основанных на гибридных нейро-нечетких сетях.

Факторное пространство ИДО включает в себя такие параметры, как свежесть последней представленной в органы статистики отчетности компании, наличие массового директора и массового адреса регистрации, учитывает значения некоторых показателей финансовой отчетности компании и их динамику.

ИДО учитывает 40 факторов: от стандартных признаков «однодневности» до активности в интернете, участия в госзакупках, наличия патентов, лицензий, судебных споров, задолженности по налогам, залогов и т. д.

ИДО был разработан в 2010 году, с тех пор его методика постоянно совершенствовалась и развивалась с учетом изменения «поведения» фирм-однодневок. Применение ИДО соответствует критериям должной осмотрительности, рекомендованным ФНС России. Кроме того, ИДО – важный элемент анализа кредитных рисков.

Если в системе ИДО в зеленой зоне – ваш партнер имеет все признаки благонадежности, а если индекс в красной зоне, то перед сделкой рекомендуется более детально проверить контрагента.

Использование ИДО для оценки «риска однодневности»: значение индекса 1-40 – низкий риск; значение индекса 41-70 – средний риск (рекомендуется сбор дополнительной информации); значение индекса 71-99 – высокий риск (сбор дополнительной информации обязателен).

Как показывает ИДО, число компаний, имеющих признаки однодневности, сократилось с 1,7 млн в 2011 году до чуть более 600 тыс. в настоящее время. Доля потенциальных однодневок среди зарегистрированных в России компаний снизилась за это время с 45 % до 15 %.

- *Индекс финансового риска (ИФР)* анализирует финансовое состояние компании с точки зрения возможного банкротства. ИФР классифицирует юридические лица по трем уровням риска, учитывая 11 коэффициентов, базирующихся на финансовой отчетности компании.

ИФР представляет собой меру риска несостоятельности компании. Его высокие значения указывают на наличие признаков неудовлетворительного финансового состояния, которые могут привести к тому, что компания утратит платежеспособность.

Для расчета индекса используются комбинированные финансовые коэффициенты компании, такие как коэффициенты ликвидности, достаточности оборотных средств, автономии и другие. Модель построена с использованием нейросетевого моделирования.

Если ИФР находится в красной зоне, рекомендуется проявлять осторожность при предоставлении товаров и услуг на условиях отсрочки платежа. Отсутствие ИФР говорит о том, что компания не сдает финансовую отчетность в органы статистики.

- *Индекс платежной дисциплины (ИПД) (Paydex)* – это аналитический показатель, отражающий средний фактический срок исполнения компанией финансовых обязательств по различным контрактам. Данные о платежах по счетам поступают в СПАРК на добровольной основе от крупных энергоснабжающих, коммунальных, телекоммуникационных, торговых и иных предприятий. ИПД рассчитывается примерно для 100 000 юридических лиц.

Значение индексов является скоринговыми аналитическими показателями, рассчитываемыми на основании публично доступной информации о деятельности юридического лица. За достоверность указанной информации Интерфакс ответственности не несет. Оценка компании может быть автоматически изменена при получении новой и/или дополнительной информации. Данная оценка является мнением Интерфакс и не дает каких-либо гарантий или заверений третьим лицам, а также не является рекомендацией для покупки, владения или продажи ценных бумаг, принятия (или непринятия) каких-либо коммерческих или иных решений.

11.3. Мониторинг информации о контрагентах

Мониторинг позволяет получать оповещения о важных изменениях в жизни контрагента: реорганизация, ликвидация, смена адреса, телефона, руко-

водителя, учредителей и т.п. Оповещения о событиях мониторинга можно просматривать непосредственно в программах 1С и в личном кабинете на портале 1С: ИТС. Отслеживание изменений в жизни контрагента происходит на основе использования множества различных источников информации, в том числе: ЕГРЮЛ, Единый федеральный реестр сведений о фактах деятельности юридических лиц, «Вестник государственной регистрации». Система мониторинга контрагентов позволяет вовремя реагировать на изменяющиеся условия ведения бизнеса.

Особенности мониторинга контрагентов с помощью сервиса «1СПАРК Риски»:

❖ Предупреждение о важных событиях у контрагентов раньше, чем они появляются в ЕГРЮЛ.

❖ Сообщения на начальной странице программы и при формировании платежного поручения.

В мониторинг контрагентов попадает:

• Изменение статуса компании с системе СПАРК

• Изменение адреса

• Смена совладельцев

• Смена руководителя

• Введение процедуры банкротства

• Подача заявление по форме Р

• Сообщения в Вестнике гос. регистрации.

Примеры формы Р:

Р 11001 Заявления о государственной регистрации юридического лица при создании;

Р-12003 Уведомление о начале процедуры реорганизации;

Р-14002 Заявление о внесении в ЕГРЮЛ сведений о нахождении хозяйственного общества в процессе уменьшения уставного капитала;

Р-15001 Уведомление о ликвидации юридического лица;

Р-34002 Заявление физического лица о недостоверности сведений о нем в ЕГРЮЛ.

Примеры статусов:

• Действующая

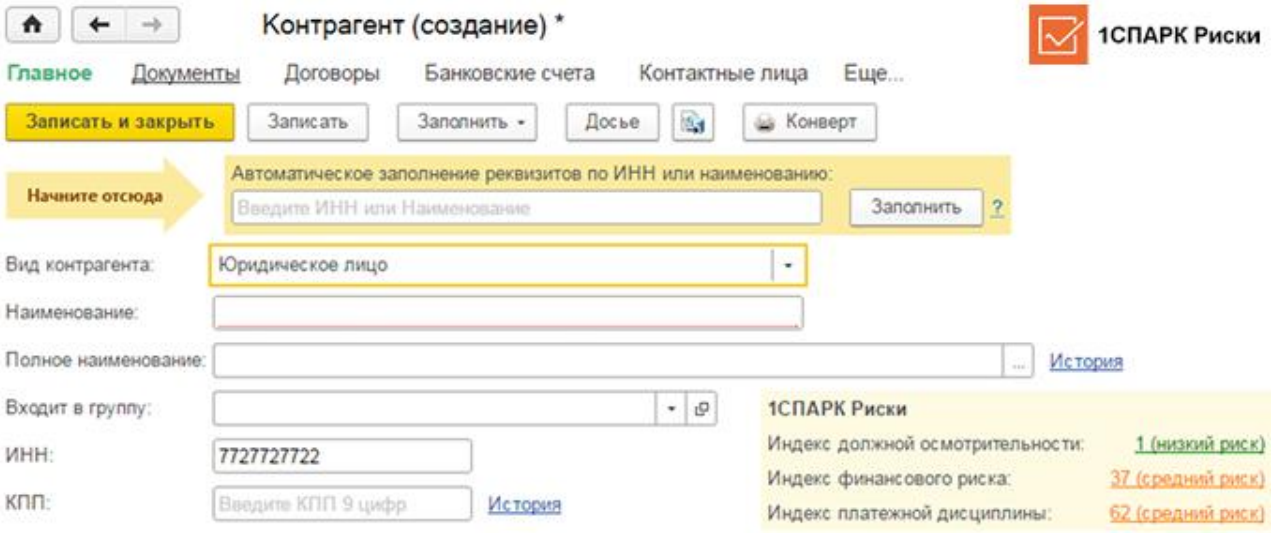
• В процессе реорганизации

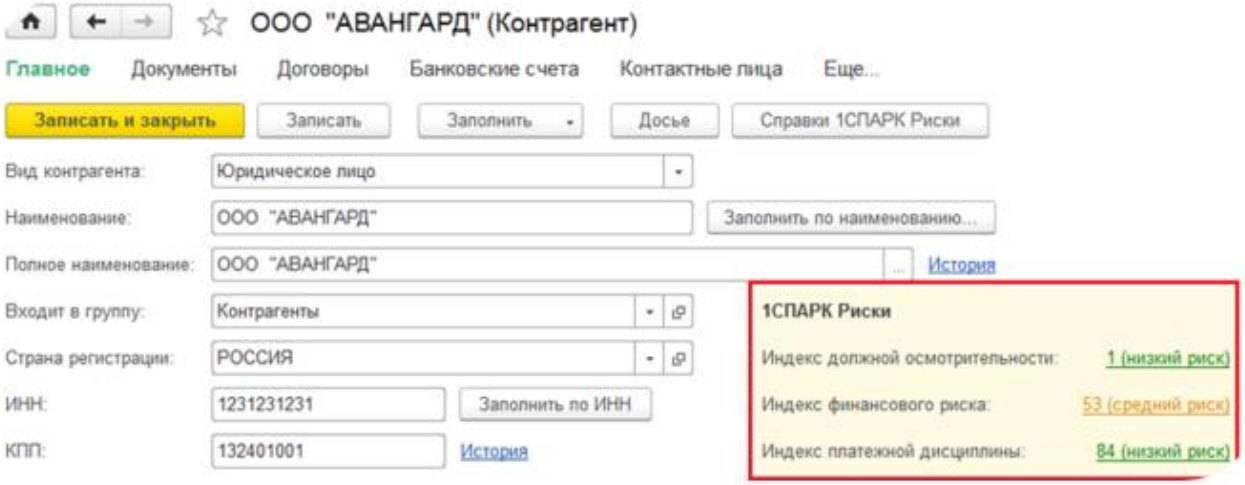
• В стадии ликвидации

• Ликвидация в следствии банкротства

• Ликвидация недействующего юрлица

• Ликвидирована





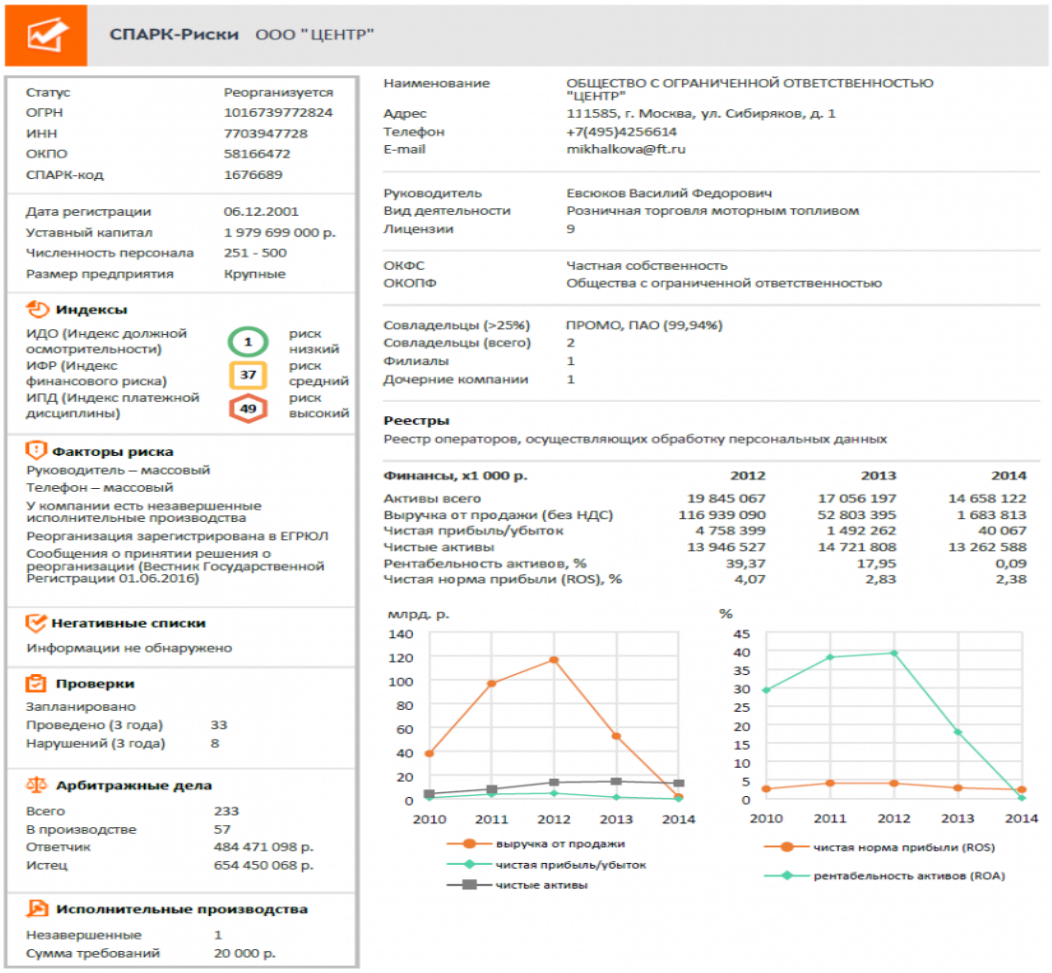
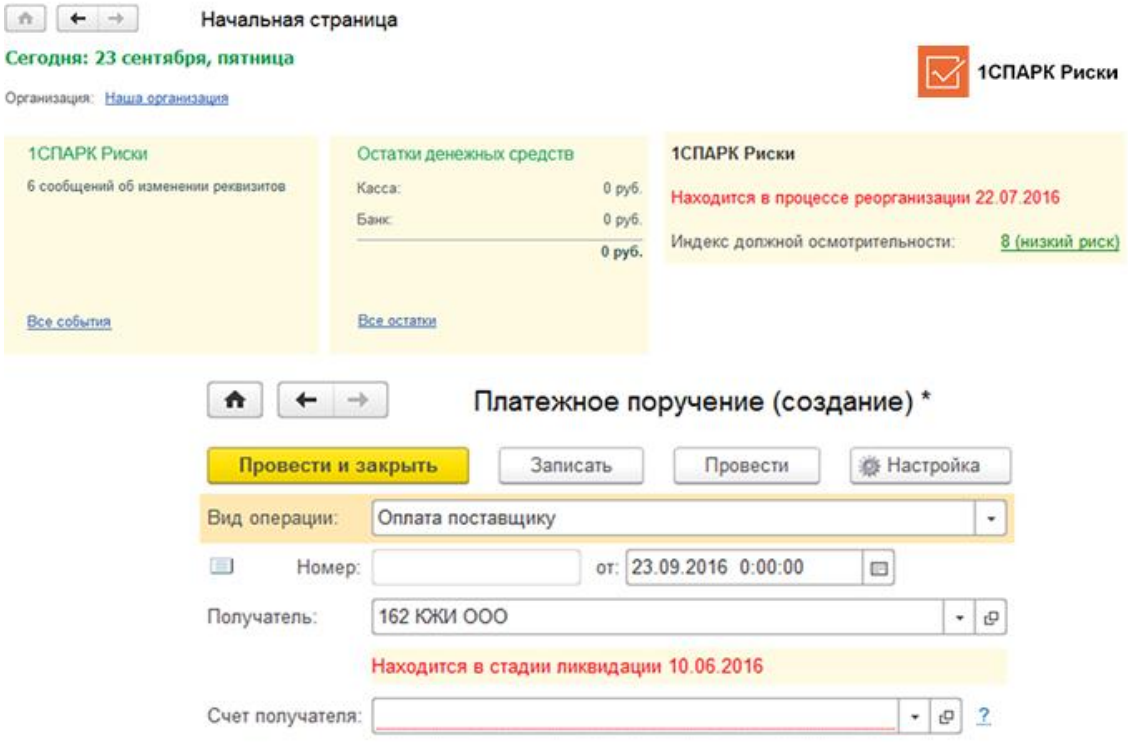


Рис. 9. 1СПАРК – Риски. Оценка благонадежности контрагента



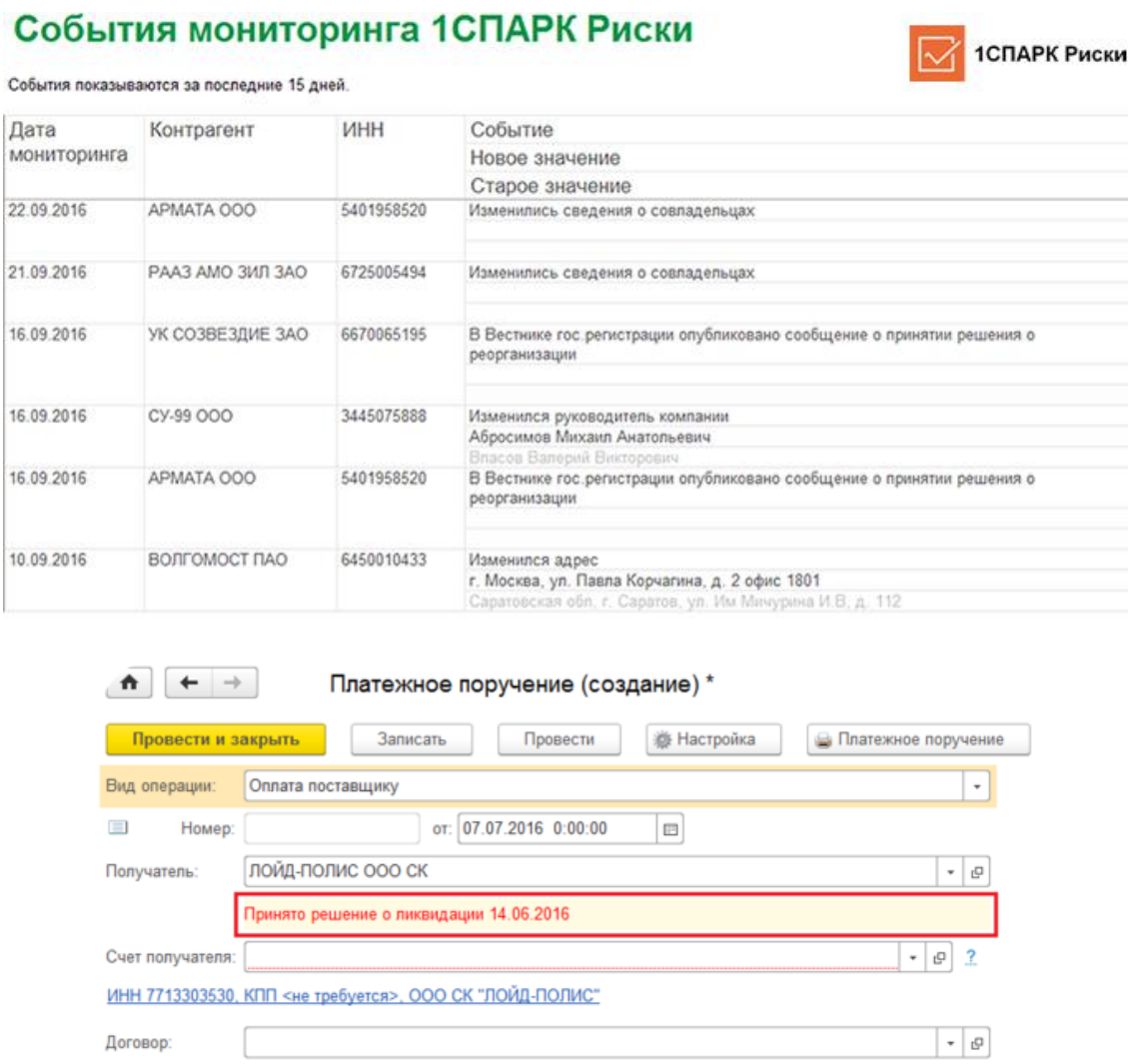


Рис. 10. 1СПАРК – Риски. Мониторинг информации о контрагентах

11.4. Бизнес-справка с подробной информацией о контрагенте, заверенная электронной подписью Интерфакс.

Бизнес-справку о компании является юридически значимой и заверяется электронной подписью агентства «Интерфакс».

Бизнес-справка:

содержит необходимую информацию для экспресс-оценки благонадежности контрагента;

может использоваться в спорах с налоговой инспекцией, поскольку является юридически значимой;

может быть получено неограниченное количество справок по конкретному юридическому лицу;

можно предъявлять справку в суде или в контролирующих органах как доказательство проявления должной осмотрительности при работе с контрагентами.

Бизнес-справка о компании хранится 3 года, ее можно скачать на Портале 1С:ИТС.

Рис. 11. 1СПАРК – Риски. Бизнес-справка о контрагенте

11.5. С помощью встроенных инструментов, программа позволяет решать следующие задачи:

- минимизировать риски несвоевременной поставки оплаченных товаров;
- минимизировать риски формирования просроченной дебиторской задолженности;
- минимизировать риски отказа в вычете сумм налога на добавленную стоимость со стороны контролирующих органов.

Например, сервис «1СПАРК-Риски» позволяет проанализировать тенденции своевременной оплаты счетов контрагентами. В случае, когда по сведениям, имеющимся в базе данных сервиса, покупатель обладает низкой платежной дисциплиной необходимо предпринять возможные действия для страховки рисков несвоевременного осуществления платежей: включить в договор пункт о наличии существенных пеней за нарушение сроков оплаты, предусмотреть залог или упрощенную процедуру подачи иска в суд в случае возникновения просроченной задолженности.

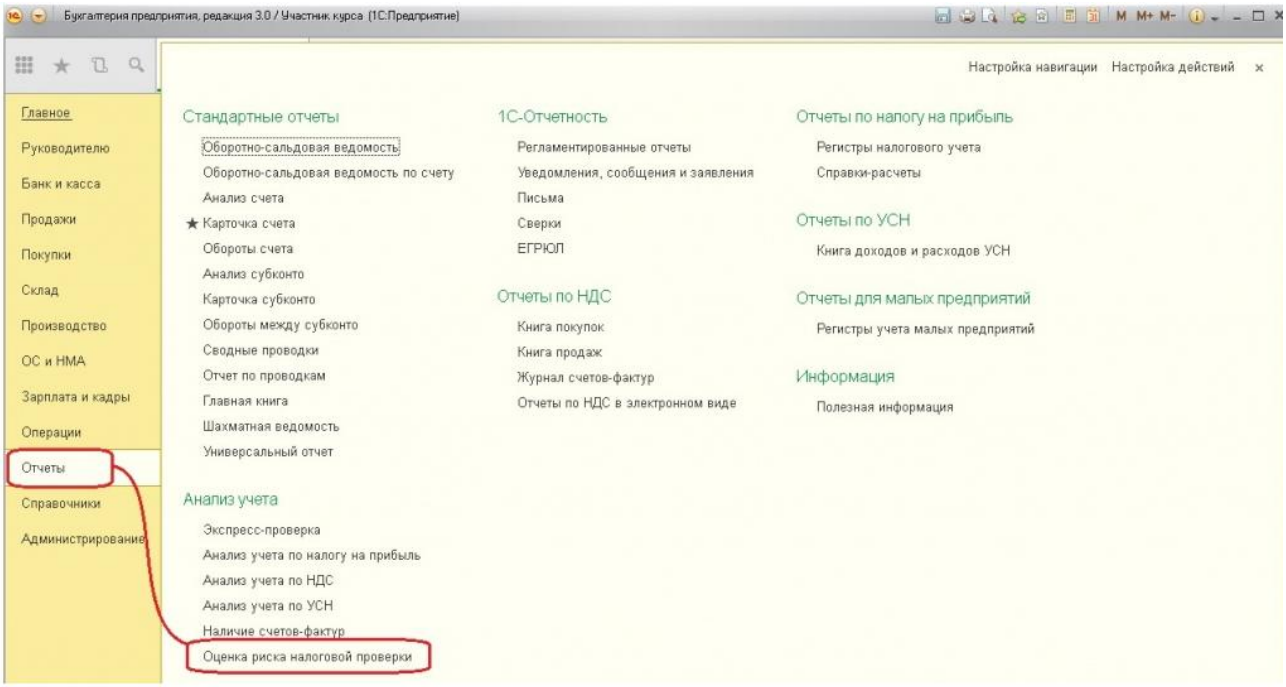


Рис. 12. 1СПАРК – Риски. Встроенный инструмент

При принятии решения об осуществлении оплаты контрагенту за еще не поставленный товар информация сервиса «1СПАРК-Риски» о нем, как о финансово неустойчивом, позволит правильно решить, что лучше – отказаться от сотрудничества или оплатить только после получения товара, услуги.

Существенно важной является информация сервиса «1СПАРК-Риски» позволяющая проанализировать благонадежность партнера с точки зрения налоговых платежей. Отсутствие регулярных платежей по налогам и сборам говорит о высокой вероятности того, что контролирующие органы операции с таким контрагентом признают фиктивными и не позволят учесть в расходах и при расчете налога на добавленную стоимость, а, следовательно, появляется риск для

предприятия в виде до начисления сумм налогов и пеней по ним и проведения выездной налоговой проверки. Предварительная проверка налоговых рисков с использованием сервиса «1СПАРК-Риски» позволит избежать этого.

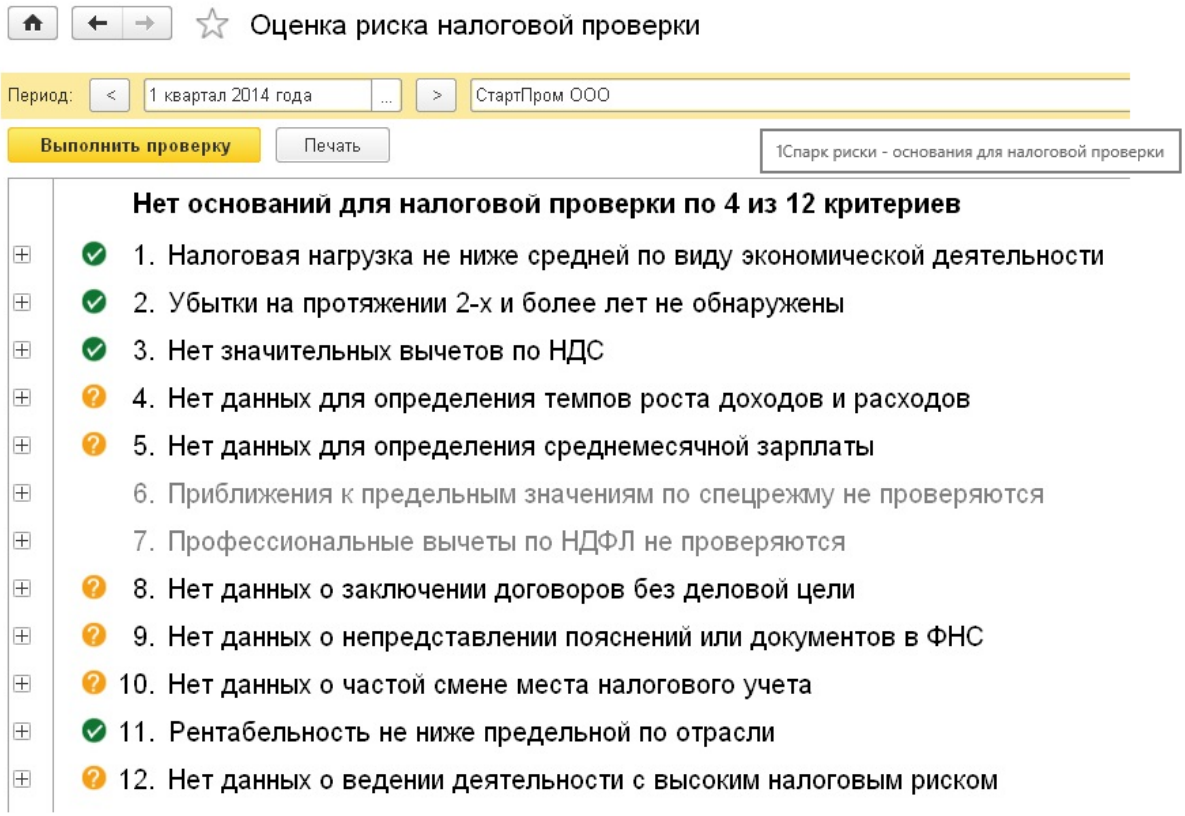


Рис. 13. 1СПАРК – Риски. Оценка риска налоговой проверки

11.6. Программы, в которых реализован сервис «1СПАРК-Риски»:

- «1С:Бухгалтерия 8» (ред. 3.0) с версии 3.0.43.253;
- «1С:Бухгалтерия 8» (ред. 3.0) базовая с версии 3.0.43.253;
- «1С:Бухгалтерия 8» (ред. 3.0) КОРП с версии 3.0.43.253;
- «1С:Бухгалтерия 8» (ред. 3.0) базовая для 1 с версии 3.0.43.253;
- «1С:Управление холдингом 1.2» с версии 1.2.14.5;
- «Управление небольшой фирмой 1.6» с версии 1.6.7.43;
- «Бухгалтерия государственного учреждения (ред. 2.0)» с версии 2.0.48.34;
- «1С:ERP Управление предприятием 2» с версии 2.2.2.127;
- «1С:Комплексная автоматизация 2» с версии 2.2.2.129;

- «1С:Управление торговлей, редакция 11» с версии 11.3.2.157;
- «1С:Бюджет муниципального образования 8» с версии 1.3.4.6;
- «Розница, редакция 2.2» с версии 2.2.5.22;
- «Розница, редакция 2.2 базовая» с версии 2.2.5.22;
- в "облачных" решениях, предоставляемых на сервисе 1cfresh.com: "1С:Бухгалтерия 8", "1С:Предприниматель 2015", "1С:Управление небольшой фирмой", "1С:Бухгалтерия государственного учреждения".

Вопросы для самоподготовки

1. С использованием какой базы данных создан сервис "1СПАРК Риски".
2. Основные функции сервиса "1СПАРК Риски".
3. Оценка контрагентов на основе индексов системы СПАРК.
4. Является ли бизнес-справка юридически значимым документом?
5. Каковы особенности мониторинга контрагентов с помощью сервиса "1СПАРК Риски".
6. Мониторинг информации о контрагентах.

Литература

1. http://www.spark-interfax.ru/1cspark
2. https://portal.1c.ru/download/public/instruction/1spark-report.pdf
3. https://portal.1c.ru/download/public/instruction/Instructions_1SPARK_Risks_account_3.0.pdf
4. https://portal.1c.ru/applications/47
5. https://buh.ru/articles/documents/48913/
6. http://net-consult.ru/services/1spark_riski/

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 1. Оценка риска информационной безопасности предприятия.

Цель: изучить методику и приобрести практические навыки по оценки рисков информационной безопасности предприятия.

Практическое занятие предназначено для проведения оценки рисков информационной безопасности (ИБ) в рамках совершенствования системы информационной безопасности на предприятиях малого и среднего бизнеса.

Постановка задачи. Основная задача данной методики заключается в том, чтобы определить численный показатель риска ИБ с целью принятия эффективных мер по защите информации. Предлагаемая методика оценки рисков позволяет выполнить полноценный анализ и оценку рисков без привлечения высококвалифицированных специалистов.

Обобщенный алгоритм проведения оценки рисков ИБ на предприятиях малого и среднего бизнеса (далее МСБ) приведен ниже.

Алгоритм оценки рисков ИБ

Этап 1	Идентификация
Этап 2	Определение риска и соответствия требованиям законодательства
Этап 3	Разработка модели угроз
Этап 4	Процедура количественного определения риска
Этап 5	Определение обобщенного допустимого уровня риска

Процедуры оценки рисков ИБ как комплексного подхода выполняются сотрудниками предприятия совместно с руководящим звеном, а также с сотрудниками отделов предприятия.

Этап 1. Идентификация активов. На данном этапе эксперты проводят интервью с персоналом каждого подразделения или отдела с целью выявления используемых активов. Активы системы информационных технологий являются компонентом или частью общей системы, в которую предприятие напрямую

вкладывает средства и которые, соответственно, требует защиты со стороны предприятия. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства, но и программное обеспечение. Могут существовать следующие типы активов:

— информация/данные (например, файлы, содержащие информацию о платежах или продукте);

— аппаратные средства (например, компьютеры, принтеры);

— программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения);

— оборудование для обеспечения связи (например, телефоны, медные и оптоволоконные кабели);

— программно-аппаратные средства (например, электронные носители информации);

— документы (например, контракты);

— продукция предприятия;

— услуги (например, информационные, вычислительные услуги);

— конфиденциальность и доверие при оказании услуг (например, услуг по совершению платежей);

— оборудование, обеспечивающее необходимые условия работы;

— персонал организации;

— престиж (имидж) организации.

Этап 2. Определение риска несоответствия требований законодательства в области ИБ. Любая организация, имеющая информационные системы или работа которой связана с использованием информационных технологий для ведения бизнеса, должна соблюдать федеральные законы в этой отрасли. Невыполнение данных требований может повлечь за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Риск невыполнения требований

законодательства влияет на общий риск ИБ МСБ. Алгоритм определения риска несоответствия требований законодательства в области ИБ включает в себя проведение всестороннего анализа состояния системы защиты с целью выявления выполнения требований в соответствии с требованиями законодательства. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются и определяется процент выполненных требований. В заключение анализа необходимо определить уровень риска несоответствия требований по ИБ, который определяется по таблице 1.

Этап 3. Разработка модели угроз. С целью максимально точного определения риска ИБ, разрабатывается частная модель угроз ИБ предприятию с учетом вида его деятельности. Вероятности наступления неблагоприятных событий определяются экспертом или группой экспертов, занимающихся разработкой модели угроз. Экспертным методом определяется и актуальность угроз ИБ.

Таблица 8

Определение риска несоответствия требованиям законодательства

Процент выполненных требований (Пз)	**Риск несоответствия требованиям законодательства Rn**
85-100	0,01
40-84	0,25
Менее 40	0,5
Не выполняются	0,9

После завершения оценки угроз составляют перечень актуальных идентифицированных угроз на каждый идентифицированный актив или группы активов, подверженных этим угрозам, а также определяют вероятность реализации угроз.

Этап 4. Процедура количественной оценки рисков ИБ. Основным этапом в процессе оценки рисков является процедура количественного определения рисков ИБ. Пошаговый алгоритм количественного определения риска ИБ представлен в таблице 9.

Таблица 9

Алгоритм количественного оценивания риска ИБ

Шаг 1	Выбор актуальных угроз ИБ частной модели угроз
Шаг 2	Определение вероятности реализации угроз
Шаг 1	Определение ценности актива
Шаг 4	Определение возможности использования организационных технических уязвимостей
Шаг 5	Вычисление численного значения риска

Процедура количественной оценки рисков ИБ включает в себя следующие шаги:

Шаг 1. Выбор актуальных угроз частной модели угроз. На данном шаге, используя частную модель угроз, формируется перечень актуальных угроз ИБ активов предприятия. На данном шаге количественного оценивания рисков сопоставляются идентифицированные активы с направленными на них угрозами. Для этого используется перечень активов предприятия и каждому из них сопоставляются актуальные угрозы из модели угроз.

Шаг 2. Определение вероятности наступления угрозы. В связи с тем, что на один актив могут воздействовать одновременно несколько угроз, необходимо определить вероятность того, что хотя бы одна угроза реализуется по отношению к выбранному активу.

Определение вероятности наступления неблагоприятных событий в связи с реализацией хотя бы одной угрозы из перечня актуальных угроз на рассматриваемый актив. Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз y_1, y_2, ..., y_n, где n – количество угроз, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

Шаг 3. Определение ценности актива. Ценность актива определяется стоимостью информационного актива. В связи с тем, что зачастую невозможно определить точные стоимости активов и предприятия в целом, рекомендуется ценность актива задавать в диапазоне от 0 до 1, которая будет показывать отношение цены актива к стоимости всего бизнеса ($С_б$).

Так как универсальной методики оценки активов нет, то в данной методике оценка актива определяется владельцем предприятия совместно с экспертом по оценке рисков.

Шаг 4. Определение возможности использования организационных и технических уязвимостей. Возможность использования организационных уязвимостей проводится экспертным методом, анализируя применяемые организационные меры защиты информации. В ходе проведения анализа, всем организационным мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В таблице 10 представлены соответствие процента выполняемых организационных мер защиты информации и коэффициента уязвимости организационных мер защиты информации. Возможность использования технических уязвимостей проводится экспертным методом, анализируя применяемые технические меры защиты информации. В ходе проведения анализа всем техническим мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются и вычисляется процент от количества технических мер. В таблице 11 представлено соответствие выполняемых технических мер защиты информации и коэффициент уязвимости технических мер защиты информации.

Таблица 10

Определение коэффициента уязвимости организационных мер защиты информации

Процент выполняемых мер защиты ($П_о$)	Коэффициент уязвимости ($К_о$)
75–100	0,01
20–74	0,25
Менее 20	0,5
Не выполняются	0,9

Шаг 5. Вычисление численного значения риска. В разрабатываемой методике процедура оценки рисков реализации хотя бы одной угрозы основывается на взаимности нескольких факторов – вероятности происшествия, а именно вероятности реализации хотя бы одной актуальной угрозы, коэффициента ценно-

сти актива, среднеарифметического значения коэффициентов возможности использования организационных уязвимостей и возможности использования технических уязвимостей и риска несоответствия требованиям законодательства.

Таблица 11

Определение коэффициента уязвимости технических мер защиты информации

Процент выполняемых мер защиты($П_t$)	Коэффициент уязвимости ($К_t$)
70–100	0,01
20–69	0,25
Менее 20	0,5
Не выполняются	0,9

Под коэффициентом ценности актива понимают ценность или критичность актива по отношению ко всему бизнесу. Процедура количественной оценки рисков реализации хотя бы одной угрозы из всего перечня актуальных угроз по отношению к конкурентному активу определяется относительно каждого типа актива, на который воздействует совокупность угроз ИБ, что позволяет дискретно определить риск наступления неблагоприятных событий на каждый тип актива. Общая формула (4) определения риска реализации хотя бы одной угрозы из всего перечня актуальных угроз с учетом наличия уязвимостей по отношению к конкурентному i-му активу:

$$R_i = P_{угрi} R_{ni} C_{бi} \{(K_{0i} + K_{ti})1/2\} 100\%, \quad (4)$$

где R_i – численная величина риска реализации угроз ИБ;

$P_{угрi}$ – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз;

R_{ni} – риск несоответствия требованиям законодательства;

$C_{бi}$ – ценность актива;

K_{oi} – вероятность использования организационных уязвимостей;

K_{ti} – вероятность использования технических уязвимостей, i=1,…m, m-количество активов.

Этап 5. Определение допустимого уровня обобщенного риска $R_{общ}$.

$$R_{общ} = \sum_i^m Ri. \quad (5)$$

Допустимым обобщенным риском $R_{добщ}$ принято считать риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. Для предприятия МСБ рекомендованное значение обобщенного риска не должно превышать 5% выручки.

$$R_{добщ} <= 0{,}05\ В, \qquad (6)$$

где В – выручка МСБ.

Это обусловливается в первую очередь тем, что максимальная выручка предприятий МСБ за отчетный период, например, 1 год, может составлять до 40 млн. рублей, это из расчета того, что в случае реализации одной из актуальных угроз, может повлечь убыток в размере более 5% выручки, является недопустимым и требующим принятия эффективных мер.

Выполнение всех этапов проведения оценки рисков ИБ на предприятиях МСБ повторяется для каждого типа актива. Полученное значение рисков ИБ необходимо для выработки рекомендаций по снижению уровня риска, а также принятия эффективных мер по обеспечению ИБ предприятия. В случае если итоговое значение риска менее 5%, то делается вывод о том, что на предприятии выполнены требования по ИБ в полной необходимости, а также что риск ИБ оцениваемого типа актива допустимый. Но необходимо периодически проводить переоценку рисков ИБ. В случае если итоговое значение риска более или равно 5%, то делается вывод о том, что на предприятии не выполняются требования по ИБ, а также что риск ИБ оцениваемого типа актива повышенный и требует немедленного принятия решений.

Задание для выполнения

1. Рассчитать риски для всех активов и обобщенный риск информационной безопасности МСБ для организационных технических мер защиты, реализованных в МСБ. Для расчета рекомендуется использовать Microsoft Excel. Исходные данные для каждого варианта находятся на севере в папке группы, номер варианта получить у преподавателя, пример приведен в таблице 12.

Таблица 12

Пример исходных данных

№ варианта	№ актива	$Р_{угр}$	$С_б$ (тыс.руб)	$П_з$ (%)	$П_т$ (%)	$П_о$ (%)
1	1	0,001	1	89	26	2
	2	0,002	2	69	54	43
	3	0,003	3	20	40	70
	4	0,004	4	5	80	37

Риск несоответствия требованиям, коэффициенты уязвимостей для организационных и технических мер защиты взять из таблиц 1, 2 и 3 соответственно.

2. Подготовить электронный отчет с анализом полученных результатов.

3. Электронный отчет сохранить в своей папке на сервере.

4. Представить электронный отчет преподавателю и защитить результаты исследований.

Практическое занятие 2. Оценка риска экономической безопасности предприятия

Цель практического занятия изучить один из способов оценки рисков и приобрести практические навыки по проведению оценка риска экономической безопасности предприятия.

Для оценки потерь, потенциальная возможность которых порождается внутренними и внешними риска, может быть использована следующая методика.

Вероятные потери ($В_П$) предприятия определяются по следующей зависимости:

$$В_П = Ц*Р_В + Р_Ц*О, \quad (7)$$

где $Р_В$ – разница выпуска (вероятное суммарное уменьшение объема выпуска продукции); $Р_Ц$ – разница цены (вероятное уменьшение цены единицы выпуска продукции); О – общий объем намеченной к выпуску продукции; Ц – цена реализации единицы объема продукции.

Первое слагаемое определяет вероятные потери от снижения намеченных объемов производства и реализации продукции вследствие проявления рисков, вызывающих уменьшения производительности труда, простоя оборудования, потерь рабочего времени, отсутствия материалов, брака и т.д.

Второе слагаемое определяет вероятные потери от рисков снижения цен, по которым намечается реализация продукции, в связи с недостаточным качеством, неблагоприятным изменением рыночной конъюнктуры, падением спроса, инфляцией и т.д.

Потери от превышения материальных затрат ($П_{МЗ}$), обусловленных перерасходом материалов, сырья, топлива, энергии, вычисляются по следующей формуле:

$$П_{МЗ} = \sum_{i}^{N} (Цi * Mi) \quad , \qquad (8)$$

где *Цi* – цена единицы i-го ресурса;

Mi – вероятный перерасход i-го материального ресурса *(i=1, N),*

N – количество ресурсов.

Потери, обусловленные повышением транспортных тарифов, торговых издержек, акцизов, заработной платы, ставок налогов и платежей, естественной убылью, определяются методом прямого счета, путем сопоставления фактических затрат с планируемыми.

Для уяснения сущности показателей риска выделяются определенные зоны риска в зависимости от величины потерь, приведенные на рисунок 14. Область, в которой потери не ожидаются, называют безрисковой зоной. Ей соответствуют нулевые потери или отрицательные (превышение прибыли).

Под зоной допустимого риска понимается область, в пределах которой данный вид деятельности сохраняет свою экономическую целесообразность. Граница ее соответствует уровню потерь, равному расчетной прибыли от предпринимательской деятельности.

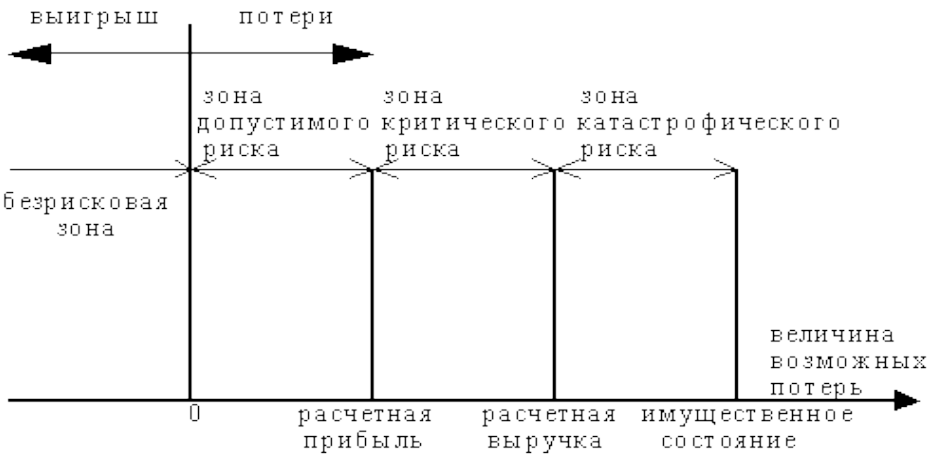


Рис. 14. Зоны риска в зависимости от величины потерь

Следующая зона является более опасной и называется зоной критического риска. Это область, характеризуемая возможностью потерь, превышающих величину ожидаемой прибыли, вплоть до величины полной расчетной выручки от предпринимательства, представляющей сумму затрат и прибыли. Иначе говоря, зона критического риска характеризуется опасностью потерь, которые заведомо превышают ожидаемую прибыль и в максимуме могут привести к невозмещаемой потере всех средств, вложенных предприятием (фирмой) в дело. В последнем случае оно не только не получает от сделки никакого дохода, но и несет убытки в сумме всех бесплодных затрат.

И наконец, зона катастрофического риска представляет область потерь, которые по своей величине превосходят критический уровень и в максимуме могут достигать величины, равной имущественному состоянию предприятия (фирмы). Катастрофический риск способен привести к краху, банкротству предприятия, его закрытию и распродаже имущества. К категории катастрофического следует относить вне зависимости от имущественного или денежного ущерба риск, связанный с прямой опасностью для жизни людей или с возникновением экологических катастроф.

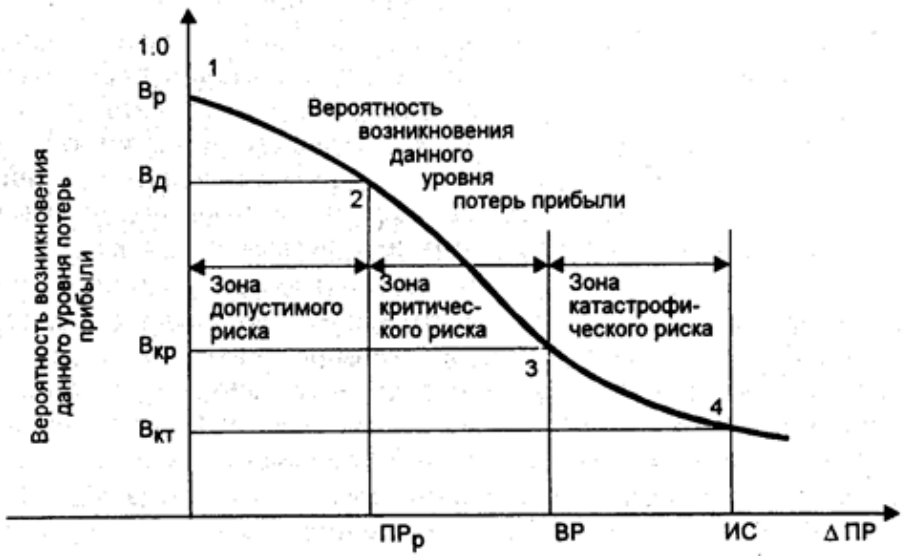


Рис. 15. Зависимости вероятностей возможных потерь прибыли от уровня потерь

Наиболее полное представление о риске дает графическое изображение зависимости вероятностей возможных потерь прибыли от уровня потерь (рисунок 15). При благоприятных условиях, т.е. в случае, когда потери равны нулю, прибыль может быть максимальной и она может быть больше расчетной. При наличии потерь и их увеличении прибыль, естественно, уменьшается, что изображается соответствующей кривой, на которой можно выделить ряд характерных точек.

В первой точке вероятность ($В_р$) потерь прибыли (П) будет равна нулю, хотя может быть и меньше единицы. Вторая точка характеризуется величиной возможных потерь, равной ожидаемой прибыли ($ПР_р$), вероятность которой равна $В_д$. Точки 1 и 2 являются граничными, определяющими положение зоны допустимого риска.

Третья точка соответствует величине потерь, равных расчетной выручке ($В_Р$). Вероятность таких потерь равна $В_{кр}$. Точки 2 и 3 определяют границы зоны критического риска.

Четвертая точка характеризуется потерями, равными имущественному состоянию (ИС) предприятия, вероятность которых равна Вкт. Между точками 3 и 4 находится зона катастрофического риска.

Потери, превышающие имущественное состояние предприятия (фирмы), не рассматриваются, так как их невозможно взыскать.

Вероятности определенных уровней потерь являются важными показателями, позволяющими высказать суждение об ожидаемом риске и его приемлемости, поэтому построенную кривую называют кривой риска.

В процессе принятия решений допустимости и целесообразности риска важно представлять не столько вероятность определенного уровня потерь, сколько вероятность того, что потери не превысят некоторого уровня. По логике именно это и есть основной показатель риска.

Вероятность того, что потери не превысят определенного уровня, и есть показатель надежности, уверенности. Очевидно, что показатели риска и надежности тесно связаны между собой в рамках экономической безопасности предприятия (фирмы).

Знание показателей риска – Вр, Вд, Вкр, Вкт – позволяет выработать суждение и принять решение об осуществлении производства. Но для такого решения недостаточно оценить значения показателей (вероятностей) допустимого, критического и катастрофического риска. Надо еще установить или принять предельные величины этих показателей, выше которых они не должны подниматься, чтобы не попасть в зону чрезмерного, неприемлемого риска.

Обозначив предельные значения вероятностей возникновения допустимого, критического и катастрофического риска соответственно Кд, $К_{кр}$, $К_{КТ}$, руководитель вправе определить свои собственные предельные уровни риска, которые он не намерен превышать. Хотя в принципе эти величины должна устанавливать и рекомендовать прикладная теория экономической безопасности.

Это означает, что не следует идти на сделку, если в 10 случаях из 100 можно потерять всю прибыль, в одном случае из 100 потерять выручку и хотя бы в одном случае из 1000 потерять имущество.

Задание для выполнения

1. Предприятие выпускает смартфоны, его деятельность характеризуется следующими параметрами:

● объем выпуска – 10000 в месяц;

● цена одного смартфона – 25000 руб.;

● материальные затраты на закупку сырья – $М_1$ = 300 руб., топлива – $М_2$ = 350 руб., электроэнергии – $М_3$ = 350 руб. на ед. товара;

● расходы на транспорт – $Т_р$= 1000 руб., торговые издержки – $Т_и$ = 1000 руб., акцизы – $Т_а$ = 500 руб., заработную плату – $Т_з$ = 10000 руб., налоги и ● платежи – $Т_н$ = 1500 руб., естественную убыль – $Т_у$ = 1000 руб. на ед. товара;

● количество работников – 20 чел.;

● расчетная прибыль в месяц – П = 10000000 руб.;

● расчетная выручка в месяц – В = 100000000 руб.;

● имущественное состояние – $И_с$ = 1000 000 000 000 руб.

Предприятие в процессе своей деятельности подвергается множеству внешних и внутренних угроз, которые приводят к рискам изменения стоимости компонентов материальных затрат и иных расходов на определенный процент: $Р_{м1}$, $Р_{м2,}$ $Р_{м3}$, $РТ_и$, $РТ_а$, $РТ_з$, $РТ_н$, $РТ_у$.

2. Используя методику провести оценку возможных потерь от рисков и построить зоны рисков. Считается, что предельные значения показателей риска Кд = 0,1; $К_{кр}$ = 0,01; $К_{кт}$ = 0,001, т.е. соответственно 10, 1 и 0,1 %, могут быть допустимы в предпринимательском риске. Исходные данные для каждого варианта находятся на севере в папке группы, номер варианта получить у преподавателя, пример приведен в таблице

Таблица 13

№ варианта	$Р_в$ (%)	$Р_ц$ (%)	М (%)	Ц (Руб)	$Р_{м1}$ (%)	$Р_{м2}$ (%)	$Р_{м3}$ (%)	$РТ_{р1}$ (%)	$РТ_и$ (%)	$РТ_а$ (%)	$РТ_з$ (%)	$РТ_н$ (%)	$РТ_у$ (%)
1	20	30	10										
			20										
			30										

3. Подготовить электронный отчет с анализом полученных результатов.

4. Электронный отчет сохранить в своей папке на сервере.

5. Представить электронный отчет преподавателю и защитить результаты исследований.

Практическое занятие 3. Комплексная оценка уровня экономической безопасности предприятия

Цель занятия показать умения и приобрести навыки в проведении комплексной оценки уровня экономической безопасности предприятия. При выполнении задания использовать теоретические знания, полученные в одноименной лекции и при самостоятельной подготовке.

Для оценки уровня экономической безопасности необходимо.

1. Определить соответствие необходимого объема имеющихся ресурсов задаче безопасного функционирования предприятия.

Порядок определения соответствия необходимого объема имеющихся ресурсов выступает одним из элементов комплексной методики оценки экономической безопасности. Для оценки соответствия рекомендован расчет величины $\overline{d_{mi}}$ – усредненная величина, характеризующая достаточность имеющихся ресурсов по составляющим предприятия;

d_{mi} – величина, характеризующая достаточность имеющихся ресурсов по составляющим предприятия;

$$d_{mi} = \frac{x_{ij}}{m_{ij}} \ , \qquad (9)$$

где x_{ij} – текущее значение, j -го показателя в i-ой детерминанте (финансовая, интеллектуально-кадровая, технико-технологическая, информационная, сырьевая, управленческая или сбытовая); m_{ij} – пороговое значение j -го показателя в i-ой детерминанте.

Величина $\overline{d_{mi}}$ рассчитывается по каждой составляющей ресурсов (детерминант микроуровня в системе экономической безопасности) как средняя геометрическая стандартизированных значений показателя для каждой характеристики. Система данных показателей приведена в таблице 14.

Объем ресурсов следует считать соответствующим задаче безопасного функционирования, если усредненная величина, характеризующая достаточность имеющихся ресурсов по составляющим предприятия ($\overline{d_{mi}}$) по каждой составляющей превышает единицу.

Это свидетельствует о том, что при неизменности воздействия факторов макро- и мезо- уровней у предприятия имеются необходимые ресурсы для безопасного функционирования. Если же по какой-либо составляющей значение не превышает единицы – это свидетельствует о нехватке определенного типа ресурсов и обусловливает необходимость соответствующей корректировки реализуемой стратегии развития.

2. Выявить характер и силу воздействия детерминант мезо- и макроуровней хозяйствования на функционирование предприятия.

Таблица14

Система данных показателей

№ п\п	Составляющая детерминант	Показатели, характеризующие составляющие	Порядок расчета показателей	m[5]	
1	финансовая	коэффициент текущей ликвидности	$К_{ТЛ}$ = $О_{б}А$ / КДО	2	ОбА – оборотные активы КДО – краткосрочные обязательства
		коэффициент финансовой независимости	$К_{ФН}$ = ВБ / СК	0,5	ВБ – валюта баланса СК – собственный капитал
		коэффициент обеспеченности СОС	$К_{ОБ.СОС}$ = СОС \ ОбС	0,1	СОС – собственные оборотные средства ОбС – Оборотные средства
		вероятность получения займа или инвестиций при подаче заявки	экспертная оценка Впз	100%	
2	интеллектуально-кадровая	профессионально-квалификационный уровень кадров	экспертная оценка доли соответствующих требованиям предприятия	100%	$П_{ку}$
		доля персонала, не имеющая нарушений трудовой дисциплин	$К_{ПН}$ = $ЧП_{НН}$/ЧП	0,9	
		коэффициент постоянства кадров	$К_{ПК}$ = $К_{ПОСТ}$ \ $К_{СП}$	0,8	

[5] Пороговое значение (m) может варьироваться в зависимости от специфики сферы деятельности и особенностей предпринимательской структуры.

Окончание табл. 14

№ п\п	Составляющая детерминант	Показатели, характеризующие составляющие	Порядок расчета показателей	m^5	
3	технико-технологическая	доля технологического процесса, охваченного инновациями	$К_{ИО} = ТП_{И}/ТП$	0,8	
		технический и технологический уровень производства	экспертная оценка в баллах (от 1 до 3)	3	$Т_{уп}$
4	информационная	вероятность сохранения коммерческой тайны	экспертная оценка	100%	$В_{кт}$
		уровень надежности компьютерной техники	экспертная оценка в баллах (от 1 до 3)	3	$Н_{кт}$
5	сырьевая	коэффициент годности основных средств	$К_{ГОС} = О_{СТ}$ Ст / $П_{ОЛН}$Ст	0,7	ОстСт – остаточная стоимость основных фондов ПолнСт – Первоначальная стоимость осн средств
		коэффициент ресурсного обеспечения	$К_{РО} = РО_{ФАКТ} / РО_{НОРМ}$	1	
		коэффициент автоматизации труда	$К_{АТ} = К_{ОЛ-ВОАВ} \setminus К_{ОЛ-ВОАВ}+К_{ОЛ-ВО РУЧ}$	0,7	
6	управленческая	профессиональный уровень руководителей	экспертная оценка в баллах (от 1 до 3)	3	$П_{ур}$
		репутация предприятия	экспертная оценка в баллах (от 1 до 3)	3	Рп
		разрыв в оплате труда аппарата управления и основной категории работников	$Кр = ВОТ_{Р} / ВОТ_{У}$	0,5	
7	сбытовая	уровень развития сбытовой деятельности	доля реализованной продукции от планируемого объема	0,9	Урсб
		качество продукции	доля продукции, соответствующей мировым стандартам, в общем объеме	0,7	Кп

Определение характера и силы воздействия детерминант мезо- и макроуровней хозяйствования производится только на основе экспертных оценок. Важными составляющими в системе оценки уровня экономической безопасно-

сти являются детерминанты макро- и мезо- уровней. При комплексной оценке их учет производится в виде применения уточняющих коэффициентов $\overline{k_{ma}}, \overline{k_{me}}$.

$\overline{k_{ma}}$ –коэффициент влияния детерминант макроуровня в системе экономической безопасности предприятия, полученный как усредненное значение параметров, полученных в результате экспертной оценки;

$\overline{k_{me}}$ – коэффициент влияния детерминант мезоуровня в системе экономической безопасности предприятия, полученный как усредненное значение параметров, полученных в результате экспертной оценки.

3. Провести оценку детерминант макроуровня. В данном случае для целей оценки детерминант системы экономической безопасности макроуровня целесообразно адаптировать применяемый в стратегическом управлении ПЭСТ-анализ (таблица 15).

Таблица 15

Параметры экспертной оценки детерминант мезоуровня в системе экономической безопасности предприятия[6]

Ключевые детерминанты	**Характеристика ключевых детерминант**	**Параметр экспертной оценки**
характеристики сферы деятельности	характеристика контрагентов; особенности развития сферы деятельности	– надежность партнеров; – надежность инвесторов; – объем и перспективность развития рынка; – характер конкуренции на рынке; – сезонные колебания; – инновационное развитие конкурентов; – привлекательность бизнеса
характеристики территории	ресурсное обеспечение территории; инфраструктурное обеспечение территории; привлекательность региона	– уровень безработицы в регионе; – уровень жизни населения в регионе; – инвестиционная привлекательность территории; – границы рынка сбыта; – наличие местных ресурсов; – транспортно-логистическая инфраструктура

[6] Совокупность параметров для экспертной оценки воздействия детерминант мезоуровня на безопасное функционирование предприятия может быть изменено в зависимости от специфики предпринимательской деятельности и сферы деятельности.

4. Оценка детерминант мезо-уровня системы экономической безопасности. В данном случае следует учитывать, что мезо-уровень хозяйствования можно понимать, как в отраслевом, так и в территориальном аспекте. В данном расчете параметрами экспертной оценки характера воздействия детерминант мезоуровня будут выступать следующие (таблица 16):

Таблица 16

Значения оценок факторов в составе детерминант мезо- и макроуровней в соответствии с экспертной оценкой их силы и характера воздействия

№ п/п	Сила воздействия	Характер воздействия	Оценка, используемая при расчетах
1	полная независимость	угроза для бизнеса	1
		благоприятные условия для бизнеса	1
2	слабое воздействие	угроза для бизнеса	0,9
		благоприятные условия для бизнеса	1,1
3	чувствительное воздействие	угроза для бизнеса	0,8
		благоприятные условия для бизнеса	1,2
4	сильное воздействие,	угроза для бизнеса	0,7
		благоприятные условия для бизнеса	1,3
5	очень сильное воздействие	угроза для бизнеса	0,6
		благоприятные условия для бизнеса	1,4

Задание для выполнения

1. Для комплексной оценки экономической безопасности предприятия вычислить: $\overline{d_{mi}}$, $\overline{k_{ma}}$, $\overline{k_{me}}$. Для расчета рекомендуется использовать Microsoft Excel. Файл с таблицей исходных данных для каждого варианта находится на севере в папке группы, номер варианта получить у преподавателя, пример приведен в таблице 17.

2. Рассчитать интегральный показатель уровня экономической безопасности $Э$, представлен в мультипликативном виде:

$$Э = \overline{d_m} * \overline{k_{ma}} * \overline{k_{me}} \qquad (10)$$

Таблица 17

Варианты с исходными данными для задания

№ вар	Финансовая				Интеллектуально-кадровая			Технико-технологическая		Информационная		Сырьевая			Управленческая			Сбытовая	
	$К_{тл}$	$К_{фн}$	$К_{об-сос}$	$В_{пз}$	$П_{ку}$	$К_{пн}$	$К_{пк}$	$К_{ио}$	$Т_{уп}$	$В_{кт}$	$Н_{кт}$	$О_{стС}$	$К_{ро}$	$К_{ат}$	$П_{ур}$	$Р_{п}$	$К_{р}$	$У_{рсб}$	$К_{п}$
1	1	0.3	0.2	1	1	0.9	0.7	0.6	2	1	3	0.6	1	0.6	3	2	0.5	0.8	0.7

3. Пороговым значением для оценки данного показателя выступает единица. Если Э больше или равно единице, то уровень экономической безопасности не просто высокий, а у предприятия достаточно собственных ресурсов для успешного нивелирования угроз экономической безопасности, возникающих во внешней среде. Если значение Э меньше единицы, то необходим детальный анализ детерминант в системе экономической безопасности.

4. Подготовить электронный отчет с анализом полученных результатов.

5. Электронный отчет сохранить в своей папке на сервере.

6. Представить электронный отчет преподавателю и защитить результаты исследований.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 4. Работа с Web-сервисом Контур.Фокус

Цель практического занятия – приобрести практические навыки работы с Web-сервис Контур.Фокус при подготовке электронной справке по возможностям Контур.Фокуса.

1. В электронной справке по Web-сервис Контур.Фокус дать ответы на следующие вопросы:

— что такое реестры особых адресов ФНС? Привести примеры компаний, которые по данным Контур.Фокуса, находятся в этих реестрах;

— информация из каких лицензирующих органов есть в Контур.Фокусе? Привести примеры компаний, у которых по данным Фокуса есть лицензии из 6-ти разных источников;

— что означает знак лупы напротив адреса компаний?

— когда можно увидеть в сервисе данные по предшественникам и преемникам организации?

— из какого неофициального источника в сервисе Контур.Фокусе есть информация?

— правильно расставить пары «компания-выручка», «компания- госконтракты», «компания-арбитражи»: Сбербанк, Аэрофлот, Газпром, X5, Проктер, VW, «Метро кэш энд керри», Волгоградпрограммсистем, Лукойл-нижневолжскнефтепродукт, Craft foods.

2. Для компаний с ИНН, указанными ниже с помощью Контур.Фокуса провести анализ их деятельности и показать схему связи с другими организациями:

1) 3448044327 2) 6164317329 3) 6166082658 4) 263211416007 5) 343511748130 6) 3443062516 7) 3435040396 8) 3442046977 9) 3435115806 10) 3413010503 11) 3457001256 12) 3437013060 13) 3436004418 14) 3413010888

3. В электронной справке отразить результаты исследования по 1п. и 2п.

4. Справку сохранить в своей папке на сервере.

5. Представить электронную справку преподавателю и защитить результаты исследований.

Практическое занятие 5. СПАРК-Интерфакс

Цель занятия: приобрести навыки практической работы в системе СПАРК-Интерфакс.

1. Используя СПАРК-Интерфакс определить 10 крупнейших предприятий по размерам выручки от реализации за 2016 г. по основным отраслям промышленности и основным непромышленным секторам экономики Волгоградской области (файл со списком компаний получить у преподавателя):

a. добыча полезных ископаемых;

b. обрабатывающие производства, в том числе:

— производство пищевых продуктов, включая напитки, и табак;

— текстильное и швейное производство;

— производство кожи, изделий из кожи и производство обуви;

— обработка древесины и производство изделий из дерева;

— целлюлозно-бумажное производство; издательская и полиграфическая деятельность;

— производство кокса, нефтепродуктов;

— химическое производство;

— производство резиновых и пластмассовых изделий;

— производство прочих неметаллических минеральных продуктов;

— металлургическое производство и производство готовых металлических изделий;

— производство машин и оборудования;

— производство электрооборудования, электронного и оптического оборудования;

— производство транспортных средств и оборудования;

— прочие производства;

с. производство и распределение электроэнергии, газа и воды.

(Отнесение предприятия к отрасли провести на основе Общего классификатора видов экономической деятельности (ОКВЭД), введенного с 1 января 2003 г.)

2. На основе показателей компаний провести ранжирование 10 крупнейших компаний отрасли (или основных непромышленных секторов экономики) по выручке от реализации, чистой прибыли, норме чистой прибыли, рентабельности активов и собственного капитала.

3. Подготовить электронный отчет с результатами исследований, сохранить его в своей папке на сервере.

Практическое занятие 6. Комплексное изучение ситуации на предприятии с помощью СПАРК-Интерфакс.

Цель занятия: пробрести практические навыки по комплексному изучению ситуации на предприятии и вокруг него.

1. Разработать и представить обобщенный отчет с результатами исследований по комплексному изучению ситуации на предприятии и вокруг него.(ИНН предприятия получить у преподавателя). Исследования проводить последующим вопросам:

— регистрационные данные, юридический и фактический адрес, форма собственности, дочерние фирмы. Реестродержатель;

— учредители (акционеры), владельцы контрольного и блокирующего пакетов акций. Кто де-юре и де-факто владеет предприятием – какие юридические и физические лица конкретно. Характеризующие данные на них;

— история создания и развития, приватизация;

— направления деятельности и специализация, номенклатура выпускаемой продукции. Объемы и характеристика выпускаемой продукции. Положение и роль в отрасли, регионе и т.д.;

— состояние основных фондов (износ и работоспособность оборудования и т.д.);

— деловая репутация: участие в судебных разбирательствах, претензии со стороны спецслужб, правоохранительных и таможенных органов, органов исполнительной власти, связи с криминалом. Данные по участникам арбитражных процессов (судьи и их позиции, представители противоборствующих сторон и т.д.).;

— руководство: лица, реально принимающие решения (степень влияния на политику предприятия);

— лица, связанные с организованными преступными сообществами или трудоустроенные на предприятие по их рекомендациям. Личные и деловые характеристики (психологический портрет). Деловые связи и опыт;

— участие в качестве учредителей или акционеров в других коммерческих проектах (параллельные финансовые интересы).

— отношения внутри предприятия:

— отношения и их обострения в команде управления, наличие группировок и семейных кланов;

— взаимоотношения между командой управления и трудовым коллективом, наличие в коллективе неформальных лидеров, степень их влияния на коллектив;

— другие факты, свидетельствующие о внутренней напряженности на предприятии;

— система безопасности;

— наличие «крышевого» прикрытия;

— позиции в местных и центральных органах власти и правоохранительных органах (МВД, ФСБ, ФСНП, прокуратура, ГНИ, ФСФО и т.д.). Кто из представителей этих структур реально поддерживает (лоббирует) интересы предприятия;

— собственная служба безопасности (функции, кадровый состав, его квалификация и принадлежность к правоохранительным органам и спецслужбам);

— методы решения конфликтных ситуаций;

— Сведения о финансовом положении:

- финансовое положение (последний баланс), источники финансирования;
- себестоимость продукции (номинальная и реальная);
- прибыль (номинальная и реальная);
- взаимоотношения с банками, кредитная история;
- средний оборот по счету (счетам);
- распределение прибыли;

- отношения с налоговыми органами (инспекция, полиция);
- задолженность в бюджет (местный, федеральный);
- наличие задолженности своим контрагентам;
- факты неудачных инвестиционных проектов в других сферах деятельности;
- проблемы (невыплата зарплаты, отсутствие заказов и т.д.).

— Тенденции дальнейшего развития (планы на ближайшую перспективу).

— Партнеры:

- взаимоотношения;
- условия сотрудничества;
- задолженность компании своим партнерам и наоборот.

— Конкуренты. Конкуренты и противники хозяев (юридические и физические лица), формы противоборства. Характеризующие данные на лидеров противоборствующей стороны.

2. Подготовить электронный отчет с анализом полученных результатов.

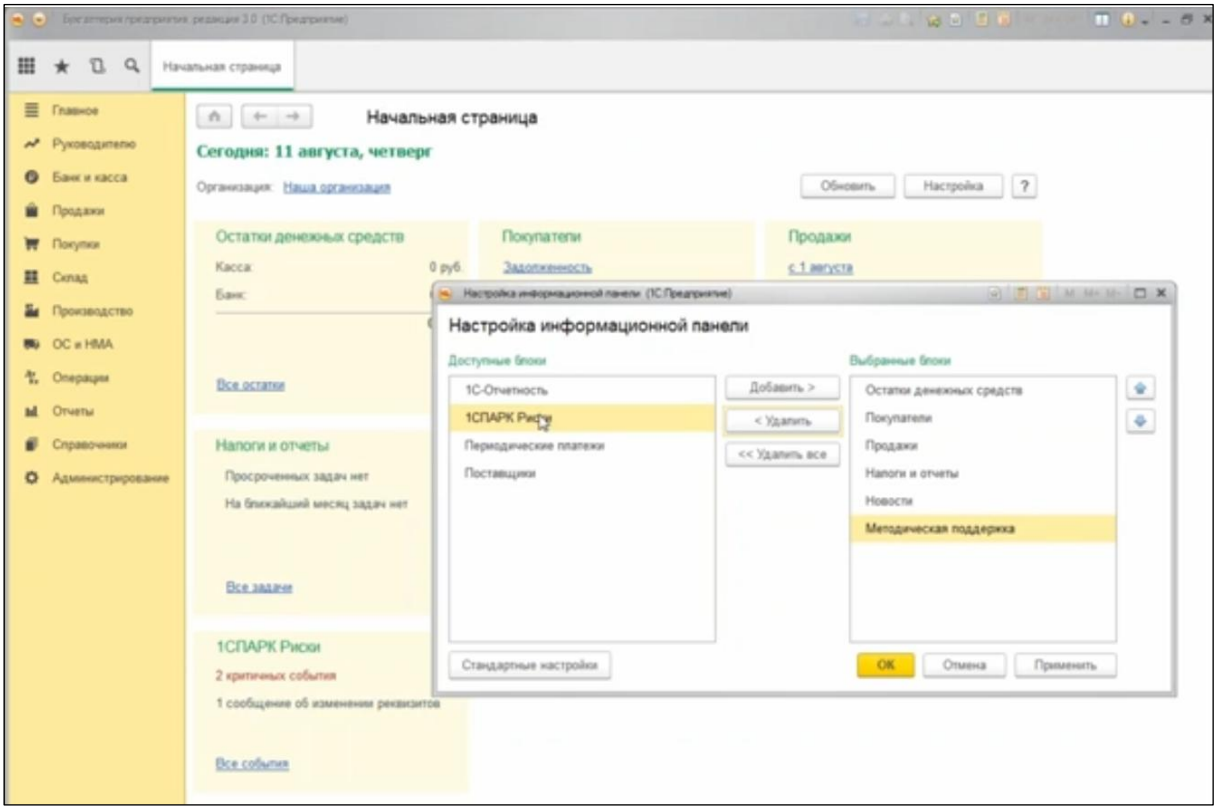
3. Электронный отчет сохранить в своей папке на сервере.

4. Представить электронную отчет преподавателю и защитить результаты исследований.

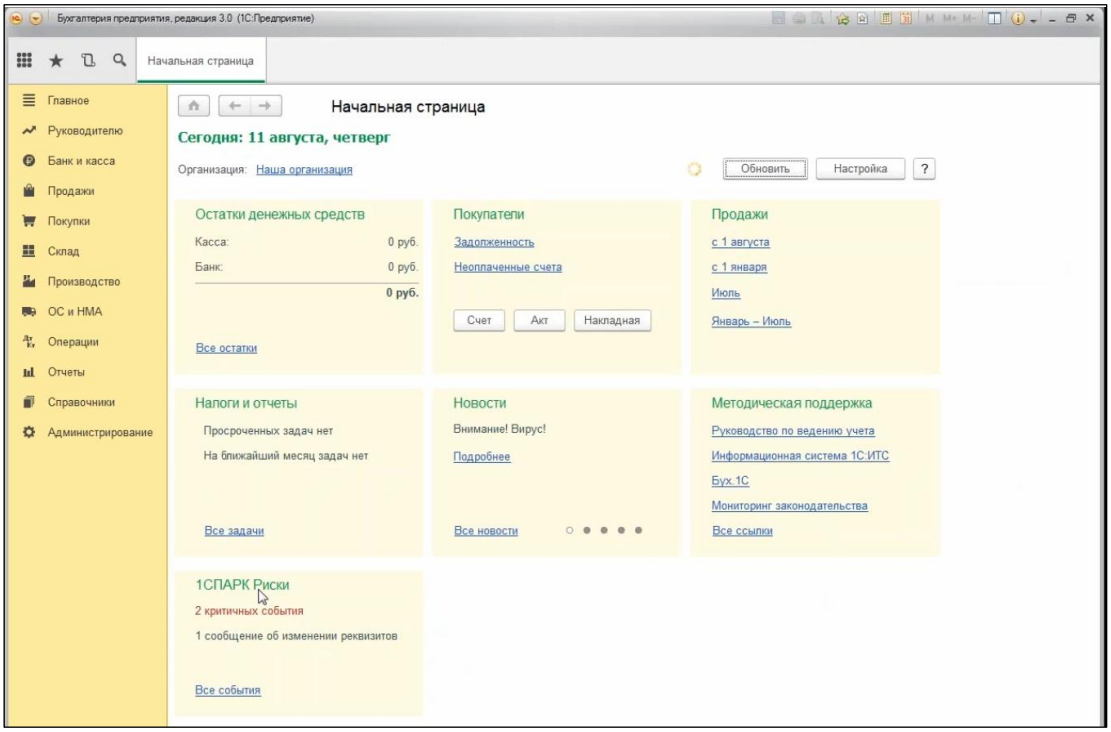
Практическое занятие 7. Комплексная оценка контрагента с помощью сервиса «1СПАРК-Риск».

Цель занятия: приобрести навыки практической работы в сервисе «1СПАРК–Риски».

1. Для вывода сервиса «1СПАРК-Риск» на начальную страницу «1С: Предприятие» зайдите в настройки и добавьте сервис из окна Доступные блоки в окно Выбранные блоки.

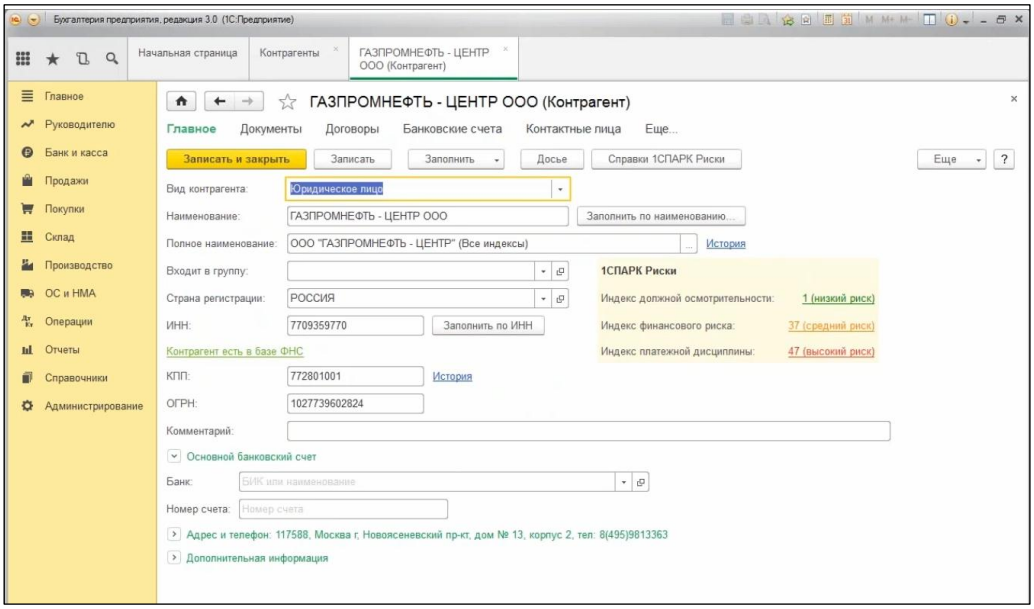


В результате на начальной странице появляется ссылка на сервис.

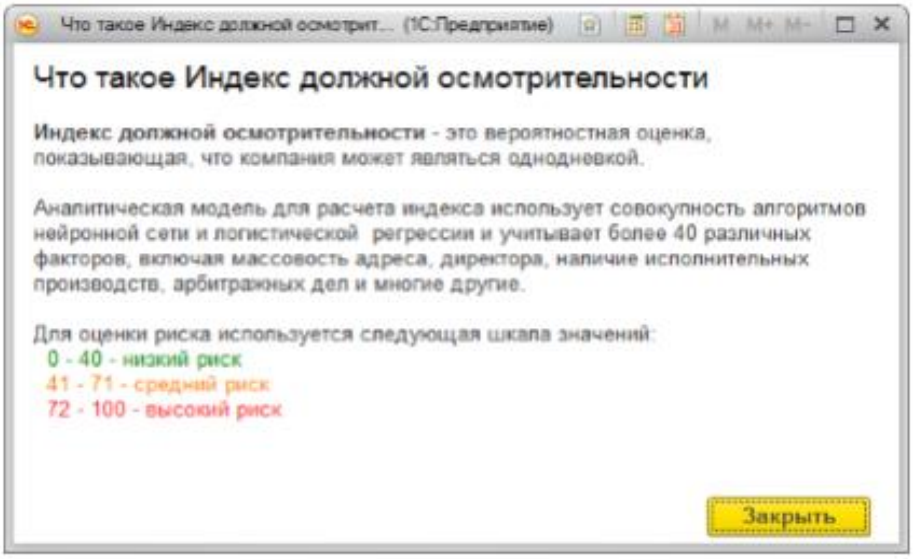


2. В «1СПАРК-Риски» для оценки надежности контрагента представлены три индекса: • Индекс должной осмотрительности – оценка, показывающая вероятность того, что компания является «фирмой-однодневкой»; • Индекс финансового риска – оценка вероятности неплатежеспособности компании; • Ин-

декс платежной дисциплины – показатель, отражающий своевременность оплаты компанией счетов. Для получения индексов по интересующему контрагенту, зайдите в «Карточку контрагента»:

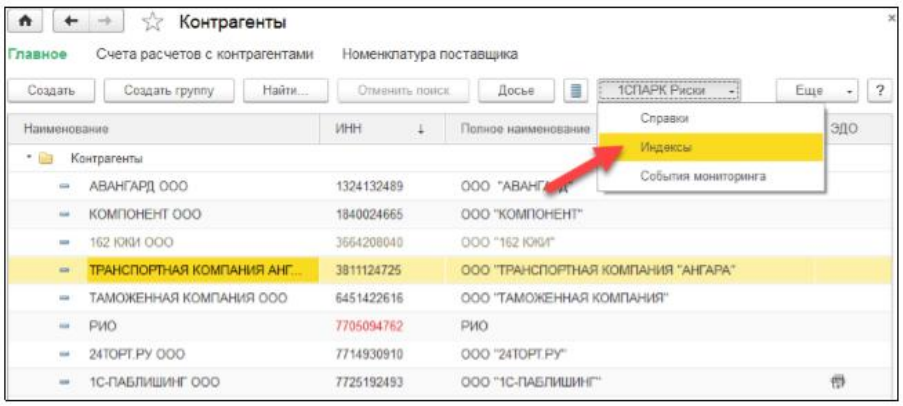


В поле «1СПАРК Риски» отображаются все три индекса. Если нажать на значение индекса, то откроется его краткое описание:

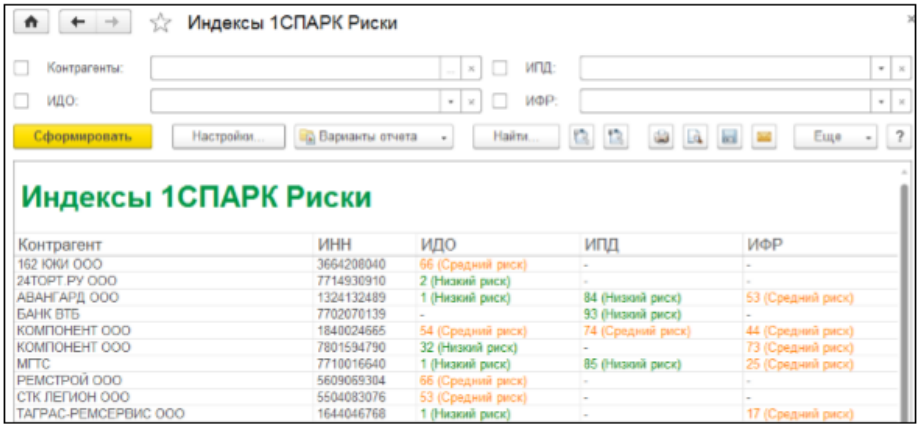


Напомним, что значение индексов рассчитывается на основании публично доступной информации о деятельности юридического лица. Если данной информации недостаточно для проведения анализа, индекс не отображается.

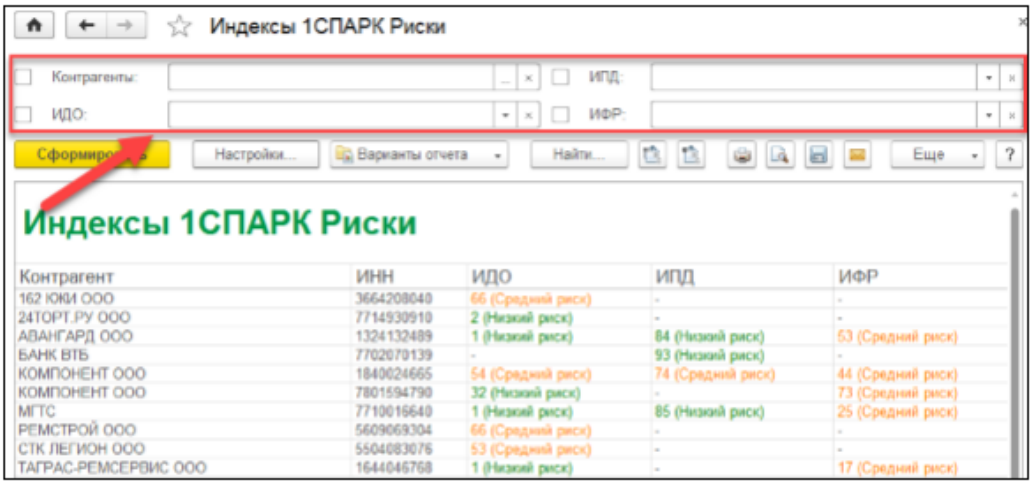
Чтобы получить значение индексов сразу по всем контрагентам из информационной базы, зайдите в справочник «Контрагенты» и нажмите на кнопку «1СПАРК-Риски»/ «Индексы»:



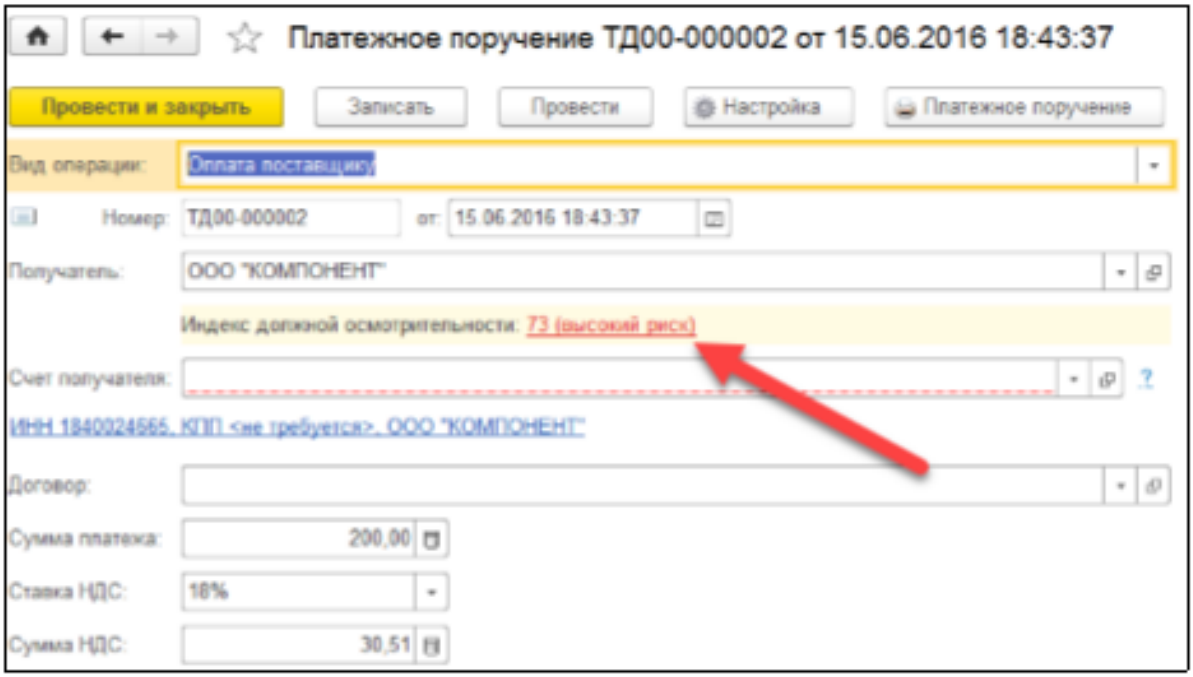
Откроется форма отчёта со списком индексов по всем контрагентам:



Для удобства работы со списком укажите в верхней части формы критерии их отбора:



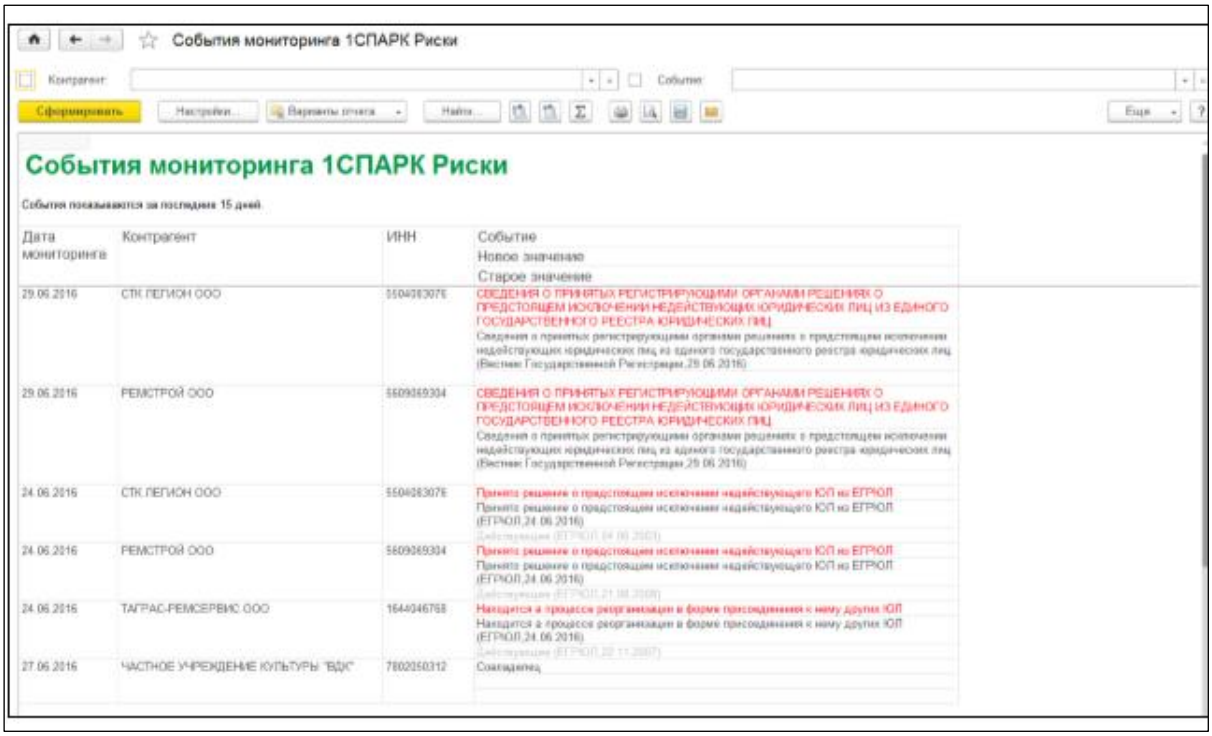
3. Осуществите предупреждения «по месту» при формировании платежного поручения. Для этого откройте документ платежное поручение и убедитесь, что рядом с полем «Получатель» показан Индекс должной осмотрительности, который предупреждает о возможных рисках при оплате счёта данному контрагенту:

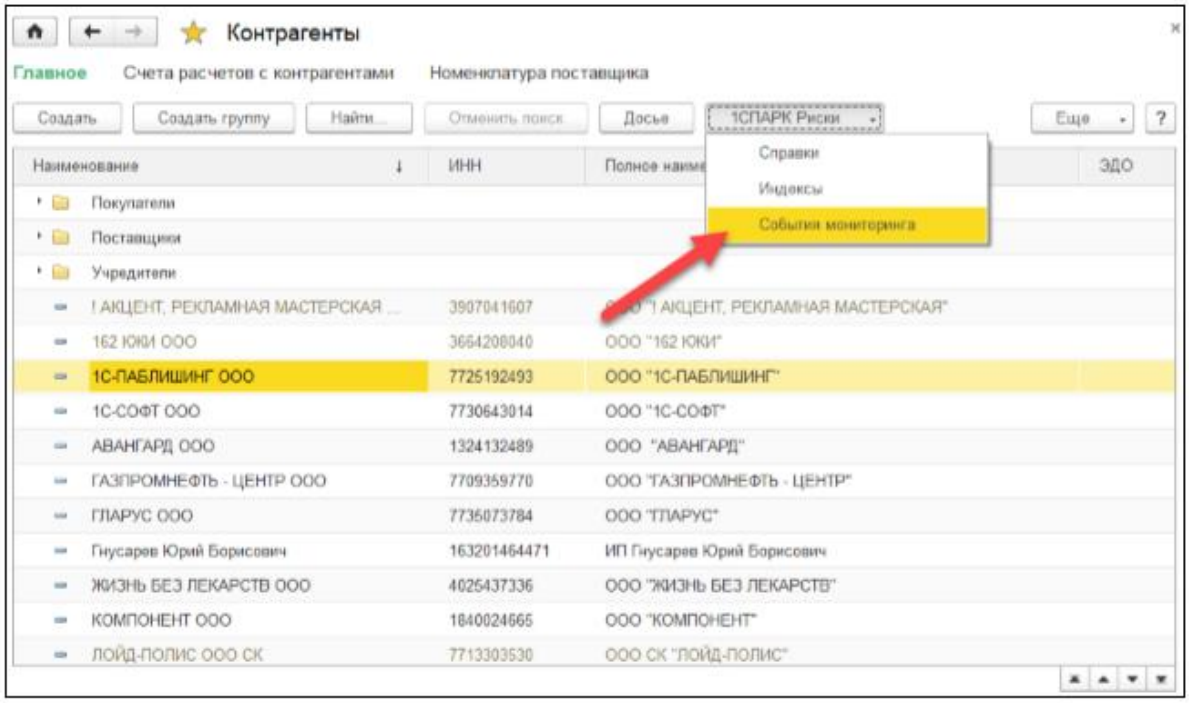


4. На начальной странице программы отображается блок «1СПАРК Риски». В этом блоке отображаются важные изменения у контрагентов, такие как ликвидация, реорганизация, изменение реквизитов и т.д.

Нажмите в блоке на ссылку «Все события», откроется отчет с подробным описанием событий.

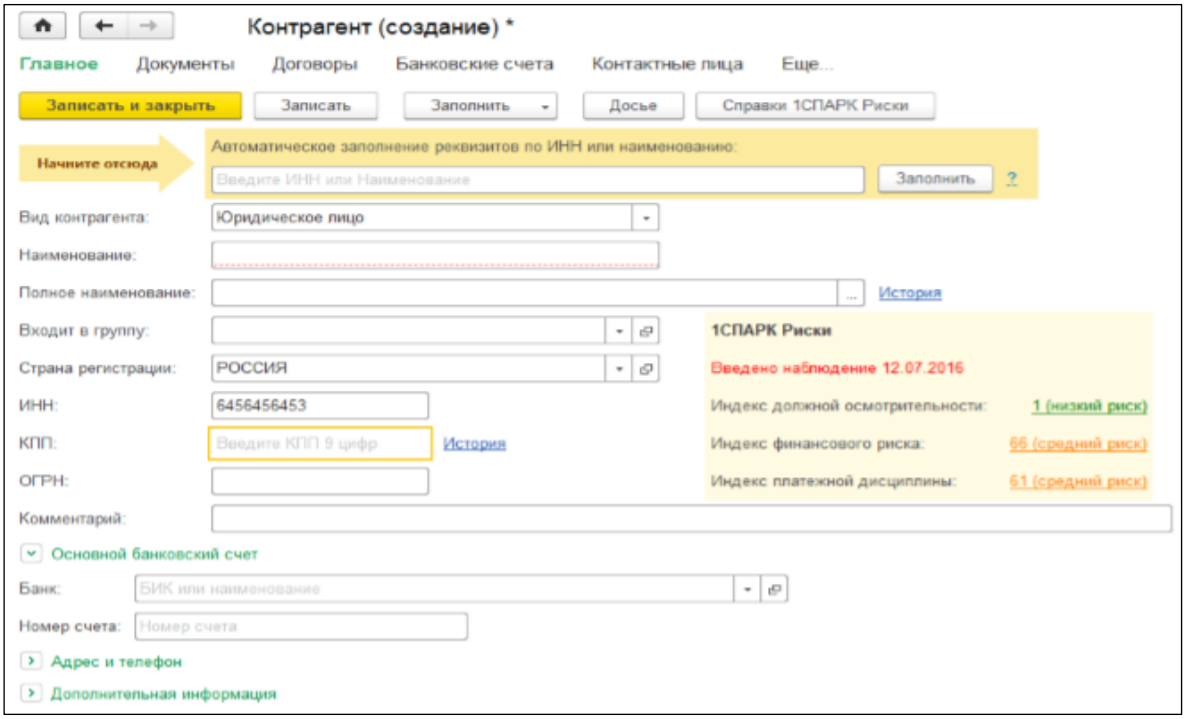
Получите аналогичный отчет с помощью справочника «Контрагенты»: кнопка «1СПАРК Риски»/ пункт «События мониторинга».



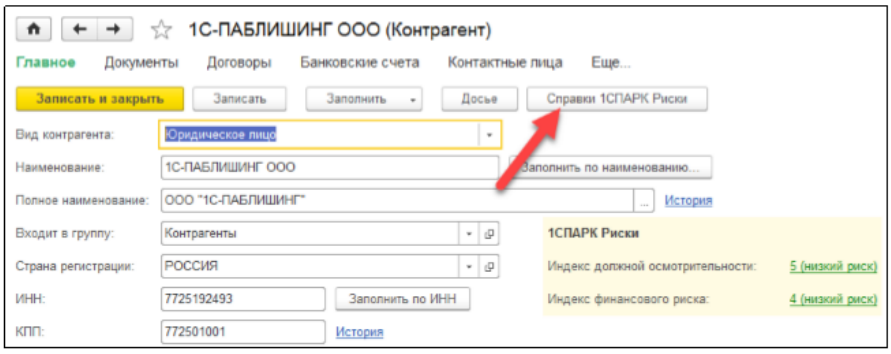


Мониторинг ведется по всем контрагентам из информационной базы.

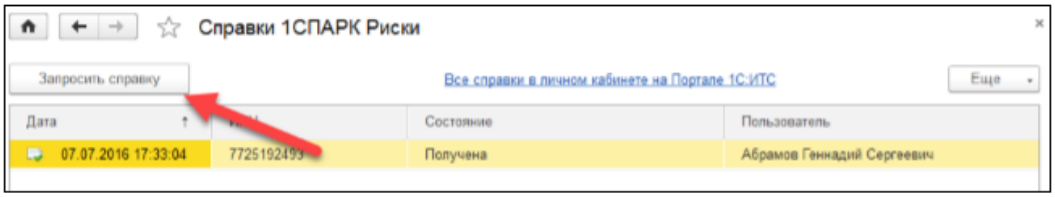
Если контрагента не нужно ставить на мониторинг, а только оценить его, то при создании нового контрагента в программе достаточно ввести его ИНН. Индексы будут отражены в карточке нового контрагента:



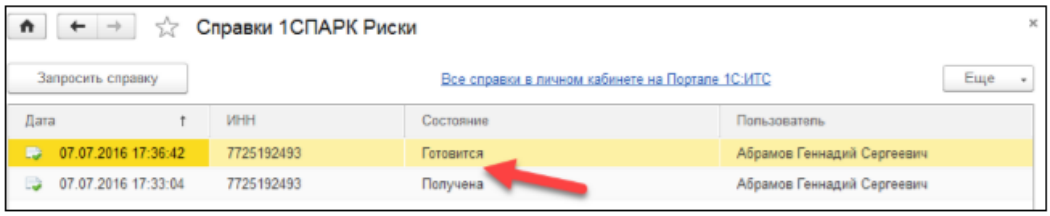
5. Получите бизнес-справку о контрагенте, для этого перейдите в «Карточку контрагента»/ кнопка «Справки 1СПАРК Риски»:



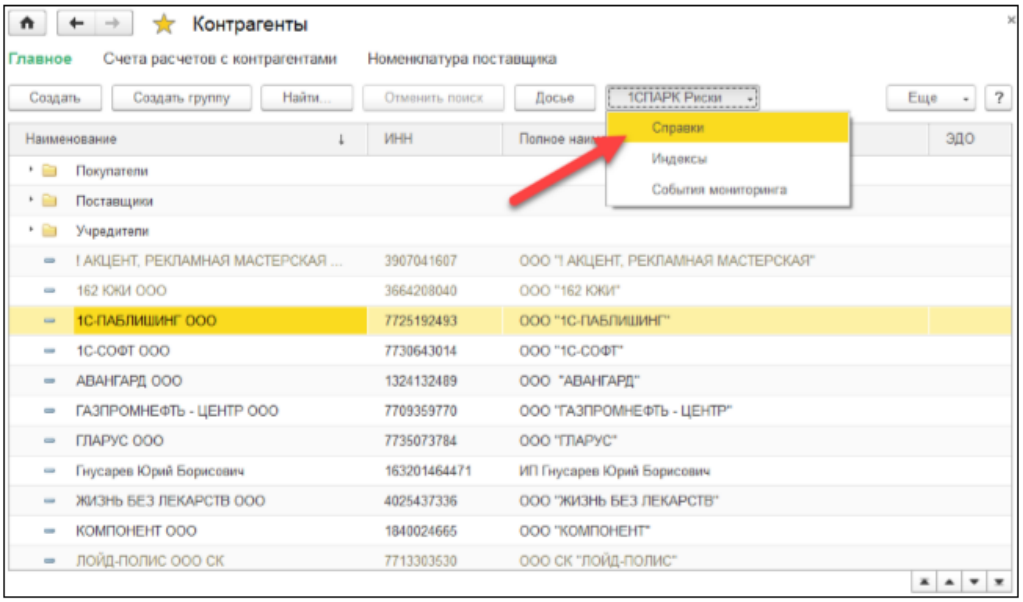
В открывшейся форме со списком ранее полученных справок по этому контрагенту закажите новую справку, нажав на копку «Запросить справку»:

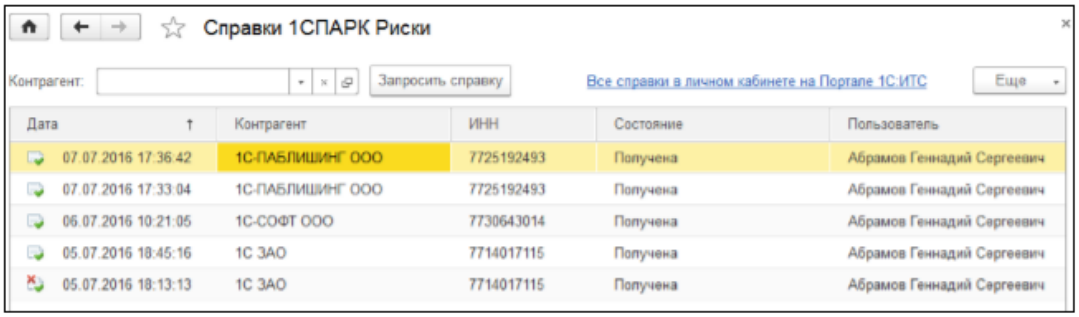


Подготовка справки занимает некоторое время. Как только справка готова, напротив нее в столбце состояния значение «Готовится» будет изменено на «Получена». Справки выдаются в формате PDF.



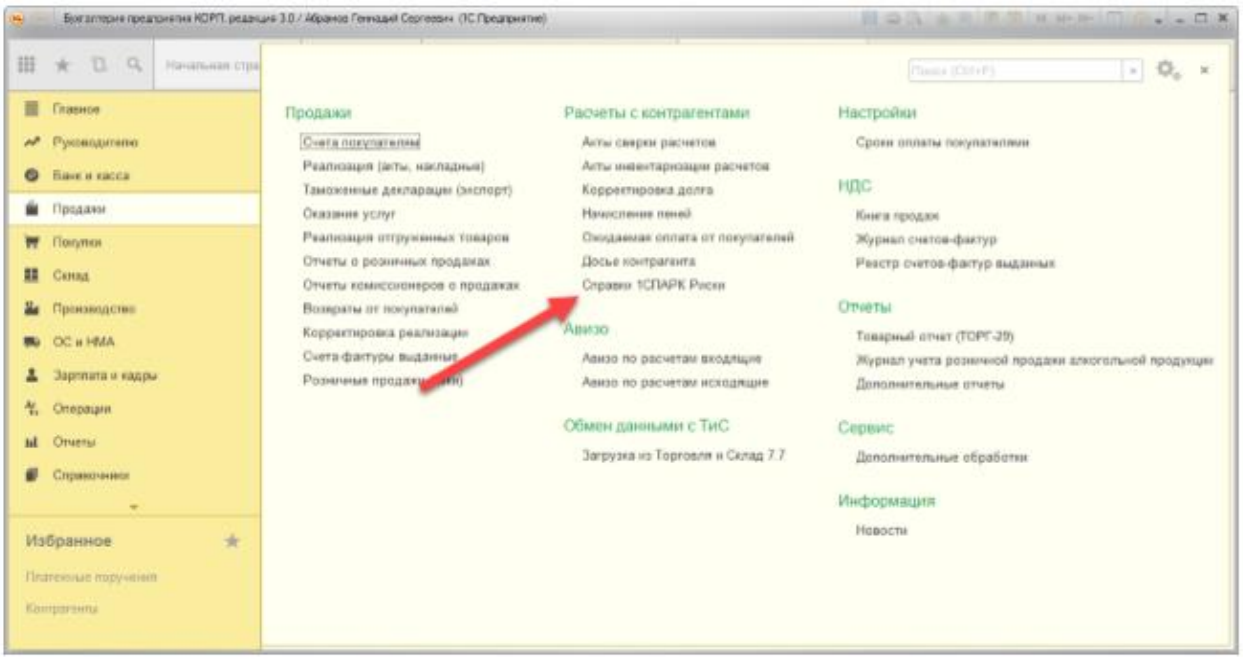
Посмотрите справки по всем контрагентам: кнопка «1СПАРК Риски»/ пункт «Справки»:





В открывшейся форме запросите повторную справку о контрагенте. Для этого нужно выберите нужного контрагента и нажмите «Запросить справку».

Откройте список полученных справок другим способом: из раздела «Покупки» или «Продажи»/ Расчеты с контрагентами/ Справки 1СПАРК Риски:



БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года». ГАРАНТ.РУ: http://www.garant.ru/products/ipo/prime/doc/71572608/#ixzz4wuKM9Lm3
2. Российская Федерация. Указ Президента РФ от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Система ГАРАНТ: http://base.garant.ru/71556224/#friends#ixzz4x0uCVEwN
3. ГОСТ Р 51897-2002, Менеджмент риска. Термины и определения.
4. ГОСТ Р 51898-2002, Аспекты безопасности. Правила включения в стандарты.
5. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
6. ГОСТ Р ИСО/МЭК 27001-2013 Системы менеджмента информационной безопасности.
7. Астахов, А.М. Искусство управления информационными рисками / А.М. Астахов. – М.: ДМК Пресс, 2010. – 312 с.
8. Варфоломеев, А.А. Основы информационной безопасности: учеб. пособие / А.А. Варфоломеев. – М.: РУДН, 2008. – 412 с.: ил.
9. Гапоненко, В.Ф. Экономическая безопасность предприятия. Подходы и принципы / В.Ф. Гапоненко, А.Л. Беспалько, А.С. Власов. – М.: Издательство «Ось-89», 2007. – 208 с. www.zahvat.ru 33743.pdf
10. Гильфанов, М.Т. Организационно-методический инструментарий оценки детерминант обеспечения экономической безопасности предприятия / М.Т. Гильфанов // Социально-экономические явления и процессы. – 2013. – № 8. – 1,0 п.л.
11. Гильфанов, М.Т. Дифференцированный инструментарий обеспечения экономической безопасности предприятия / М.Т. Гильфанов // Социально-экономические явления и процессы. – 2013. – №10. – 0,4 п.л.
12. Колесниченко, Е.А. Методические аспекты оценки и обеспечения экономической безопасности предприятия / Е.А. Колесниченко, М.Т. Гильфанов // Вестник Тамбовского университета. Серия: гуманитарные науки. – 2013. –

Вып. 11. – 0,8 п.л. (авт.0,5 п.л.)

13. Кришталюк, А.Н. Управление безопасностью бизнеса [Электронный ресурс]: курс лекций / Кришталюк А.Н. – Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 116 с.

14. Кузнецов, И.Н., Бизнес-безопасность [Текст]. – 3-е изд. / И.Н. Кузнецов. – М.: ИТК «Дашков и К°», 2012. – 416 с.

15. Ланкина, С.А., Флегонтов, В.И. Классификация и проблемы оценки рисков промышленного предприятия [Электронный ресурс]: http://schooled.ru/economic/safety/index.htm Интернет-журнал «НАУКОВЕДЕНИЕ», http://naukovedenie.ru, Том 7, №3 (май – июнь 2015) publishing@naukovedenie.ru

16. Павленков, М.Н. Экономическая безопасность (учебное пособие): НГ. Изд-во НГГУ им. Н.И. Лобачевского. 2015 г. – 151 с.

17. Пичугин, В.Г. Безопасность бизнеса [Электронный ресурс]: защита от уголовного преследования / В.Г. Пичугин. – М. – 175 с.

18. Суглобов, А.Е. Экономическая безопасность предприятия [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А.Е. Суглобов, С.А. Хмелев, Е.А. Орлова. – М. – 271 с.

19. Уразгалиев, В.Ш. Экономическая безопасность. Учебник и практикум для вузов / В.Ш. Уразгалиев. – СПб.: Издательство «Юрайт», 2017. – 374 с.

20. Фирсова, О.А. Экономическая безопасность предприятия [Электронный ресурс]: учебно-методическое пособие / О.А. Фирсова. – Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 165 с.

21. Экономическая безопасность предприятия [Электронный ресурс]. http://schooled.ru/economic/ safety/index.htm

22. Электронное учебно-методическое пособие. Обеспечение безопасности персональных данных. ООО «Издательский Дом «Афина», 194017, Санкт-Петербург, пр. Мориса Тореза, д. 98, корп. 1.

23. http://www.securitylab.ru/analytics/485289.php

24. http://www.spark-interfax.ru/1cspark

25. https://portal.1c.ru/download/public/instruction/1spark-report.pdf

26. https://portal.1c.ru/applications/47

27. https://buh.ru/articles/documents/48913/

28. http://net-consult.ru/services/1spark_riski/

Цыбулин Анатолий Михайлович
Запрягайло Валерий Митрофанович
Кулагина Ирина Ивановна

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ ПРОВЕРКИ БЕЗОПАСНОСТИ БИЗНЕСА

Учебно-методическое пособие

Электронное издание

Издательство Волгоградского института управления –
филиала ФГБОУ ВО РАНХиГС
400078, Волгоград, ул. Герцена, 10