Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тверской государственный университет»

Д.В. Трошин

Безопасность предприятия
смысл, онтология, оценка

Монография

ТВЕРЬ 2015

УДК 658:005
ББК У291-983
Т76

Рецензенты:
Доктор экономических наук, профессор, профессор кафедры КБ-10 «Экономическая безопасность» Московского государственного университета информационных технологий, радиотехники и электроники
Р.В. Илюхина
Доктор экономических наук, профессор кафедры конституционного, административного и таможенного права Тверского государственного университета
А.Н. Сухарев
Доктор военных наук, снс, заместитель начальника Центра международных и национальных систем прогнозного мониторинга АО «Российские космические системы»
С.В. Черкас

Д.В. Трошин
Т76 Безопасность предприятия: смысл, онтология, оценка: монография. – Тверь: Твер. гос. ун-т, 2015. – 212 с.

ISBN 978-5-7609-1048-6

В монографии на основе витального подхода предложена парадигма существования организационной системы для построения методологии анализа и обеспечения безопасности предприятия (хозяйствующего субъекта). Безопасное существование предприятия рассматривается, как его главная ценность. Содержание существования различных субъектов, ассоциированных с предприятием, а также самого предприятия как системной целостности. Оценка безопасности предприятия осуществляется на основе измерения степени удовлетворения интересов в результате противодействия угрозам с использованием потенциала обеспечения существования. В работе предложены формализованные подходы и модели для оценки безопасности предприятия с учётом когнитивной модели распространения рисков, модель аудита безопасности, а также модели для оценки достаточности финансовых ресурсов. В монографии выдвинута гипотеза: парадигма существования при достаточной методической проработке может объединить в единый механизм стратегического управления предприятием подходы к обеспечению безопасности, управления рисками, эффективности, обеспечения конкурентоспособности, стратегического планирования.

Работа предназначена для научных работников, консультантов и экспертов, разработчиков инструментария аудита безопасности предприятий, а также для владельцев представителей руководства хозяйствующих субъектов. Она также может оказаться полезной в учебном процессе.

УДК 658:005
ББК У291-983

ISBN 978-5-7609-1048-6

Оглавление

Предисловие

Становление неокапитализма в России в конце XX века сопровождалось жёсткой, недобросовестной конкуренцией, как правило, с густой криминальной окраской. Тотальный размах приобрело воровство, получившее нравственное оправдание в глазах обывателя, ощутившего результаты «всенародной» приватизации и лишённого какой-либо метафизической и даже социальной идеи, кроме лихо брошенного «обогащайтесь!». Эти условия диктовали нарождающейся буржуазии и коммерсантам решение лишь насущных вопросов выживания – физическая защита себя и семьи, оберегание обретённой собственности, страховка от всевозможных жуликов, которыми зачастую оказывались партнёры, борьба с хищениями и мошенничеством со стороны персонала, «согласование интересов» с чиновниками разрешающей и контролирующей подсистем государственного и местного управления. К решению этих задач, не считая криминальных элементов и организованных преступных групп (далее – ОПГ) и сообществ, ближе всего, естественно, оказались бывшие сотрудники правоохранительных органов и в какой-то мере военнослужащие.

В дальнейшем проблематика безопасности хозяйствующих субъектов развивалась. Неизбежно образ мышления многих «новых русских» должен был выходить за рамки элементарной расчётливости мелкого коммерсанта, если он хотел утвердиться как влиятельный участник экономических процессов, в том числе региональных и глобальных. Обеспечение безопасности стало неотъемлемой частью хозяйственной деятельности, успешного функционирования промышленных, коммерческих и других предприятий.

Сегодня обеспечение безопасности рассматривается как один из важных аспектов управления предприятием, на которое оказывают воздействия различные внешние и внутренние факторы, однако в традиционном варианте оно включает решение задач физической защиты ресурсов и борьбу с различными действиями криминального характера в ущерб предприятию. Например, в работе [1] проблематика обеспечения безопасности корпоративного уровня сводится, главным образом, к борьбе с хищениями и тому подобными неблаговидными

деяниями. Центральная роль, естественно, отводится службе экономической безопасности бизнеса, которой рекомендуется работать в тесном взаимодействии с правоохранительными органами.

Однако исследования и практическая работа показали, что локализация проблем обеспечения безопасности в пределах некоторой методологической, организационной и информационной подсистем не позволяет эффективно решать задачи хозяйственной деятельности на стратегическом уровне, ограничивает возможность построения мировоззренческого основания определения отношения безопасности и развития, препятствует созданию эффективной системы управления предприятием с использованием программно-целевого или проектного подхода, наконец, не в полной мере отвечает природе существования организационных систем.

Сегодня сотрудники служб безопасности крупного дела должны хорошо в нём ориентироваться, владеть финансовым и экономическим анализом, методами программно-целевого планирования и проектного управления, выполнять информационно-аналитическую работу, анализировать риски, обеспечивать защиту информационных ресурсов, организовывать создание и эксплуатацию сложных комплексов инженерной защиты объектов предприятий.

Очевидно, что в настоящее время сложилось новое направление профессиональной деятельности – обеспечение безопасности предприятия. Предмет и содержание этой профессии находятся на стыке проблематики прикладных задач обеспечения безопасности и экономической кибернетики в масштабе предприятий, функционирующих в том или ином секторе рынка, каждый из которых имеет свои сущностные особенности. В связи с этим предмет исследования в работе в отличие от традиционного расширен до охвата системной взаимосвязи основных аспектов жизнедеятельности предприятия. С этой позиции рассмотрены, так называемые, традиционные задачи обеспечения безопасности, которые, сохранив свою технологичную и содержательную специфику, более не автономизированы, а вписаны в общий контекст стратегического управления предприятием.

В работе фактически предпринята попытка поднять проблематику безопасности на высший уровень системности. Предложенная

парадигма безопасного существования позволяет увязать единой логикой управления задачи стратегии и тактики, известные в практике управления подходы (SWOT-анализ, пять сил Портера, STEP-анализ, или, по-другому, PEST-анализ, управление рисками, оценку эффективности деятельности). Однако для реализации замысла работы потребовалось осмысление самой категории «безопасность», её места и роли в системе ментальных и организационных моделей функционирования предприятия.

В связи с этим в первой главе проведён анализ точек зрения на содержание категории «безопасность», представленных в отечественной научной литературе. На основе парадигмы существования (витальный подход к исследованию социальных систем [2]) на вербальном уровне предложена методологическая основа обеспечения безопасности хозяйствующего субъекта, включая единый механизм обеспечения безопасного существования, интегрирующего проблематику стратегического управления, развития и традиционных задач обеспечения безопасности на разных уровнях управления. Обоснована онтология проблематики безопасности.

Вторая глава посвящена изложению формализованных подходов к решению задачи анализа состояния безопасности, разработанных на предложенной методологической основе. Стержнем методологии является оценка защиты интересов предприятия, поддержание и развитие потенциала обеспечения существования в соответствии с актуальными и развивающимися интересами и влияния на предприятие, как субъекта деятельности, среды его существования. В частности, предложены когнитивная модель оценки рисков с учётом их взаимовлияния, методика ранжирования угроз на основе оценки соответствующих им рисков.

Третья глава фактически носит прикладной характер. Она посвящена методологии анализа достаточности потенциала обеспечения существования, в части касающейся финансовых ресурсов. Эти ресурсы являются системообразующими для деятельности хозяйствующего субъекта. Несмотря на обилие работ по финансовой устойчивости и финансовой безопасности предприятия проблема их оценки остаётся актуальной. В монографии представлен краткий анализ существующих подходов к оценке финансовой устойчивости, предложена модель её

комплексной качественной оценки и модель оценки достаточности финансового ресурсов на основе имитации движения денежных средств и рационального использования ликвидов.

Объектом исследования в работе является предприятие как «территориально обособленная хозяйственная организация, систематически осуществляющая производство товаров, выполнение работ или оказание услуг для удовлетворения внешних относительно предприятия потребностей, обладающая правом самостоятельности распоряжаться своим имуществом и результатами своей деятельности, ведущая предписываемые регламентами формы учёта своей деятельности и не содержащая в своём составе обладающих перечисленными свойствами объектов» [3]. Однако общесистемный характер используемой парадигмы позволяет использовать идею предлагаемого подхода к рассмотрению и обеспечению безопасности любых организационных систем, в том числе не относимых к агентам экономических отношений. В качестве синонима предприятия в работе используется термин «хозяйствующий субъект».

В исследованиях и практической деятельности распространено понятие «безопасность бизнеса», отношение к которому требуется определить для однозначности смысла дальнейшего изложения. В работе [3] отмечена взаимная превращённость ролей понятий «бизнес» (в качестве предпринимательской деятельности) и «предприятие» (в смысле вышеприведённого определения) в паре содержание-форма. Однако «предпринимательская деятельность» не является субъектом, поэтому с точки зрения парадигмы существования, которая рассмотрена в первой главе монографии, выражение «безопасность бизнеса» является научно некорректным и допустимо лишь в разговорных формах общения.

Предлагаемая работа не претендует не всеохватность. В ней не представлено прикладное методическое обеспечение для решения задач оценки потенциала обеспечения существования по ряду составляющих: входные потоки (кроме финансов), кадры, информация и знания, гудвилл и др. Осталась за рамками монографии лишь обозначенная в общих методологических основаниях проблематика выявления и оценки конфликта интересов в узлах их сосредоточения, как источников угроз. Методология анализа и конфликта интересов экономических агентов на

уровне предприятия с использованием математических инструментов и численных измерений представлена в работе [4]. Перспективными являются исследования и разработки по созданию единого информационного пространства анализа и оценки безопасности предприятия, включающего базы данных и знаний, комплекс методик, программно-инструментальных средств и типовых регламентов, адаптируемых к конкретным условиям применения. Требуют теоретического изучения условия и границы применения витального подхода, а также проблематика выявления интересов и оценки их достижения в части, выходящей за пределы финансового результата.

В монографии отражен в основном авторский подход к ряду ключевых аспектов анализа проблем безопасности хозяйствующего субъекта, но используются и заимствования, и некоторые общеизвестные положения для достижения «сюжетной» целостности. Тематика, хорошо представленная в имеющейся литературе, как правило, только упоминается. Задача подготовки всеобъемлющей теории безопасности хозяйствующего субъекта, вбирающей в себя всю методологию эффективного ведения дела и методический арсенал решения соответствующих частных задач исследования операций сохраняет актуальность.

Работа предназначена для научных работников, консультантов и экспертов, разработчиков инструментария аудита безопасности предприятий, а также для владельцев и представителей руководства хозяйствующих субъектов. Она также может оказаться полезной в учебном процессе.

Автор с признательностью отмечает, что в значительной мере на разработку методологической основы работы повлияло её заинтересованное обсуждение с доктором философских наук, профессором Селивановым А.И.

Введение

Развитие глобального финансово-экономического кризиса 2007–2008 годов в российском направлении наглядно показало губительность недооценки задач обеспечения безопасности предприятия по сравнению с задачами его экстенсивного расширения. Даже в некоторых крупных российских бизнес-империях не оказалось сил и средств, которые могли бы предостеречь собственников от рекомендаций некомпетентных, узкомыслящих стратегов и аналитиков, удержать азартных, безответственных, а порой недобросовестных топ-менеджеров от добывания прибылей «здесь и сейчас» в ущерб диверсификации и развития технологий для переделов высоких уровней. В результате активы ряда крупнейших отечественных неокапиталистов оказались беззащитны. Часть из них была спасена государством. Несомненно, что в этих случаях экономическая безопасность не была обеспечена. Одной из причин этого является методологическая узость взгляда на проблематику безопасности. Новые угрозы потери зарубежных активов и отсутствия ресурсов для перекредитования возникли у ряда российских компаний в связи с наложением на Россию экономических санкций США и их союзниками в 2014 году. Выяснилось, что поиск рентабельных мест приложения капитала, вывод его из России в целях сокрытия от правоохранительных органов и минимизации налогообложения могут привести к фактической утрате активов в результате политики иностранных государств.

Проблемы выживания и процветания хозяйствующих субъектов явно обостряются в условиях глобализации. Причём касается это не только крупных транснациональных корпораций, но и хозяйствующих субъектов всех уровней деловой лестницы вплоть до малых предприятий и предпринимателей без образования юридического лица. Несмотря на изменившийся характер конкурентной борьбы, институциональную организацию хозяйственной деятельности, современная глобализация не создала принципиально новых, несуществовавших ранее, хотя бы в малом, угроз безопасности в экономической сфере, как на национальном уровне, так и на уровне отдельных хозяйствующих субъектов. В то же время она существенно преобразовала механизмы реализации угроз и соответствующие им уровни рисков, поменяла расстановку акцентов в структуре задач управления созданием и реализацией товаров и услуг.

В этой связи основные современные проблемы практики российских хозяйствующих субъектов можно свести к следующему [5].

1. Вытеснение отечественных производителей с внутреннего рынка в результате предложения более популярных, более качественных, или более дешёвых импортных товаров. Большое значение здесь имеет создание сетей сервисного обслуживания сложных товаров на протяжении всего их жизненного цикла. При этом в ряде случаев эксплуатация таких товаров увязывается с использованием сопутствующих товаров, предлагаемых под тем же брендом той же корпорацией: масло для двигателей, чернила для картриджей и т. д.

2. Целевое банкротство российских предприятий с последующим выкупом и ликвидацией или перепрофилированием для устранения конкурента.

3. Необходимость использования международных стандартов, в том числе разработанных (или заказанных) транснациональной корпорацией (далее – ТНК). При этом стандарт может иметь формальное символическое значение, однако его несоблюдение повлечёт применение правовых запретов на ввоз товаров (например, якобы шумных авиалайнеров) или снижение стоимости бренда.

4. Эмиграция наиболее квалифицированных кадров, в том числе через структуры ТНК, в орбиту деятельности которых вовлечены российские хозяйствующие субъекты. Этому также способствует конкуренция на рынке образовательных услуг. Стремление ВУЗов увеличить свой сектор рынка потребления образовательных услуг приводит к тому, что они участвуют в международных процессах подготовки высокопрофессиональных кадров для зарубежных и международных компаний за счёт людских ресурсов России.

5. Заполнение рынка труда рабочих и аналогичных профессий низкоквалифицированной, зачастую необразованной и несоответствующей культурным стандартам России рабочей силой, формируемой мигрантами из стран СНГ и развивающихся стран Юго-Восточной Азии. Непритязательность трудовых мигрантов на уровни оплаты труда и социальной защиты вытесняет россиян из целых отраслей экономики, прежде всего, строительства, сферы услуг, жилищно-коммунального хозяйства, торговли, транспорта. Предприятия, которые ориентируются на отечественные трудовые

ресурсы и пытаются соблюдать соответствующее законодательство, проигрывают по уровню рентабельности.

6. Перевод российских ноу-хау в ТНК с последующим патентованием зарубежными субъектами через хорошо отлаженные механизмы.

7. Утечка конфиденциальной (технической, коммерческой, персональной и другой) информации по телекоммуникационным корпоративным, технологическим и глобальным сетям, непосредственно через вычислительную и оргтехнику. Эта угроза приобрела очевидность в широких слоях общества в свете разоблачений в 2013 году шпионской деятельности американских спецслужб в глобальном масштабе. Своим вниманием последние не обходят и зарубежные корпорации[1].

Утечка конфиденциальной корпоративной информации может происходить и с эмигрирующими сотрудниками. В этом случае эмиграция может быть и, так называемой, внутренней, например, из российской компании в ТНК или предприятие-нерезидент.

8. Вытеснение с традиционных зарубежных рынков, в том числе в результате протекционизма, конкурентов со стороны мотивированных органов власти иностранных государств.

9. Сильная зависимость от состояния мировой экономики и рынков. Эта проблема наиболее наглядно отражает диалектику взаимосвязи интересов и угроз в национальном и корпоративном масштабах. В ходе процессов мирового разделения труда, активно развернувшихся в 90-х годах прошлого столетия, наиболее выгодным бизнесом в России являлись торговля, добыча и экспорт природного сырья, в особенности углеводородов. Обрабатывающие отрасли промышленности, лишённые государственной защиты, захлестнула волна экономической глобализации. Они до сих пор не восстановлены по валовому выпуску продукции в объёмах 1991 года. В результате в международном разделении труда Россия переместилась в сторону поставщика сырьевой продукции с низкой добавленной стоимостью и попала в сильную зависимость от состояния мировой экономики и экспортных цен на энергоносители, металлы и другие природные ресурсы. Когда рынок спроса в развитых странах в 2008–2009 гг. сжался, цены на нефть, газ, металлы упали, российская экономика также

[1] См., например, RG.RU. Российская газета. 17.12.2013. [Электронный ресурс]. URL: http://www.rg.ru/2013/12/17/brazil-site.html Дата доступа 18.04.2015.

претерпела рецессию, не являясь источником кризиса. Если бы достаточно большая часть экономики России была отведена машиностроению, продукции товаров широкого потребления и т. п., то она бы обладала необходимым уровнем самодостаточности для обеспечения устойчивости к экономическим катаклизмам за рубежом.

10. Зависимость от состояния мировых финансов при кредитовании в зарубежных и транснациональных источниках, если выплаты процентов и долга увязаны с учётными ставками и покупательной способностью валюты. Здесь следует отметить, что по состоянию на 1 апреля 2015 г. общий внешний корпоративный долг (банки и другие сектора, исключая органы государственного управления и Центральный банк) России составил $ 510,6 млрд, хотя и сократился сравнению с предыдущим годом почти на 27 %. Долг превышает стоимость внешних активов этого сектора экономики почти на 3 %[2].

11. Сильная зависимость реализации крупных инвестиционных проектов в обрабатывающей промышленности от зарубежных поставок станочного и другого технологического промышленного оборудования, поскольку в России в настоящее время оно почти не выпускается. Например, уровень производства станков в 2014 году от уровня 1990 года сократился в 20–25 раз по различным современным типам.

12. Инфляция издержек российских хозяйствующих субъектов вслед за повышением мировых цен на нефть и газ. В результате снижается рентабельность и спрос. Проблема имеет решение, если государство будет жёстко демпфировать волатильность внутренних цен в ответ на колебания глобальной конъюнктуры энергоносителей.

13. Утрата или «замораживание» активов за рубежом в результате социально-политических потрясений в стране деловых интересов, политически тенденциозного и внеправового применения административного ресурса иностранными властями.

Одной из важнейших угроз экономической безопасности хозяйствующих субъектов России, вытекающих из глобализации, является необходимость для предприятий конкурировать в глобальном масштабе. При этом речь идёт не о конкуренции среди тысяч или сотен компаний, где значительно легче найти свою нишу, а о соперничестве с несколькими, но огромными вертикально-интегрированными

[2] URL: http://www.cbr.ru/statistics/?Prtid=svs&ch=itm_47538#CheckedItem [Электронный ресурс]. Дата доступа 15.08.2015.

транснациональными структурами, функционирующими под всемирно известными брендами. Подобные структуры, как отмечено выше, имеют значительные преимущества в продвижении своей продукции за счёт фактора «масштаба». Рентабельность издержек на продвижение своих брендов у них значительно меньше. Они пользуются массированной поддержкой на политическом уровне. Например, в период кризиса 2007–2010 годов правительство США не позволило разориться американским гигантам автомобильной индустрии, в частности «General Motors», а президент Б. Обама заявил: «мы не можем, не должны допустить и не допустим, чтобы наша автомобильная промышленность попросту исчезла»[3].

Конкурентоспособность – понятие относительное. Оно отражает не столько качество и эффективность предлагаемого товара, сколько способность выиграть борьбу за потребителя. В конкурентной борьбе каждый её участник в идеале стремится достичь монополии на рынке. В её арсенале у современных компаний широко представлены различные способы ведения информационных торговых войн, скупки патентов и других ключевых активов, коммерческий и промышленный шпионаж, «вербовка» руководителей и лучших специалистов, подкуп должностных лиц государственных органов для оказания давления на конкурентов, скрытая скупка активов, спекуляции в информационном пространстве на экологическую тему, подстрекательство протеста в трудовых коллективах, хакерские атаки на корпоративные сети, переманивание поставщиков и клиентов и др. Наиболее распространёнными, простыми и эффективными средствами завоевания рынков и закрепления на них являются массированная рекламная компания, демпинг, коррупция и коммерческий подкуп.

Сегодня даже мелкий отечественный производитель товаров и услуг широкого потребления ощущает давление конкуренции в глобальном масштабе. Так, в российских городах обычные торговые точки пищевых продуктов ежедневного употребления почти вытеснены брендовыми сетями супер- и гипермаркетов. Большая часть этих коммерческих структур являются ТНК, работающими под популярными торговыми марками. Их полки заполнены в основном импортной технологичной (долго хранимой, удобно перегружаемой, привлекательно упакованной)

[3] Радио «Свобода». [Электронный ресурс] URL: http://www.svobodanews.ru/content/transcript/1746288.html. Дата доступа. 12.07.2014.

продукцией, что ставит барьер перед местными и региональными производителями аналогичной по сути продукции, зачастую более экологичной, но непопуляризированной. В данном случае фабрики и заводы по изготовлению еды, в том числе зарубежные или в форме совместных предприятий, вступили во взаимовыгодной альянс с торговыми сетями. При этом маркетинговые стратегии согласовывают фасовку и упаковку товаров с технологиями внутренней логистики и хранения в крупных магазинах самообслуживания, используют метафоры, сопровождающие товар по всей цепи его продвижения до прилавка (полки), включая оформление торговых залов, мерчендайзинг, мультимедийные технологии непосредственно в местах продажи. Активно эксплуатируются физиологические и психологические особенности восприятия информации и формирования мотивации человека, который оказывается слабо защищённым перед системой манипулирования его потребностями и поведением как покупателя-добытчика. Мелкие и средние отечественные производители и торговцы таких возможностей не имеют.

Изучение состояния дел в сфере обеспечения безопасности в отечественных хозяйствующих субъектах позволяет сформулировать следующие основные проблемы [5].

1. Не сложился единый подход к определению смысла категории «безопасность». Эта категория чётко не увязана со стратегическими целями функционирования и развитием.

2. В организационной и практической плоскостях задачи обеспечения безопасности, как правило, сводятся к задачам физической защиты персонала, товарно-материальных ценностей (далее – ТМЦ), информационных ресурсов, осуществлению контрольно-пропускного режима, изучения персонала в целях выявления лиц, имеющих плохую репутацию и(или) отношение к криминальным структурам, детективной деятельности, контроля соблюдения противопожарных правил и т. п.

3. Деятельность по обеспечению безопасности в узком смысле, представленном в предыдущем пункте, управление рисками, задачи устойчивого развития (прежде всего, обеспечения конкурентоспособности), кадровая политика, развитие информационных технологий (в аспекте информационной безопасности), вопросы качества и дисциплины исполнения бизнес-процессов и технологий организационно, методически и информационно разобщены.

Взаимодействие носит, как правило, фрагментарный характер и в основном по фактам нанесения конкретного ущерба. Горизонтальные связи не стимулированы (порой пресекаются) и недостаточно регламентированы «сверху».

4. Внутренние документы, определяющие управление рисками и устойчивым развитием, во многом носят декларативный характер и не могут служить руководством к действию в реальных ситуациях, поскольку не содержат методик, алгоритмов выработки и реализации решений в плановом и чрезвычайном режимах, не поддержаны регламентированной системой интерактивных программно-инструментальных средств и постоянно актуализируемыми базами данных и знаний. Методически грамотно организованные ситуационные анализы в практике принятия бизнес-решений используются редко.

5. Задачи оценки рентабельности и эффективности деятельности системы обеспечения безопасности, как правило, декларируются, однако до конкретных методик не доведены и на практике решаются на уровне «волевых» оценок со стороны менеджмента компаний.

Следует отметить, что адекватная оценка эффекта, в частности, экономического, деятельности систем обеспечения безопасности имеет объективные трудности и в прикладной науке не решена. Основная из них заключается в получении адекватной и очевидной для лиц, принимающих решения (далее – ЛПР), оценки пользы предупредительных мероприятий и мер.

6. Проблемы формирования лояльности персонала и формирования корпоративной солидарности (коллективизма) в решении стратегических задач хозяйствующего субъекта и обеспечения его безопасности решаются через социальную политику и составление кодексов этики. Однако они разрабатываются, главным образом, как дань сложившейся моде, диктуемой крупными западными и транснациональными корпорациями, и, как правило, не служат одним из конкурентных преимуществ. Кодексы этики утверждают общие принципы взаимной ответственности, которые, за редким исключением, не идут дальше перечисления прав и обязанностей, уже определённых законодательством России. В то же время состояние дел в части, касающейся корпоративной солидарности, не благоприятно. В редких случаях компании являются предметом гордости их сотрудников. Большая часть персонала, включая топ-менеджеров, традиционно

рассматривают их, исключительно как временно наиболее удобное средство извлечения доходов и других выгод. В среде российских офисных работников и руководителей сложился обычай менять место работы каждые 2–3 года.

Укреплению сплочённости коллектива не способствует недопустимо большой разрыв уровней оплаты труда и различных вознаграждений высшего руководства и среднего управленческого звена, которые в крупных корпорациях достигают 10 и более раз. Сравнить же зарплату рядовых клерков в управляющих компаниях и заводоуправлениях, рабочих, младшего технического и обслуживающего персонала с доходами топ-менеджмента можно только по шкале десятичных логарифмов. В результате сложившейся системы распределения результатов общественного труда трудовые коллективы фактически отстранены от участия в этих процессах. В целом общественное мнение расценивает распределение доходов, как несправедливое. Интересно отметить, что в схоластичной картине мира, разработанной в античной философии, высшей ценностью считалась безопасность жизнедеятельности и для её обеспечения предписывалось равномерно распределять богатство среди населения, не допускать имущественного расслоения, предоставлять всем гражданам одинаковые средства, необходимые для жизнедеятельности [6].

Не выполняют функции сплочения и стабилизации коллектива и профсоюзы, которым практически повсеместно в России отведена символическая роль. В стратегических планах, концепциях обеспечения безопасности ответственность и роль профсоюзов, как правило, не предусматриваются. Несмотря на активную либеральную пропаганду после шокового перехода к капиталистической системе хозяйствования и внедрение в массовое сознание россиян западных ценностей потребительского общества, типичный россиянин в основе своего мироощущения и самоидентификации не стал западным. Отчуждение российского работника от бытия предприятия – не только и даже не столько от собственности, сколько от смысла, цели, значимости его существования – приводит к невозможности добиться от него не только инициативы и самоотдачи, но и элементарной добросовестности.

В таких условиях сохранять и приумножать человеческие ресурсы и укреплять безопасность предприятий под натиском глобализации невозможно. Для эффективного решения проблем безопасности

необходимо не только совершенствование организационных механизмов и информационных технологий, но и радикальный пересмотр отношения к хозяйственной деятельности, к предприятию. Первая должна рассматриваться не как частное дело, удовлетворяющее актуальные потребности собственников и технократии, а как общественно значимый процесс. Второе требует увидеть в себе не только средство для получения прибыли, но и социальный организм, представляющий ценность не только для собственников, но и для социальных групп различного масштаба, имеющий сложную систему интересов, переплетённую с интересами региональных социально-экономических систем и общества в целом.

Следует отметить, что позитивным фактором сегодня является проникновение в среду российского предпринимательства и производства идей системного подхода к решению проблем безопасности. В ряде передовых компаний это нашло отражение на уровне системы основных взглядов и принципов в локальных нормативных и концептуальных документах. Объективные потребности экономики мотивировали интерес к проблематике безопасности предприятий, как исследователей, так и работников образования. Однако перестройка мировоззрения и обычаев делового оборота происходит с заметным отставанием от темпов глобализации.

Задача настоящей монографии состоит в том, чтобы придать ускорение и научную поддержку отмеченным положительным тенденциям за счёт коррекции концептуального взгляда на проблематику безопасности и развития методологии решения соответствующих задач.

Очевидно, что проблематика безопасности тесно увязана с тематикой стратегического управления, обеспечения конкурентоспособности. Из вышеизложенного прямо явствует, что предприятию может быть нанесён большой урон, вплоть до ликвидации (кончины), при ошибках управления, при выборе неверной стратегии развития, даже если защита материальных и финансовых ресурсов будет поставлена должным образом на уровне охраны и контроля правомочности их использования. Однако и на практике, и в научно-прикладных исследованиях обеспечение безопасности рассматривается как отдельный, содержательно автономный блок деятельности,

дополняющий усилия по развитию, повышению эффективности, обеспечению конкурентоспособности и т. д.

Объём научной литературы – монографий, учебных пособий, научных статей – огромен и трудно обозрим. В литературе специалисты рассматривают понятийную базу, концептуальные и организационные вопросы обеспечения безопасности предприятия, вплоть до должностных инструкций, приводят рекомендации по осуществлению информационно-аналитической работы, предлагают различный методический инструментарий (см., например, [7–14]). Однако существующие результаты далеки от совершенства, имеют множество пробелов. Прежде всего, не завершена разработка понятийной базы, задачи обеспечения безопасности, как отмечено выше, системно недостаточно увязаны с целями ведения и развития бизнеса. Задачи методического обеспечения управления безопасностью, включая её оценку, в основном решаются на уровне вербального описания проблем и подходов к решению, обобщённых экспертных оценок [15–23], а также с использованием индикативных методов [24–30]. Важно отметить, что ныне распространённый индикативный подход может дать лишь поверхностную оценку, поскольку, реализуя методологию позитивизма, эклектично и поверхностно рассматривает ограниченное множество аспектов состояния интересующего объекта обеспечения безопасности, не учитывает взаимосвязь между индикаторами, влияние индикаторов на интересы, цели функционирования, отношения с внешней средой и механизмы использования ресурсов предприятия для парирования угроз. Интегрированная оценка безопасности осуществляется путём аддитивного агрегирования различных индикаторов, степени превышения пороговых значений некоторых показателей состояния активов и процессов предприятия и т. п. Такие агрегации не позволяют обнаруживать причины негативных явлений, маскируют конфликты интересов, лежащие в основе нарушения безопасности, прямо не соотносятся с интересами функционирования предприятия.

В отдельную группу можно выделить работы, посвящённые оценке и управлению рисками, например, [22, 31–37]. Здесь также не сложилась понятийная база, множатся смыслы риска и соответственно утрачивается строгость анализа и возможность построения для него математических моделей, что подробно будет рассмотрено в главе 1. Наблюдается явный недостаток методологии описания отношений

между рисками, отношений риски-интересы, риски-угрозы. В литературе приведено множество классификаций рисков, включающих десятки их наименований, однако достаточно детально проработаны только методы и методики оценки финансовых рисков, поддающихся статистическому анализу. Одной из причин этого является то, что риски не дифференцируются от угроз.

В работе [38] на основе посылки о циклических колебаниях (по логике работы, надо понимать гармонического характера) деловой активности предлагается оценивать экономическую безопасность как ограничение значений «ключевых параметров хозяйственной деятельности» в заданном коридоре, который содержит тренд, определяемый некими долговременными факторами. Верхняя граница параметров ограничивается лишь на основе спорного постулата, что чем больше подъём, тем глубже падение. При этом отношения со средой функционирования рассматриваются лишь косвенно. Смысловые корни и научное обоснование этого подхода не рассмотрены, и его операциональная полезность не ясна.

Методологической новизной и практической перспективностью отличаются работы Минаева Г.А. (представителя школы Прохожева А.А.) [39, 40], в которых в основе безопасности как научной категории рассматриваются диалектические отношения интересов и угроз. Обосновано, что разрешением этих отношений достигается безопасность и обеспечивается развитие организации, реализация её интересов. При этом функции безопасности отводится роль защиты функции развития и реализации интересов. Очевидно, что здесь также безопасность рассматривается как дополнение развитию. Однако смысл и цель развития остаются фигурами умолчания. Представляется, что после обнаружения отношения интерес-угроза подчинение безопасности развитию нелогично. Их роли следует поменять местами.

В работе [41] безопасность оценивается через ущерб интересам организации по различным функциональным составляющим, что формально близко идеям указанных работ Минаева Г.А. и предлагаемой в настоящей монографии парадигме. Однако, поскольку содержание используемых категорий: интерес, ущерб, воздействие - не раскрыто, определить концептуальную широту и глубину подхода невозможно. Статус оценки безопасности в системе задач управления предприятием однозначно неартикулирован.

Настоящая работа выполнена с намерением уточнить системную парадигму исследования безопасности предприятия, конкретизировать смысл основных понятий в проблематике безопасности, определить место и взаимосвязь соответствующих категорий в системе задач стратегического управления предприятием, предложить системно проработанный подход к оценке безопасности предприятия, которая могла бы служить для применения инструментов управления. Основное внимание сосредоточено на методических, информационных, и частично организационных аспектах системного подхода к стратегическому управлению жизнедеятельностью предприятий, исходя из положения, что безопасное существование – ключевая ценность организационной системы и стремление к нему является системообразующим мотивом деятельности, включая развитие.

В специальной литературе применительно к хозяйствующим субъектам зачастую рассматривается экономическая безопасность предприятия без конкретизации, её места в общей онтологии проблематики безопасности предприятия. Это объяснимо, поскольку предприятие является субъектом, прежде всего, экономических отношений и содержание его деятельности определяется, главным образом, экономическими интересами. Однако для системной строгости целесообразно изначально вести речь о безопасности хозяйствующего субъекта, а в процессе углубления онтологии рассматриваемого предмета, а также по соображениям практического удобства использовать различные виды безопасности, если потребуется, в том числе экономическую.

1. Методологическая основа анализа безопасности

1.1. Онтология безопасности субъекта. Основные понятия

Базовой категорией проблематики, рассматриваемой в настоящей работе, является «безопасность». Её содержание задаёт вектор развития методологии деятельности по обеспечению безопасности, является ключом к решению практических задач. Сегодня в специальной литературе можно обнаружить десятки подходов к определению безопасности и связанных с ней основных понятий: безопасность, экономическая безопасность, угроза, риск, интерес, ущерб, источник угрозы, субъект угрозы, объект угрозы. Различные модификации наиболее распространённых формулировок исчисляются сотнями.

На бытовом уровне смысл понятия «безопасность» кажется банально очевидным. Однако, когда потребность в нём возникает для решения конкретных методологических или прикладных профессиональных задач, оказывается, что не всё так просто.

Неочевидность ответа на вопрос: «Что означает «безопасность?», - становится наглядной при рассмотрении, по крайней мере, следующих типовых определений, предлагаемых в специальной литературе.

Безопасность – это состояние объекта в системе его связей с точки зрения способности к выживанию и развитию в условиях внутренних и внешних угроз, а также действия непредсказуемых и труднопрогнозируемых факторов [25].

Безопасность – такое состояние субъекта, которое означает, что вероятность нежелательного изменения каких-нибудь качеств субъекта, внешней среды невелика (меньше определённого предела) [11].

Безопасность предприятия – это такое состояние его правовых экономических и производственных отношений, а также материальных, интеллектуальных и информационных ресурсов, которое выражает способность предприятия к стабильному функционированию [12].

Безопасность – это защита (процесс, действие) от опасностей на системном уровне [40].

Безопасность – отсутствие опасности, т. е. ситуация, при которой для кого-нибудь или чего-нибудь не существует угрозы со стороны кого- или чего-либо [42].

Безопасность есть невозможность нанесения вреда кому-нибудь или чему-нибудь вследствие проявления угроз, т. е. их защищённость от угроз [43].

Безопасность есть условия существования субъекта, контролируемые им [44].

Безопасность есть условия, в которых субъекты, как минимум, сохраняют и воспроизводят свои ценности [44].

В работе [45] выделены 4 группы подходов к определению экономической безопасности через:

- условия, обеспечивающие устойчивость;
- состояние, обеспечивающее интересы;
- независимость, обеспечивающую эффективное удовлетворение потребностей;
- комбинацию существующих подходов.

Не трудно заметить, что большинство определений безопасности учитывает системность и объективную широту диапазона направлений соответствующей деятельности, однако позволяет на практике сжимать предмет попечения о безопасности, рассматриваемая его как относительно самостоятельную задачу управления хозяйствующим субъектом.

Подобно понятию «безопасность» в среде специалистов нет единства в трактовке понятия «экономическая безопасность» и соответственно в понимании содержания деятельности по её обеспечению.

На национальном уровне Абалкин Л.И. подразумевал экономическую безопасность как «совокупность условий и факторов, обеспечивающих независимость национальной экономики, её стабильность и устойчивость, способность к постоянному обновлению и совершенствованию» [46]. Сенчагов В.К. определяет экономическую безопасность как «состояние экономики и институтов власти, при котором обеспечиваются гарантированная защита национальных интересов, социально направленное развитие страны в целом, достаточный оборонный потенциал даже при наиболее неблагоприятных условиях развития внутренних и внешних процессов» [47]. Тамбовцев В.Л. под экономической безопасностью какой-либо системы

полагает «совокупность свойств её производственной подсистемы, обеспечивающую возможность достижения целей всей системы» [48].

Авторы работы [14] определяют экономическую безопасность на уровне хозяйствующего субъекта как «состояние предприятия, характеризуемое его способностью нормально функционировать для достижения своих целей при существующих внешних условиях и их изменении в определённых пределах». При этом под нормальным функционированием они понимают «такое функционирование предприятия, которое в существующих внешних условиях обеспечивает достижение предприятием поставленных целей оптимальным образом или достаточно близким к нему». Следует отметить: в тех случаях, когда параметры управления и их последствия не поддаются строгому аналитическому описанию, а задача оптимального управления не сводится к математическим задачам оптимального управления или математического программирования (например, задача структурной перестройки), доказать, что лучший из рассмотренных вариантов решений является оптимальным невозможно, поскольку оптимальный вариант может находиться среди оставшихся «за бортом» рассмотрения, включая непридуманные, несоставленные, неувиденные, незамеченные. Это приводит к дискурсивной и методологической дискредитации категории «экономическая безопасность» в формулировке, приведённой в этом абзаце.

Экономическая безопасность предприятия – это наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры предприятия его стратегическим целям и задачам [13].

Это определение сужает смысл определяемой категории. Наличие конкурентных преимуществ, чем бы они ни были обусловлены, не гарантирует экономическую безопасность, а лишь свидетельствует о возможностях, при чём только в условиях рынка. Кроме того, соответствие потенциалов целям не обязательно однозначно определяет конкурентные преимущества.

Безопасность экономической системы характеризуется как способность системы к стабильному функционированию (к выживанию),

т. е. сохранение структурной устойчивости, но только в выражениях не процесса, а состояния как результата поведения системы [49].

Во-первых, безопасность не является способностью системы, т. к. она зависит не только от неё, но и от состояния и влияния внешней среды. Любая «хрупкая» система будет в безопасности, если нет угроз. К способностям системы относится то, что присуще ей имманентно, например, устойчивость, о чём будет сказано чуть ниже. Во-вторых, требуется дополнительно определять, что означает «стабильное функционирование» и почему оно тождественно «выживанию» и «сохранению структурной устойчивости». Хозяйственный субъект, например, может быть подвергнут структурной реорганизации, но при этом не утратить доли рынка, прибыль, заказчиков, потребителей, партнёров. Более того, структурная реорганизация зачастую проводится как раз для обеспечения благополучия хозяйственной деятельности в изменившихся условиях.

Рассмотренные подходы к определению безопасности и экономической безопасности отражают смысловой хаос, который царит в понятийной плоскости проблематики безопасности предприятия, равно как и в целом в проблематике безопасности социальных систем. Одна из причин этого – неудачные попытки перенесения в гуманитарную сферу понятий стабильность, устойчивость, надёжность, заимствованных из математики, физики, инженерии, где они имеют чёткий однозначный смысл и закреплённые оригинальные онтологические роли.

Ни в приведённых, ни в других из известных определений «безопасности» не обнаруживаются в достаточной мере достоинства однозначности, самодостаточности, неизбыточности и операциональности на уровне решения практических задач обеспечения безопасности, в частности безопасности хозяйствующего субъекта.

Важнейшее значение в теории и практике принятия технико-технологических, социально-экономических, политических решений на всех уровнях управления организационными и техническими системами имеет также категория «риск». В то же время, как и другие рассмотренные категории в проблематике безопасности, риск не имеет однозначной трактовки.

Методологические и онтологические подходы к определению риска отражены в работе [50]. Приводится около двух десятков формулировок понятия «риск» отечественных и зарубежных авторов. Практически все эти формулировки отягощены недостатками определений, на которые было указано выше. Суть же их сводится к тому, что риск рассматривается либо как характеристика неопределённости, фактически вероятность, либо как возможный ущерб (недополученная прибыль) с учётом неопределённости его наступления. Это является отражением двух взглядов на категорию «риск». Риск – это последствия деятельности или действий. Риск – сама деятельность (совершение действий) в условиях неопределённости.

Последнее имеет прямое отношение к значению слова «риск» в общеупотребимом языке и соответствует выражениям «рискую», «иду на риск», т. е. сознательно (намеренно) действую в условиях неизвестности (сомнительности) последствий. Подобный подход к словоупотреблению имеет значение в ненаучных и ненормативных текстах, когда требуется подчеркнуть неопределённость ситуации на эмоциональном уровне. Однако при формировании методологии и онтологии проблематики, тем более ориентированной на создание методического инструментария и регламентов практической деятельности, это недопустимо. Во-первых, разные категории – деятельность и последствия – должны иметь различные обозначения. Во-вторых, при таком понимании риска, родовой категорией для него является «деятельность». Это девальвирует роль и значение «риска». С одной стороны, в реальности практически все ситуации принятия решения и деятельности в той или иной степени неопределённы (во всяком случае на модельном уровне любую детерминированность можно описать с помощью параметров неопределённости, положив их равным 1 или 0). Это означает, что риск как деятельность просто сливается с деятельностью. С другой – нецелесообразно для категории «деятельность» вводить подкатегорию «риск», когда можно ввести соответствующие атрибутивные характеристики.

Иная причина разночтений риска заключается в том, что некоторые исследователи добавляют в риск, как ущерб, ещё и возможности, которые открываются в условиях неопределённости. Такое расширение представляется неконструктивным. Можно

допустить, что в результате деятельности возникнет неожиданный полезный эффект, но оперирование им принципиально отличается от содержания деятельности по предупреждению или сокращению ущерба. Ссылка на поговорку «риск – дело благородное», которая якобы отражает отсутствие в массовом сознании жёсткой корреляции риска с ущербом и потерями [50], ошибочна. Поговорка служит стимулятором решимости деятеля (возможно, самого себя) при принятии решений как раз потому, что последствия этого решения могут сопровождать потери и страдания. Идти на лишения ради какой-либо позитивной цели – дело, действительно, благородное.

Понятийная неразбериха усугубляется тем, что основные понятия безопасность, угроза, риск не имеют достаточной нормативной определённости. Так, Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ в отличие от предыдущего одноимённого Закона Российской Федерации от 5 марта 1992 г. № 2446-1, не определяет фундаментальные, ключевые категории: безопасность, национальная безопасность, угроза, риск.

Согласно ГОСТ 51898-2002 «Аспекты безопасности. Правила включения в стандарты», «Безопасность – это отсутствие недопустимого риска». Это определение, как минимум, требует конкретизировать термин «недопустимый риск».

Единственными нормативными основаниями для определения риска являются Федеральный закон Российской Федерации «О техническом регулировании» от 24.12.2002 г. № 184-ФЗ (с дополнениями и изменениями), ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты» и ГОСТ Р 51897-2011/Руководство ИСО 73:2009 «Национальный стандарт Российской Федерации. Менеджмент риска. Термины и определения. Risk management. Terms and Definitions». В законе риск определяется как «вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учётом тяжести этого вреда». Согласно первому из указанных ГОСТов: «Риск – это сочетание вероятности нанесения ущерба и тяжести этого ущерба». Другой ГОСТ является аутентичным переводом международного стандарта ISO Guide 73:2009 «Risk

management – Vocabulary – Guidelines for use in standards» и вносит путаницу в нормативное понимание риска. Он определяет риск как следствие влияния неопределённости на достижение поставленных целей.

Смысловая выхолощенность последней формулировки, видимо, вынудила её авторов сопроводить свою дефиницию пятью примечаниями, в которых, в частности, указано, что отклонения могут быть *позитивными и/или негативными*, что риск *часто* представляют в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности и др. А как риск представляют *редко*? Подобное определение риска затрудняет его практическое использование до невозможности, поскольку оставляет произвол в трактовке смысла этого понятия, создавая неопределённость смыслов, барьеры для профессиональной коммуникации по проблемам обеспечения безопасности.

Формулировка категории «безопасность» должна точно отражать её содержание, позволять отграничивать её от других категорий проблемной области, адекватно представлять масштаб и специфику обозначаемой им предметной области, вводить критерии отличения безопасности от небезопасности и, следовательно, задавать логику методологии её исследования и использования. Аналогичные требования предъявляются и к определениям других категорий, в частности, для определения «риска» следует не прибегать к усложнениям, а отразить первичный оригинальный смысл, полезный для дальнейшего использования рассматриваемой категории в построении методологии, нормативной регуляции деятельности по управлению хозяйствующим субъектом.

В современных же исследованиях отмечается тенденция «нагрузить» понятие всевозможными сопряжёнными смыслами и прикладными интерпретациями. Это приводит к избыточности и неопределённости понятий, их набуханию атрибутивным, второстепенным и, главное, не своим содержанием. В результате смыслы понятий пересекаются, они становятся плохо различимыми, их методологическая, онтологическая и дискурсивная ценность падает. Текстуальная избыточность свидетельствует о необретении в формулировке первичного оригинального смысла.

Прежде чем дать определения основным рассматриваемым категориям необходимо рассмотреть методологические основания для определения смысла категории «безопасность», её место и роль в ментальных и организационных моделях управления предприятием.

Любой хозяйствующий субъект является организационной системой, под которой понимается «объединение людей, совместно реализующих некоторую программу или цель и действующих на основе определённых процедур и правил» [51]. Поскольку организационная система является творением людей и служит средством достижения их целей, то справедливо предположить, что она представляет для них ценность, они заинтересованы в её существовании: в том, чтобы она сохранялась, предоставляла возможности для достижения целей. Цели могут меняться, соответственно, могут меняться и факторы их достижения и, следовательно, требования к организационной системе, её ресурсам, процедурам и правилам функционирования. Таким образом, существование организационной системы предполагает наличное бытиё и его качественную определённость, которая не статична. Под качественной определённостью существования здесь понимается объём тех возможностей, которые организационная система предоставляет составляющим её людям для достижения их целей.

При любой формулировке понятия «безопасность» подразумевается отсутствие возможности нанести объекту рассмотрения (защиты, охраны) ущерб, помешать его функционированию для достижения намеченных целей. При нанесении ущерба, наличии помех достижению цели качество существования снижается. Деградация существования системы ниже некоторого уровня может привести к её ликвидации.

Таким образом, ценность «существование» реализуется через обеспечение *безопасного* существования. Безопасное существование – бытиё при субъективно самой лучшей качественной определённости, т. е. при максимальном объёме возможностей. Объём возможностей – величина не абсолютная, а относительная. Он измеряется относительно уровня достижения целей, поставленных людьми, образующими организационную систему.

Парадигма существования предусматривает, что существование является главной ценностью любых живых и социально-культурных

систем. Стремление к существованию в этой интерпретации в обозримой перспективе выступает системообразующим фактором для системы деятельности указанных систем [52]. Смыслом и содержанием существования для человека является сбережение ценностей и удовлетворение потребностей. Ценности и потребности формируют интересы, которые являются их отражением и формируют направления и содержание деятельности, конкретизируясь в целях и задачах.

Проблема смысла и содержания существования субъектов различного уровня: от живых субъектов до крупных социальных систем в отношении проблематики безопасности рассмотрена в [53]. Логика перехода от частных интересов людей, составляющих организационную систему – предприятие - к интересам предприятия, как субъекта, а также соотношение этих интересов кратко рассмотрены в разделе 1.2. Здесь важно отметить, что в какой мере в интересах предприятия опосредованы интересы, ассоциированных с ним групп и персон, в такой мере оно является объектом, существование которого интересует эти группы и персоны. Безопасность системы (предприятия) всегда субъективно окрашена, т. е. изучается, оценивается, обеспечивается в интересах некоторого субъекта [54].

Внешняя среда и внутренние механизмы изменения интересов хозяйствующего субъекта оказывают на него постоянные воздействия. Воздействия первой, как правило, направлены на снижение качества его существования или препятствуют возрастанию этого качества. Вторые приводят к рассогласованию сущего (располагаемого) с должным (желаемым). При этом «дистанцию» между желаемым и располагаемым также можно считать субъективно воспринимаемым снижением качества существования. Эту разницу субъект воспринимает как нарушение условий благоденствия – безопасного существования.

Стремление к новому уровню качества существования, воспрепятствовать деградации и разрушению (ликвидации) приводит к усложнению внутренней структуры систем и расширению спектра их реакций на внешние раздражители, т. е. выступают движителем развития систем субъектного типа – хозяйствующего субъекта в данном контексте. При этом развитие должно осуществляться в упреждающем режиме на основе прогноза изменений среды.

В работах, посвящённых проблематике безопасности на уровне системного анализа и в связи со стратегическим управлением, рассматривается отношение между безопасностью и развитием. При этом безопасность рассматривается, как условие развития, а цели развития оказываются фигурами умолчания. В этом случае развитие приобретает самостоятельную, но, по сути, фиктивную ценность, поскольку обессмысливается, приводит к увеличению неопределённости [1], истощению ресурсов.

В работе [40] отмечается диалектическое противоречие между безопасностью и развитием и предлагается решать его (как было отмечено во введении к настоящей монографии) путём подчинения «функции безопасности» выполнению «функции развития».

Вопрос об уравнивании «в правах» безопасности и развития на концептуальном уровне поставлен в работах [42, 55], где устойчивое развитие определяется в том числе как обеспечение безопасности через развитие и развитие через обеспечение безопасности.

В рамках парадигмы существования развитие мотивируется стремлением обеспечить безопасное существование и является средством этого обеспечения, а диалектическое противоречие существует не между развитием и безопасностью, а между обеспечением безопасного существования в различной временной перспективе – сегодня, завтра, …, в будущем.

В работе [3] рассматривается отношение безопасности предприятия и эффективности его деятельности. Эти категории признаются дополняющими друг друга. При этом в качестве основных угроз указаны три:

- угроза существованию или суверенности предприятия;
- угроза целостности предприятия;
- угроза рыночной позиции предприятия.

Отмечено, что первые две непосредственно связаны с безопасностью, а последняя соотносится с конкурентной борьбой.

Важно отметить, что конкурентная борьба не сводится к ограничению рыночной позиции конкурента, снижению его эффективности. Формы и результаты этой борьбы определяются условиями конкуренции – иногда до полного устранения конкурента.

Приведённые перечень угроз и комментарий к нему подтверждают противоестественность механистичного разделения безопасности и эффективности деятельности. В парадигме существования эффективность отражает отношение степени достижения безопасного существования, т. е. степени удовлетворения интересов предприятия, к объёму затраченных для этого ресурсов. В то же время в методических, исследовательских и практических целях целесообразно выделять угрозы, реализация которых приводит к катастрофическим последствиям, т. е. не к снижению качества существования, а к прекращению существования (кончины, «нулевой» эффективности, банкротству). Противодействие таким угрозам выходит на первый план организации деятельности предприятия.

Авторы работы [49] в категорию «безопасность» вкладывают «смысл сохранения гомеостаза внешней и внутренней систем как системообразующий фактор». В связи с этим следует обратить внимание, что последний должен образовывать систему, определять основу её морфологии, функциональности и, в конечном итоге, эмерджентность. Системообразующий фактор имманентно принадлежит системе, входит в её конструкцию, является её внутренним фактором. Безопасность же есть определённое состояние существования системы и системообразующим фактором являться не может. Таким образом, системообразующий фактор служит для достижения безопасности субъекта, но не является ею. При этом важно не путать систему и её деятельность и отличать системообразующий *процесс* для *системы – деятельности* от самой *системы – субъекта*. Системообразующим фактором деятельности, как было отмечено выше, является стремление к безопасному существованию.

В рамках парадигмы существования важно определить «безопасность» таким образом, чтобы задать необходимые и достаточные рамки для создания организационно-методического и информационного обеспечения системы управления хозяйствующим субъектом в целях достижения и постоянного упреждающего достигания его безопасного существования. Базовое (родовое) определение безопасности должно быть инвариантно для любых организационных систем, условий хозяйствования и другой деятельности, масштаба и строгости решения задач управления

системой. Специфика появляется при рассмотрении интересов, угроз, рисков, особенностей существования конкретной системы.

В соответствии с рекомендацией создателя силлогистики Аристотеля определение должно описывать определяемое понятие через другие, уже известные, а в качестве исходных следует принять неопределяемые понятия [56]. Неопределяемыми здесь служат понятия, ненаделённые специфическим смыслом для рассмотрения проблем безопасности. Смысл слов, используемых для их обозначения, тождественен смыслу этих слов в общеупотребительном языке или соответствующих тематических словарях. Целесообразно начать с определения понятий, строящихся только на неопределяемых понятиях, и последовательно развернуть всю понятийную систему, наполняя каждый её компонент содержанием необходимым для формирования методологических подходов к обеспечению безопасного существования хозяйствующего субъекта.

Вначале – ресурсы. Эта категория какой-либо специальной идентифицирующей её формулировки не требует. Её содержание вполне раскрывается перечислением основных составляющих компонент. В отношении хозяйствующего субъекта это:

- основные и оборотные производственные фонды;
- товарно-материальные ценности и финансовые ресурсы;
- непроизводственные фонды;
- кадровый потенциал: наличие, квалификация;
- качество коллектива: идентификация интересов работников с интересами предприятия, атмосфера со-трудничества и творчества, дисциплина;
- информационные ресурсы, включая интеллектуальную собственность;
- внутренний организационный ресурс: бизнес-процессы и их регламентация, система мотивации, цели, миссия, этический кодекс, традиции предприятия и т. п.;
- гудвилл: клиентская база (долговременные договора и контракты), деловые связи, положительная репутация в обществе и государственных органах; «капитал влияния» для формирования локальной «макровласти» [4].

В ресурсы во многих случаях целесообразно включать партнёров и поставщиков, поскольку их благополучие прямо или косвенно влияет на благополучие предприятия. Осознание последнего приводит от конкуренции и выгадывания на короткой дистанции к созданию стратегических альянсов, кооперации ко взаимному благу на протяжении мыслимых будущих периодов.

В современных концепциях развития бизнеса на основе управления знаниями («знаниевый менеджмент», «knowledge management») последние четыре из указанных видов ресурса объединяются в «интеллектуальный капитал». При этом в настоящее время стоимость «интеллектуального капитала» в среднем в 5–10 раз превосходит стоимость физических и финансовых активов («физического капитала»), а для наукоёмких предприятий – в 15 раз. В перспективе это отношение будет расти.

При такой интерпретации ресурсов, очевидно, что автор придерживается точки зрения на ресурсы, когда в их состав включаются способности предприятия, как неявные знания и умения.

Ресурсы предприятия совместно с механизмами их использования образуют потенциал обеспечения существования (далее – ПОС).

Интересы хозяйствующего субъекта – отражают потребности и ценности хозяйствующего субъекта как организационной социально-экономической системы.

При этом под ценностью понимается любое материальное или идеальное явление, имеющее значение для человека и (или) общества, ради которого тот и(или) то прилагает усилия [57], а потребностью – надобность в чём-либо необходимом для поддержания существования субъекта [58].

Подробней вопрос об интересах хозяйствующего субъекта рассмотрен в следующем разделе.

Цели и задачи хозяйствующего субъекта – цели и задачи, поставленные собственниками и органами управления перед хозяйствующим субъектом на заданный период, закреплённые в концептуальных, программных, плановых, распорядительных документах. Цели и задачи конкретизируют, опредмечивают интересы.

Целевое расходование ресурсов хозяйствующего субъекта – расходование ресурсов хозяйствующего субъекта на обеспечение его интересов, достижение целей и решение задач.

Ущерб хозяйствующему субъекту – сокращение степени удовлетворения интересов хозяйствующего субъекта.

Безопасность хозяйствующего субъекта (безопасное существование) – отношения в системе хозяйствующий субъект - среда, при которых вероятность нанесения ему значимого ущерба на заданном интервале времени пренебрежимо мала.

В качестве заданных интервалов времени целесообразно рассматривать периоды отчётности исполнительных органов управления перед коллегиальными (акционерами), этапы планирования, длительность жизненного цикла сложной продукции или контракта, длительность основного производственного цикла, период использования базовой технологии и т. п.

В этой дефиниции учитывается неопределённость состояния и воздействия среды, а также относительность и требуемая (на качественном уровне) точность измерения величины ущерба.

Обеспечение безопасности хозяйствующего субъекта (безопасного существования предприятия) – деятельность, направленная на предотвращение ущерба этому хозяйствующему субъекту.

Необходимо отметить, что достижение абсолютной безопасности практически невозможно. Полное удовлетворение своим существованием возможно лишь кратковременно. В силу разных причин, в том числе изменения окружающей среды и эволюции самой организационной системы, оно всё время ускользает и ставит новые задачи развития (изменения качественной определённости) существования. Как отмечал Моисеев Н.Н.: «Риск и опасность в развитии цивилизации были, есть и будут. И нам придётся приучить себя к мысли о необходимости жить под этим бременем. Но это означает лишь одно: Человечеству необходимо научиться предельно снижать этот риск и опасность».

Угрозы безопасности хозяйствующего субъекта – возможности, реализация которых приводит к нанесению ущерба хозяйствующему субъекту.

Здесь важно отличать вкладываемый в эту формулировку смысл от понимания угрозы на бытовом уровне как выраженное намерение причинить зло.

Введённые дефиниции позволяют методологически корректно сформировать и обосновать подход к оценке и обеспечению безопасности на основе тезиса, что «безопасность достигается путём установления баланса между существующей угрозой и способностью противостоять ей» [59][4].

Риск – характеристика угрозы безопасности хозяйствующего субъекта, отражающая соответствующую ей величину ущерба хозяйствующему субъекту с учётом неопределённости распределения этой величины в области ожидаемых (прогнозируемых) значений.

Данное определение построено на идее, использованной в определениях риска по вышеуказанному закону и ГОСТу Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты», поскольку она конструктивна для определения риска в рамках парадигмы существования. Его преимуществом является дополнительное операциональное качество, позволяющее онтологически связать категорию «риск» с категориями «угроза», «ущерб» и наметить методологию измерения риска с точки зрения безопасного существования.

Рисковое событие – факт реализации угрозы.

Источник угрозы – субъект или объект физического мира, явление или процесс, обладающий возможностью нанести ущерб.

Объект угрозы – организационные структуры, физические и юридические лица, учётные единицы материальных и нематериальных активов хозяйствующего субъекта (технические и инфраструктурные объекты, объекты недвижимости, товарно-материальные ценности, наличные деньги, ценные бумаги, документированные обязательства, информационные ресурсы и т. п.), на которые воздействует источник угрозы.

Предмет угрозы – ресурс хозяйствующего субъекта, расходуемый (утрачиваемый) в результате рискового события.

---

[4] Источник ссылается на: Nelson D. Melt the tanks, bring the boys home. The cost of demilitarizing security in Soviet and Easters Europe. Цит. по: Актуальные проблемы Европы: экономика, политика, идеология. Вып. 4 // Реферативный сб. М.: РАН ИНИОН, 1991. С. 19.

Аналогично.

Объект защиты – организационные структуры, физические и юридические лица, учётные единицы материальных и нематериальных активов хозяйствующего субъекта (технические и инфраструктурные объекты, объекты недвижимости, товарно-материальные ценности, наличные деньги, ценные бумаги, документированные обязательства, информационные ресурсы и т. п.), на которые воздействует или может воздействовать источник угрозы.

Предмет защиты – ресурс предприятия, который может расходоваться (утрачиваться) в результате рискового события.

Определение безопасности, угрозы и риска через ущерб, а ущерба через ресурс позволяет построить полную, неизбыточную, непротиворечивую онтологию проблематики безопасного существования.

Укрупнённая схема этой онтологии представлена на рисунке 1 [60].

Для выявления источников угроз целесообразно также ввести понятие «вызов». Под вызовами понимаются новые обстоятельства, факты, характер и результат влияния которых на безопасное существование предприятия неизвестны.

В заключение важно также разобраться с категорией «устойчивость».

В соответствии с общей теорией систем под устойчивостью системы следует понимать её способность сохранять минимально необходимый потенциал для применения по прямому назначению после некоторым образом описанных внешних воздействий. Для этого система должна сохранить эмерджентность и внутренние ресурсы для её воплощения. Проявляется это в сохранении целостности (системообразующих факторов) и, хотя бы минимально необходимой, производительности. Для динамических систем производительность – мощность генерации выходных продуктов, сигналов, выполнения работы с учётом надёжности, в том числе за счёт резервирования. Для статических – прочность. Устойчивая система должна остаться инвариантной самой себе после воздействий [61].

Воздействие может быть продолжительным. В этом случае в целях моделирования его можно представить, как последовательность сколь угодно малых по продолжительности актов.

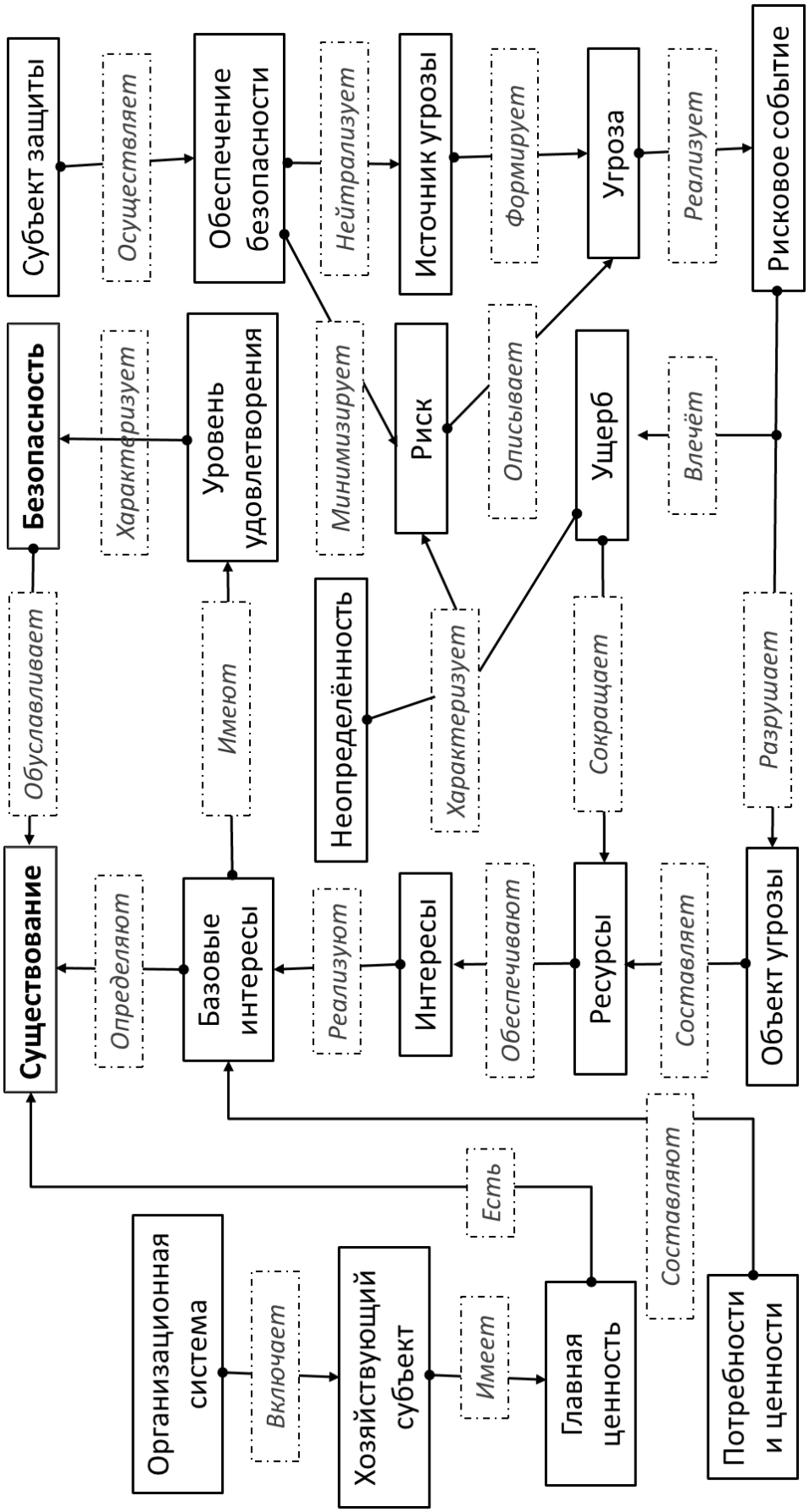

Рисунок 1 – Укрупнённая схема онтологии проблематики безопасного существования предприятия [60]

Абсолютной устойчивости, как и безопасности, не бывает, поэтому она рассматривается на некоторой области определения сформированного набора возмущающих воздействий. Спектр возмущающих воздействий также ограничен, поскольку невозможно определить способность системы противостоять неизвестным воздействиям. Он составляется в зависимости от целесообразности рассмотрения, осведомлённости исследователя об окружающей систему среде, его проницательности и фантазии.

В отличие от безопасности устойчивость – это внутреннее свойство системы, которое непосредственно не определяется внешней средой. Безопасность зависит не только от способности противостоять угрозам, но и наличия и реализации угроз. В отношении же устойчивости внешняя среда может лишь мотивировать систему к её увеличению, генерируя различные вредные воздействия. Недостаточная устойчивость при наличии угроз приводит к снижению уровня безопасности.

Исходя из изложенного предлагается определять устойчивость предприятия, как состояние его ПОС, характеризующееся возможностью обеспечивать удовлетворение интересов предприятия в условиях заданных изменений и(или) воздействий среды, в том числе макроэкономических показателей, конъюнктуры целевых секторов рынка, параметров региональных социально-экономических систем.

В приведённую дефиницию, в отличие от многих встречающихся в литературе вариантов, не включена категория «развитие», поскольку отношение устойчивость–развитие полностью определяется выше обоснованным отношением безопасность–развитие.

Реализация системы управления хозяйствующим субъектом на основе парадигмы существования позволит:

- разработать и внедрить целевой, системный критерий управления – безопасное существование в сколь угодно продолжительной перспективе;

- выстроить единую иерархическую систему целей и задач;

- системно на операциональном уровне объединить единым механизмом известные подходы к управлению хозяйствующим субъектом и реализацией проектов, в частности «пять сил Портера», SWOP-анализ, STEP-анализ, риск-менеджмент и другие.

1.2. Интересы предприятия

В предлагаемой парадигме исследования безопасности предприятия удовлетворение интересов играет роль целевой функции деятельности по обеспечению безопасного существования, а степень этого удовлетворения служит оценкой безопасности (что будет подробно рассмотрено ниже), в связи с этим необходимо рассмотреть категорию «интерес» несколько глубже, чем это сделано выше.

Интерес понятие многогранное и подходы к наделению его смыслом и содержанием разнятся. В толковых словарях в качестве наиболее распространённого (первого) смысла указано: корысть, выгода, прибыль (например, Даль, Ожегов), а также внимание к чему-нибудь или кому-нибудь важному, полезному (например, Ушаков, Ефремова). В социологии интерес часто определяется как реальная причина действий, лежащая в основе непосредственных побуждений, мотивов, а в психологии – как отношение личности к предмету как к чему-то для нее ценному, привлекательному.

В работе [62] отмечается, что в экономической литературе нет единого взгляда на трактовку взаимосвязи потребностей и интересов и подробно анализируются подходы к определению понятия «экономический интерес». Так, выделяются следующие подходы:

- интерес – выражение целевой функции потребностей;
- интерес – осознанная потребность;
- интерес служит опосредующим звеном между потребностями субъектов и их производственной и иной общественной практикой, при этом потребности составляют материальную основу экономических интересов.

Ряд авторов придерживается взглядов на экономический интерес как субъективную категорию, поскольку прежде чем стать мотивами действий, они должны быть осознаны субъектом. Другие полагают объективную природу экономических интересов, выводимую из объективности экономических законов.

Представляется, что более практически значимым является дуалистический подход, рассматривающий в диалектическом единстве субъективную и объективную стороны интереса, в том числе и экономического. С точки зрения общих закономерностей существования

и развития самоорганизующихся, живых, в том числе организационных систем, можно выделить объективные потребности, ценности, цели деятельности, удовлетворение и достижение которых на всех уровнях иерархии жизни позволяет обеспечить благополучие всей системы. С другой стороны, поведение живых систем не столь строго подчиняется объективным законам как неживые физико-химические системы и принципиально новое качество в их поведение вносит фактор свободной воли человека, субъективности его ценностей и предпочтений. Этот фактор не позволяет полагать, что интересы и, следовательно, деятельность организационных систем и их элементов (людей и коллективов) будет обязательно находиться в объективной гармонии с научно обоснованными целесообразностями. Для соблюдения строгости рассуждений следует учитывать полную группу возможных событий, поэтому в числе интересов конкретного человека, в частности, владельца или руководителя предприятия, может быть деструктивный интерес по отношению к предприятию – его ликвидация, банкротство. В этой связи всегда необходимо учитывать субъектные основания методологии оценки безопасности [54].

В дальнейшем в настоящей работе принято, что интересы определяют содержание того, что нужно достичь для сбережения ценностей и удовлетворения потребностей, и принимают форму, или воплощаются в целях и задачах конкретной деятельности.

В работе [3] представлена точка зрения, что предприятие в общем случае может иметь неперсонифицированные интересы. Надо полагать, что такие интересы должны иметь объективный характер. Однако в этом случае не ясно: каким образом формируется их представление в качестве предмета деятельности, как зарождается соответствующая мотивация деятельности конкретных лиц. Напротив, принцип методологического индивидуализма предполагает личный интерес в качестве первичной формы экономического интереса. «Это означает, что научная постановка вопроса об интересах субъектов различного уровня (организации или группы организаций) осуществима лишь при возможности (пусть даже и чисто теоретической) сведения их к совокупности частных интересов. В противном случае эти категории приобретают в известной степени «мифический» характер» [4]. Применение этого принципа также вызывает возражения.

В одной из своих ипостасей предприятие является средством (иногда единственным) обеспечения существования своих собственников, средством удовлетворения их интересов. Интересы предприятия с точки зрения рафинированного частника (теоретически идеального в качестве социально специфической роли) составляют:

- дивидендные выплаты в соответствии с заданной общим собранием акционеров динамикой; при этом в целях развития или спасения производства акционеры могут временно отказаться от дивидендов;

- поддержание высокой репутации предприятия как производителя общественно полезных товаров и услуг (например, наукоёмкой продукции) в деловых кругах, в том числе международных, в обществе, в государственных и муниципальных органах России.

В первом случае проявляются материальные потребности собственника и интерпретация его социальной значимости [58] через ценность «богатство». Во втором – потребность в приобретении социальной значимости в качестве полезного для общества деятеля.

Первый интерес, как правило, является приоритетным, поскольку определяется логикой бизнеса [63]. Второй, если присутствует, то сопутствует первому. В отдельных случаях он может иметь и самостоятельное значение, что определяется мировоззрением и модусами социальной значимости собственников. Этот интерес нередко проявлялся в дореволюционном капитализме в России, что соответствовало её культурной традиции. Яркими примерами тому в отечественной истории служат предприниматель С.Т. Морозов, нижнетагильские купцы Демидовы, предприниматель-меценат П.М. Третьяков.

Во второй ипостаси предприятие служит средой, в которой его руководители и работники проводят большую часть своего времени на определённом этапе жизни. Это время препровождения содержательно наполнено деятельностью, которая по ожиданиям её участников должна каким-то образом удовлетворять их интересы. Для работников эти интересы сводятся, прежде всего, к потребностям в материальном достатке и приобретению социальной значимости через профессиональную самореализацию. Социальная значимость может также получать дополнительную подпитку за счёт осознания

приобщения к общественно полезной деятельности – созданию важных общественных благ, например, выпуск наукоёмкой продукции для общественных нужд (сложная космическая, морская или медицинская техника, вооружение, производство экологически чистого продовольствия). Удовлетворение материальных потребностей взаимосвязано с профессиональной самореализацией, поскольку специалист может стремиться к профессиональному росту, предполагая, что успехи на этом поприще приведут к росту личных доходов в будущем. Правильное сочетание внешней и внутренней мотивации работников способствует или препятствует инновационным процессам, что прямо отражается на благополучии предприятия в ближней и дальней перспективе.

На закате XX столетия предприятие «Уралвагонзавод» было спасено во многом благодаря сплочению трудового коллектива вокруг руководства в лице генерального директора и генерального конструктора для реализации смысла – сохранение производства современных танков. Примечательно, что на вопрос журналиста: что для вас значит завод, – рабочие и инженеры отвечали: «моя жизнь», «всё», «не знаю» и т. п. Последний ответ по сути тождественен ответу «всё», поскольку смысл завода не вмещается в прагматичные ценности: работа, зарплата, карьера, самореализация и т. п., а выразить в интервью более высокие смыслы человеку, неискушённому в философском дискурсе, затруднительно.

Государственные предприятия или предприятия с долей, находящейся в государственной собственности, в числе приоритетных интересов должны рассматривать национальные интересы, т. е. интересы всего общества, через выполнение государственных заказов, реализацию социально-экономических проектов, в том числе в регионах размещения производственного потенциала. Аналогично, дополняются интересы муниципальных и тому подобных предприятий, но в масштабе соответствующей административно-территориальной единицы. Смысл существования предприятия, как хозяйствующего субъекта, с точки зрения государства заключается в его полезности для обеспечения национальной безопасности, т. е. безопасного существования страны. Чтобы быть полезным предприятие должно производить общественно полезные, прежде всего необходимые, продукты позволять пополнять

консолидированный государственный бюджет, обеспечивать некоторый уровень благосостояния и в ряде случаев поступление валютной выручки от экспорта для формирования валютных резервов государства и экономики в целом для участия российских экономических агентов в международных финансовых и экономических сношениях. В связи с этим в числе государственных интересов в отношении предприятия целесообразно рассматривать следующие:

- выполнение государственных заданий;
- получение прибыли по коммерческим проектам;
- получение налоговых платежей;
- поступление экспортной валютной выручки (в некоторых случаях);
- поддержание социально-экономического уровня жизнедеятельности работников;
- повышение рентабельности производства и рентабельности продаж.

Эти интересы являются частично противоречивыми и взаимообусловленными. Удовлетворение некоторых их них может быть отложено с целью извлечения пользы в стратегической перспективе.

Часто в число интересов государства применительно к предприятиям, особенно высокотехнологичным, причисляют повышение конкурентоспособности, производительности труда, уровня используемых технологий и т. п. Однако эти аспекты являются обеспечивающими для достижения указанных выше интересов предприятия. Они представлены в потенциале предприятия. Действительно, технологии нужны не сами по себе, а для экономически эффективного выпуска продукции. Для этой же цели осуществляется повышение производительности труда. При этом следует заметить, что на уровне общества в целом рост производительности труда должен уравновешиваться созданием рабочих мест для недопущения безработицы.

Следует также учитывать современное явление бюрократизации предпринимательства и управления крупными хозяйствующими структурами, когда управленцы верхнего уровня иерархии фактически перехватывают у собственников возможности распоряжаться доходами предприятий и определять его стратегию, становясь зарплатной

буржуазией или технократами [63, 64], следуя тенденции «управленческого империализма» [4]. Особенно остро эта проблема стоит, когда нет ярко выраженного мажоритария. При некорректно поставленных учредителями (акционерами) задачах и слабом (зачастую неквалифицированном) контроле создаются предпосылки к предпочтению управленцами решения тактических задач – быстрому повышению прибыли и улучшению бухгалтерского баланса [65] в ущерб стратегическому управлению. Это характерно также и для государственных, и муниципальных предприятий, где интересы всего общества или локального социума олицетворяются конкретными должностными лицами, прежде всего, руководителем предприятия, а также «государственными» («муниципальными») членами коллегиальных органов управления. Таким образом, российские предприятия оказываются охваченными эпидемией деградации содержания производственной деятельности, примитивизации промышленной структуры, подмены создания и производства высокотехнологичной наукоёмкой продукции операциями с недвижимостью, распродажей фондов, интеллектуальной собственности, спекуляциями на фондовых рынках и т. п. Нельзя не учитывать и так называемый конфликт интересов, заключающийся в прямом или косвенном коммерческом подкупе управленцев со стороны конкурентов (прежде всего ТНК, в случае крупного бизнеса) и выполнении их стратегий на банкротство и распродажу активов предприятия. Конфликт интересов может проявляться и в мошенничестве со стороны управленцев, «уводе бизнеса» и других неправовых и недобросовестных по отношению к собственникам действиях.

Поскольку предприятие объективно является элементом экономики, предназначенным для непосредственного производства общественно полезных продуктов (товаров и услуг), то с позиции общества интерес предприятия (смысл его существования) заключается в производстве, в поддержании производственных циклов сколь угодно долго. Разумеется, это возможно при обеспечении необходимых входных и выходных потоков. Если этот интерес не обеспечивается, то элемент-предприятие вступает в конфликт (не обязательно осознанный и не обязательно проявляющийся немедленно) с системой-общество. В

этом контексте справедлива постановка вопроса о разработке законодательной защиты предприятия, как субъекта, которая бы ограждала его от деструктивного проявления воли собственников или руководства [3]. Здесь предприятие рассматривается уже как элемент более общей социально-экономической системы, которая соблюдая свои интересы, беспокоится о сохранности и полезности своих элементов, в числе которых предприятие – непосредственный производитель товаров и(или) услуг.

Таким образом, частные (индивидуальные) интересы всех лиц и групп, ассоциированных с предприятием, взятые сами по себе являются в общем случае несовпадающими и часто противоречивыми. Они все не могут быть удовлетворены полностью. Их сумму (суперпозицию) нельзя, поэтому, рассматривать в качестве интересов предприятия, как целостной системы и субъекта деятельности (системных интересов). Хозяйствующий субъект, как система неизбежно накладывает ограничения на пространство возможностей каждого своего элемента в отдельности.

В соответствии с используемой в монографии парадигмой существования субъекту, в данном случае предприятию, имманентно присуща главная ценность – существование, содержательно наполненное реализаций интересов предприятия. Ценность существования – составляет объективную основу для определения системных интересов. Смысл интересов предприятия, как системной целостности, состоит в том, что они поднимаются над мотивами эгодеятельности отдельных лиц или их групп и направлены на обеспечение безопасного существования предприятия, что позволяет в достаточной степени удовлетворять интересы всех ассоциированных лиц (всех людей, объединившихся в рамках организационной системы для достижения своих целей).

Системные интересы становятся не «мифом», а реальностью через персонализацию, отражаясь в пространстве интересов индивидуумов. При этом хотя бы властвующая часть индивидуумов, ассоциированных с субъектом, должна осознавать системные интересы и включать их в пространство личных интересов в явном виде. Успех управления предприятием, реализации корпоративной стратегии определяется увеличением части ассоциированных индивидуумов, которая включает

системные интересы в состав личных. Вероятно, решаться эта задача может на уровне формирования общей системы ценностей на основе национальной культурной традиции, её инкорпорирования в корпоративную этику и выработки согласованной системы потребностей для удовлетворения взаимных ожиданий.

В зарубежной практике корпоративного управления применяется формулировка миссии предприятия и его ценности, в качестве правил ведения бизнеса. В России это также приобрело популярность, особенно, в крупных компаниях. Миссия, например, может звучать так: создание общественно-полезных продуктов, неуклонное повышение благосостоянии сотрудников и поддержание личностного достоинства на основе устойчивого развития предприятия. Состав ценностей могут формировать, например, следующие:

- нравственные и этические идеалы на основе русской культурной традиции [66], являющиеся основой для формирования в коллективе благоприятного психологического климата и деловой творческой атмосферы, поддержания высокого авторитета предприятия в России и за рубежом;
- солидарность и взаимная ответственность предприятия и его сотрудников;
- инновационный характер предпринимательства, развитие государственно-частного партнёрства в интересах безопасного существования России.

Соотношение частных и корпоративных интересов удобно рассмотреть на следующем примере. В число интересов работника изначально (имманентно) не входит «корпоративный патриотизм». Однако, очевидно, что чем больше работников охвачено этим чувством, тем более сплочён и эффективен трудовой коллектив, существование предприятия опирается на крепкую человеческую основу. Исходя из этого «корпоративный патриотизм» должен занимать определённое место в системе ценностей предприятия. Эта ценность существует не абстрактно, а в отношениях работников к предприятию. При этом она не обязательно должна быть осмыслена всеми и «оформлена» в сознании, как результат дискурса. Достаточно чтобы работники на эмоциональном уровне ассоциировали свой жизненный успех с успехом предприятия, испытывали удовольствие от идентификации себя в качестве члена его

коллектива. В то же время для укоренения «корпоративного патриотизма» в коллективе он должен быть осознан в качестве ценности руководством предприятия и мотивировать соответствующую активность руководящей деятельности.

Таким образом, интересы предприятия представляют собой, с одной стороны, диалектическое единство интересов личности и микросоциума, физических и юридического лиц. С другой – они должны являться композицией интересов различных лиц, имеющих свои социальные роли по отношению к предприятию: собственников, руководителей, трудового коллектива, государства, потребителей продукции, поставщиков. Всех субъектов способных оказывать влияние на его жизнедеятельность.

В кибернетике доказано, что из неэффективных элементов может быть построена эффективная система [67]. Однако для этого должно быть выполнено одно принципиально важное условие: система должна быть не совокупностью свободных элементов, а именно системой, т. е. обладать эмерджентностью. Применительно к организационной системе достичь этого можно, гармонизировав цели и интересы составляющих её коллективов и отдельных людей, в том числе за счёт сочетания институтов и инструментов ограничения и стимулирования деятельности. В то же время элементы системы должны быть обеспечены необходимыми ресурсами (людьми, энергией, материальными ценностями, информацией, финансами).

Деятельность предприятия направляется целями и задачами, которые перед ним ставят собственники и руководители. Эти цели и задачи определяются интересами указанных лиц. Если при этом возникнет конфликт интересов собственников, управленцев, работников, то безопасное существование предприятия не будет обеспечено. Пострадать могут все. Если уровень зарплаты, социальный пакет, охрана труда не удовлетворяют трудовой коллектив, то это рано или поздно приведёт к конфликтам в масштабах предприятия, текучести и вымыванию качественных трудовых ресурсов, снижению качества труда, ослаблению инициативы и т. п. Соперничая за трудовые ресурсы собственники и руководители также должны идти навстречу социальным притязаниям работников и жителей окрестностей.

В общем случае весь спектр интересов является взаимосвязанным. Взаимовыгодный компромисс, по утверждению Моисеева Н.Н., это «важнейший фрагмент теории кооперативного взаимодействия, которое, наряду с внутривидовой борьбой, является одним из основных механизмов, определяющих развитие живого мира и человеческого общества, в частности (и в особенности!)…» [68].

Таким образом, в организационной системе должен работать механизм консолидации усилий её элементов на решение целевых задач системы, определяющий содержание, целеустремлённость и темпы развития. При этом такой механизм должен оставлять элементам необходимую степень свободы и возможность удовлетворять свои частные интересы, не противоречащие интересам всей системы. Последнее может служить дополнительным фактором удовлетворения ожиданий работников от сотрудничества в рамках предприятия. Использоваться этот фактор может не только пассивно (как сложилось), но и путём целенаправленного формирования у элементов системы (работников, микроколлективов) частных интересов, согласующихся с системными интересами предприятия. В случае удачи таких усилий возникают эффекты резонанса и синергии в процессах деятельности предприятия.

Российский математик В.И. Арнольд с использованием аппарата «мягких» моделей показал, что, если организационная система имеет больше двух уровней управления, и каждый из них в своей деятельности руководствуется не целями (интересами) всей системы, а пытается «угодить» непосредственному начальнику, то такая организация теряет устойчивость и своих интересов не достигает [69]. Положительный результат может быть получен только в том случае, когда все уровни иерархии организационной системы в своей деятельности руководствуются интересами системы, пронизаны её ценностями.[5] Практически достичь этого можно путём формулирования требований к уровням, в пределе к каждому работнику, удовлетворение которых автоматически способствует достижению интересов предприятия, а также поддержанием корпоративной культуры, предполагающей взаимное уважение, справедливость, этику общего дела.

[5] Следует отметить, что живые системы более адекватно описываются не иерархическими структурами, а фрактальными и сетецентрическими.

Стимулирование исполнения требований может поддерживаться оценкой деятельности по разработанной системе показателей удовлетворения требований с последующим адекватным вознаграждением. Результаты работы коллектива, в особенности творческого (а таковым он и должен быть на инновационном предприятии) зависят не только от системы материальных стимулов и квалификации работников, но в значительной степени от морально-психологического климата в коллективе.

Система интересов предприятия, опредмеченная в целях, задачах, планах, определяет систему ожиданий предприятия от внешней среды [3], взаимных ожиданий собственников, руководителей и работников. Здесь уместно отметить, что внешняя среда также имеет свои интересы и соответствующую им систему ожиданий, включая ожидания от рассматриваемого предприятия.

Удовлетворение ожиданий позволяет реализовать интересы, напротив, их неудовлетворение, вероятно, является первоисточником угроз и их реализации. В общем случае антагонистическая система (конкурент) может ожидать ухода с рынка, прекращения существования (кончины) рассматриваемого предприятия. Для исполнения этого ожидания антагонист будет вести конкурентную борьбу.

Подводя итог, можно предложить следующий перечень основных интересов предприятия:

- уровень дивидендных выплат на протяжении некоторого периода;
- авторитет в обществе, как передового производителя общественно полезной продукции;
- материальный достаток и приобретение социальной значимости через профессиональную самореализацию руководства;
- удовлетворение социально-экономических ожиданий работников;
- удовлетворение ожиданий потребителей и поставщиков.

В качестве локальных интересов могут рассматриваться:

- увеличение стоимости предприятия;
- обеспечение привлекательности предприятия для трудовых ресурсов;
- поддержание статуса «социально ответственного бизнеса».

Для государственных (муниципальных) предприятий в числе интересов – выполнение государственного (муниципального) заказа (независимо от размера получаемой при этом прибыли), обеспечение занятости на локальном уровне.

Между указанными интересами существуют отношения влияния, однако каждый из них имеет самостоятельное значение, хотя бы для какой-то части стейкхолдеров.

Окончательно перечень интересов определяет ЛПР (акционеры и руководство) применительно к конкретной хозяйственной ситуации и своим предпочтениям.

1.3. Обеспечение безопасного существования предприятия

В соответствии с парадигмой существования управление жизнедеятельностью и развитием хозяйствующего субъекта направлено на достижение его интересов, отражающих содержание существования.

Согласно общей теории управления процесс управления заключается в придании объекту управления направления и скорости движения (развития, изменения) к заданной цели. Механизмы управления призваны формализовать и регламентировать порядок действий в определённых типовых ситуациях выработки решений. Это позволяет уменьшать количество ошибок, вызванных недостатком информации, эмоциональным напряжением, субъективным восприятием ситуации, сокращать время на подготовку и реализацию управленческого решения. Механизмы управления позволяют обеспечить предсказуемость решений.

Особое значение механизмы управления приобретают, когда требуется принятие решения в:

1) многокритериальном пространстве в условиях неопределённости; при этом необходимо учитывать большой объём информации, которую готовит и использует большое количество участников; например, разработка перспективного плана направлений научных исследований;

2) быстроменяющейся обстановке с нарастанием объёма неконтролируемых действий, параметров состояния системы и динамики их изменения.

Наличие механизмов облегчает труд руководителей, позволяет эффективно использовать современные информационные технологии при подготовке решений.

При рассмотрении управления жизнедеятельностью и развитием предприятия целесообразно выделить два типа задач:

- обеспечение удовлетворения интересов предприятия за счёт выполнения производственных и других процессов в штатном (регламентном) режиме;
- предотвращение нецелевого использования ресурсов предприятия.

Решение задач первого типа предполагает:

- выполнение штатных (регламентных) производственных процессов (первый подтип) для обеспечения существующих интересов предприятия;
- устранение рассогласования между требуемым уровнем существования и наличным (между желаемым и располагаемым) за счёт целенаправленного развития ПОС и совершенствования механизмов его использования (второй подтип).

Задачи второго подтипа первого типа возникают, когда появляются новые интересы предприятия или возрастает желаемый уровень удовлетворения прежних, другими словами, предприятие намерено изменить качественную определённость своего существования.

Рассогласование между желаемым и располагаемым уровнями существования может рассматриваться как условная угроза (если первое выше второго).

Второй тип задач предполагает деятельность, направленную на:

- поддержание состояния удовлетворения интересов с учётом воздействия на предприятие среды существования, т. е. предотвращение и нейтрализацию угроз и минимизацию рисков за счёт использования ПОС (первый подтип);
- обеспечение развития ПОС для предотвращения и минимизации ущербов (защиты ресурсов от ущербов) (второй подтип).

Под средой здесь понимается как сущее, не входящее в состав системы-предприятие, так и элементы этой системы, но действующие в интересах, отличных от интересов системы-предприятия, например,

работники, преследующие цели личной корысти или проявляющие недобросовестность. Использование ресурсов характеризуется эффективностью, которая через обратную связь влияет на экономию расхода ресурсов для обеспечения безопасного существования.

Описанная типология задач схематично представлена на рисунке 2.

Все указанные задачи, кроме задач первого типа первого подтипа (при допущении об идеально отлаженных механизмах жизнедеятельности), в общем случае предусматривают укрепление ПОС и совершенствование механизмов его использования, т. е. развитие предприятия. Если допустить теоретическую абстракцию, что воздействие среды не меняются по структуре, силе, частоте и другим параметрам, то задачи второго типа могут решаться и без развития. Однако удовлетворить растущие интересы предприятия без его развития невозможно никогда.

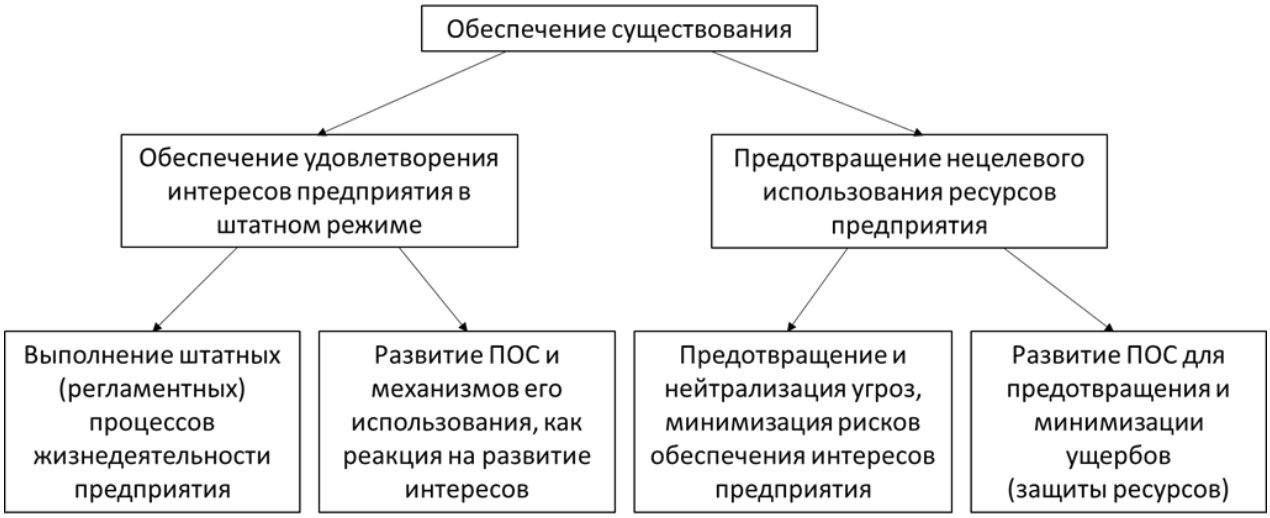

Рисунок 2 – Схема типологии задач обеспечения существования

Иерархия задач предприятия с точки зрения выполнения различных деловых процессов и взаимодействия с окружающей средой для удовлетворения его интересов (целевое функционирование) может быть представлена на пяти уровнях, отражающих стратегическое и тактическое управление (рисунок 3).

Каждый вышерасположенный уровень отличается от предыдущего более широким горизонтом прогнозирования и планирования и сокращённой возможностью использовать количественные шкалы и формальные процедуры анализа. Расширение конуса образно

демонстрирует возрастание неопределённости принятия решения, разнообразие и сложность задач, уровни и разнообразие рисков, а также фрактальную вложенность задач и функций управления нижележащего уровня в вышерасположенный. Нижние уровни без верхних теряют смысл и целенаправленность, а верхние без нижних – «материю» своего содержания.

В парадигме существования каждый уровень снизу-вверх может быть символически назван в соответствии с главной решаемой задачей: обладание, выживание, развитие, процветание, предназначение.

Рисунок 3 – Схема иерархии задач целевого функционирования предприятия в парадигме существования

С методологической точки зрения в рамках парадигмы обеспечения существования стратегическое управление предприятием включает следующие основные механизмы:

- прогнозирование воздействий внешней среды и изменения интересов, их влияния на уровень безопасного существования, т. е. аудит степени удовлетворения интересов предприятия;
- обеспечение достижения интересов, парирования (предупреждение) угроз и минимизации рисков;
- анализ и оценка состояния ПОС;
- постановка задач развития ПОС и организация деятельности по их решению.

Тактическое (операциональное) управление ограничивается эффективным использованием ПОС для решения текущих производственных задач (первый подтип первого типа), предотвращения и парирования угроз, минимизации рисков и устранение их последствий (первый подтип второго типа). Рассмотрение текущих производственных задач выходит за рамки предмета настоящей работы. Кроме того, они применительно к предприятиям различных типов, масштабов и сфер деятельности, описаны в многочисленных трудах как отечественных, так и зарубежных авторов. В дальнейшем основное внимание в монографии уделено остальным задачам, из числа указанных на рисунке 2. Именно эти задачи составляют основное содержание управления, поскольку потребность в управлении возникает, когда появляются возмущающие воздействия или требуется изменить траекторию движения, чтобы достичь цель и получить удовлетворение, т. е. добиться существования на желаемом уровне.

Для описания последствий влияния реализации угроз в форме рисковых событий на уровень безопасного существования предприятия (достижение его интересов) служат риски. Интегральный риск отражает интегральный ожидаемый ущерб предприятию в условиях неопределённости бытия и характеризует степень достижения предприятием состояния безопасного существования. Фактически интегральный риск является оценкой безопасности. При этом речь целесообразно вести об «остаточном» (если можно так сказать) риске, т. е. об оценке ущерба, который может быть нанесён при реализации угроз с учётом задействования ПОС для противодействия реализации угроз и минимизации ущерба.

Выше было отмечено, что при возникновении новых интересов рассогласование желаемого и располагаемого, субъективно переживаемое как негативное явление, может рассматриваться как условный ущерб. Этот ущерб соответственно отражает условный риск. Последний может учитываться в составе интегрального риска при оценке качества существования на заданный момент времени.

Выделение компонент интегрального риска по «физическому» содержанию ущерба (финансовые потери, подрыв авторитета руководителей в деловой среде, утечка конфиденциальной информации,

др.) или интересам (например, дивиденды, реализация статуса социального предприятия, выполнение госзаказа и др.) позволяет оценить частные аспекты безопасного существования. Однако интегральный риск далеко не всегда может быть описан тривиальной аддитивной структурой. Кроме того, интересы в общем случае также взаимосвязаны отношением влияния на степень удовлетворения. В связи с этим декомпозиция на частные виды безопасности может проводиться только как искусственный приём в целях удобства практической работы по анализу отдельных сфер деятельности: рациональное использование материальных и финансовых ресурсов, охрана товарно-материальных ценностей, управление знаниями, защита информационных ресурсов и контроль доступа к ним, управление персоналом, мотивация персонала, внедрение природоохранных мероприятий, контроль соблюдения экологических стандартов и т. д. Эти и другие задачи и функции управления и жизнедеятельности предприятия системно интегрированы в процессах выпуска различных видов продукции, а также при реализации проектов. Попытки эклектичного рассмотрения различных сторон безопасного существования приводят к некорректным оценкам, не позволяют адекватно расставить приоритеты деятельности по устранению причин угроз, нейтрализации и предотвращению рисковых событий.

Решить проблемы комплексного учёта отдельных рисков, имеющих разную природу, можно с использованием лингвистических шкал для описания рисков и степени достижения интересов, когнитивного моделирования для описания взаимовлияния угроз через риски и влияния рисков на интересы, а также взаимоотношений между интересами. Интегральные оценки могут быть получены с использованием различных методов скаляризации функций, описывающих качество решения задачи в векторном пространстве определения [70].

Оценка интегрального риска важна не только сама по себе для прогнозирования возможности безопасного существования предприятия, но и для ранжирования угроз в соответствии со степенью их влияния на величину интегрального риска. При этом последняя задача важнее, поскольку она носит активное синтетическое начало и позволяет

сформировать постановку задачи по укреплению безопасности: развитию ПОС, повышению эффективности его использования.

Задача нецелевого использования ресурсов предприятия (см. рисунок 2) сводится к задаче предотвращения угроз и минимизации ущерба при наступлении рисковых событий с учётом необходимости принятия превентивных мер, включая развитие ПОС. Задачи развития ПОС включают как задачи стратегического управления развитием, так и задачи укрепления сил и средств защиты ресурсов, традиционно решаемые в русле тематики обеспечения безопасности предприятия. Использование категории ПОС, объединяющего все ресурсы хозяйствующего субъекта, как основу его функционирования, имеет теоретическое основание в ресурсной концепции фирмы [71-73].

Среди отечественных исследователей и практиков наиболее распространён подход к обеспечению безопасности, построенный на выявлении и парировании угроз. Однако эта методология не получила всеобщего признания и в ряде работ по экономической безопасности предприятий (см., например, [14]) подвергается критике, в том числе на том основании, что спектр угроз может быть слишком велик и полностью составить его не представляется возможным. В работе [74] подход «от угроз» на национальном уровне отвергается, как порочная «окопная логика», блокирующая развитие.

Критика подхода «от угроз» иногда имеет идеологическую подоплёку, дескать, такой подход - пережиток отечественного отношения к окружающему, как враждебному, а на самом деле источник и причины неприятностей следует искать, прежде всего, в себе. Последнее во многом верно – необходимо анализировать свой потенциал и обстановку и укреплять (развивать) ПОС. Однако это всегда необходимо дополнять анализом окружения.

В отмеченной идеологической посылке обнаруживается инверсивное представление традиционного мировоззрения в России. На уровне метафизики в русской традиции Пространство осмысливается как потенциальное добро, тогда как на Западе «мир» - это потенциальное зло [66]. Возможно, с этим связана зачастую неоправданная доверчивость российских субъектов к обещаниям международных контрагентов, как на политическом, так и на

экономическом уровнях, систематическая (не означает постоянная) неподготовленность (на материальном уровне) к агрессии и другим испытаниям. Во внутреннем экономическом пространстве России в 90-е гг. повсеместно в бизнесе получали фору наиболее алчные и циничные. Одним словом, вывод «гром не грянет, мужик не перекрестится» имеет прочное культурное основание. Безусловно, это не означает необходимость духовной трансформации отечественных предпринимателей и технократов по западному типу. Напротив, актуальна активная защита ещё сохраняющегося ядра национальной традиции от зарубежных идеологических вирусов, привносимых вместе с обездушенной буржуазностью.

Критика подхода «от угроз» не предлагает конструктивную альтернативу, поскольку не конкретизирует содержание деятельности по обеспечению безопасности на практическом уровне. В то же время нельзя не согласиться с тем, что обеспечение безопасности не должно сводиться к механизму воздействие-ответ.

В настоящей работе речь идёт о необходимом уровне защиты в условиях, когда существует опасность природных и техногенных бедствий, и, главное, когда зло порождается людьми и объективно присутствует в бытии. Кроме того, следует обратить внимание, что угроза в работе рассматривается не только как проявление недобрых намерений. Она понимается в смысле предложенного в разделе 1.1 определения и на системном уровне исследования проблем безопасного существования хозяйствующего субъекта выполняет роль одного из двух факторов[6], мотивирующих деятельность по развитию этого субъекта. Парадигма существования, развивая идеи упреждающего обеспечения безопасности [75], позволяет снять противоречие между «окопной логикой» и необходимостью развития за счёт системно обобщённого смысла понятия «угроза» и гармонизации смысловых отношений между обеспечением безопасности и развитием, что было отмечено выше.

В повседневности обеспечения безопасности предприятия приходится декомпозировать эту проблему, определять её наиболее актуальные задачи и планировать работу. Это приводит к тому, что

[6] Другой фактор, как было отмечено выше, изменение интересов.

более реалистичным является подход к решению проблемы через мониторинг, анализ, прогноз и нейтрализацию угроз и рисковых событий. Практика показывает, что может быть выделено несколько десятков обобщённых угроз, представляющих собой фактически тематику мониторинга воздействия внешней среды и различных внутренних факторов на состояние безопасного существования предприятия. Отправной точкой для составления перечня угроз (в том числе маловероятных, или гипотетических), безусловно, должны являться все интересы предприятия.

Перечень угроз задаёт тематику деятельности по обеспечению безопасности. Его детализация определяется здравым смыслом и иерархией системы управления жизнедеятельностью предприятия. На каждом уровне принятия решения необходима только та информация, которая используется для принятия решения. Мониторинг угроз предоставляет исходные данные для разработки и использования средств и инструментов защиты.

Все обстоятельства, которые негативно влияют на решение задач по удовлетворению интересов хозяйствующего субъекта, в соответствии с определением, предложенным в разделе 1.1, являются угрозами. При этом само рассогласование желаемого (новые интересы или более высокий уровень старых интересов) и располагаемого (должного и сущего) не являются угрозами. Эти рассогласования, наряду с результатами анализа предотвращения и парирования угроз, являются исходными данным для развития ПОС. Угрозами здесь являются условия и факторы, реализация которых приводит к невозможности или создаёт помехи для устранения указанного рассогласования. Как было отмечено выше, указанные рассогласования могут рассматриваться как условные угрозы в целях постановки и решения задач оценки существования и постановки задачи оптимального планирования использования доступных ресурсов для обеспечения существования на заданном уровне в едином пространстве исходных данных.

Для правильной идентификации явлений как угрозы и организации соответствующей деятельности важно провести водораздел между возможностями нанести ущерб, т. е. угрозами, и невозможностями

предотвратить (компенсировать) ущерб, т. е. недостатками потенциала обеспечения существования.

В действительности разница между угрозами и недостатками ПОС улавливается не всегда. Изъяны и прорехи в системе обеспечения безопасного существования порой включаются в перечень угроз на том основании, что они могут являться предпосылками ущерба. В этих случаях к угрозам причисляют, например, кадровую неукомплектованность службы безопасности, отсутствие системы контроля доступа к ценностям, технологическую отсталость и т. п. Это запутывает методологию выявления угроз и синтеза рациональных путей их парирования, затрудняет построение стройного математического аппарата решения этих задач.

Ущерб наносят только рисковые события. Их устранение однозначно исключает ущерб. Именно угрозы, наряду с новыми интересами, формируют объективную мотивацию развития ПОС. При неизменных интересах и отсутствии угроз ПОС был бы нужен только для того, чтобы поддерживать производство продукции заданной номенклатуры на заданном уровне. Многие компоненты ПОС, например, охрана, система генерации и внедрения новшеств, были бы не нужны.

Вратарь по своему предназначению не занимается забиванием голов в свои ворота (автогол здесь не учитывается), т. е. ущерб не наносит. Беда случится, если он не сможет преградить путь мячу или шайбе. Слабый вратарь, очевидно, не увеличивает шансы команды выиграть, однако если полевые игроки соперника не в состоянии попасть в створ ворот, то в ворота можно вообще никого не ставить.

По-разному должна быть организована и осуществляться работа в отношении угроз и ПОС.

Первые возникают и развиваются «по своим законам», по своей логике, задаваемым источниками угроз. Угрозы можно и нужно превентивно диагностировать. Для этого требуется вести их мониторинг, выявлять их признаки и прогнозировать вероятность тех или иных рисковых событий, влекущих ущерб соответствующей величины. Ситуации «превентивного удара» суть дела здесь не меняют, поскольку они являются результатом противодействия угрозам на

ранних стадиях их формирования. В идеале для устранения угроз «в зародыше» необходимо выявлять и устранять причины появления угроз в тех случаях, когда это в принципе возможно. Об этом несколько подробнее будет сказано ниже.

Напротив, ПОС предприятия может изучаться в плановом порядке. Исходные данные и результаты этого изучения носят вполне определённый характер. ПОС развивается в соответствии с управленческими решениями руководства хозяйствующего субъекта в зависимости от прогнозируемого уровня риска и в соответствии с доходами бизнеса. Активные действия субъектов угроз могут привнести чрезвычайность в жизнедеятельность предприятия, но формирование, развитие и использование ПОС всё равно находится в руках руководства предприятия и его коллектива, включая силы подразделений безопасности (защиты ресурсов) с их оперативной и чрезвычайной компонентами.

Источником угроз может быть, как внешний по отношению к рассматриваемому предприятию объект, субъект, процесс или явление, так и элемент, фактор самой системы – организационное подразделение, должностное лицо, технология, деловой процесс (снабжение, внедрение инноваций, оптимизация финансовых потоков, социальные отношения на предприятии и т. п.). Вместе с рассмотрением риска в качестве характеристики угрозы это создаёт возможность интегрировать на единой методологической и модельной основе все факторы жизнедеятельности предприятия с точки зрения обеспечения его интересов.

Общий механизм стратегического управления предприятием на основе парадигмы существования представлен на рисунке 4.

Методология обеспечения безопасности на основе анализа угроз предполагает выявление причин и источников появления угроз и их реализации. Это необходимо для повышения качества организации мониторинга, выстраивания системы упреждающего противодействия, выявления слабых мест (точек) в системе защиты (в ПОС), через которые состояние безопасности может подвергаться воздействию различных угроз.

Рисунок 4 – Общий механизм стратегического управления предприятием на основе парадигмы существования

Причины и точки возникновения угроз находятся в деятельностно-пространственно-временном континууме. Причины кроются либо в действиях естественных законов физического мира, на которые система управления, предприятием влиять не может, либо следуют из конфликта интересов различных субъектов (личностей, организаций, социально-экономических систем без институционального оформления). В первую группу включаются также техногенные и антропогенные аварии, не являющиеся результатом целенаправленных действий в отношении предприятия со стороны каких-либо субъектов.

Конфликт интересов определяется конкуренцией за ограниченные ресурсы, а также поиском со стороны субъекта возможностей наилучшего удовлетворения своих потребностей и ценностей.

В последние годы в западных исследованиях и практике управления субъектами экономической деятельности развивается тема преобразования конкуренции в глобальное конкурентное сотрудничество. Однако практически это реализуется в виде развития «корпоративного индивидуализма» и конкуренции на уровне корпораций,

стран и их сообществ. Создатель японского чуда в менеджменте, почитаемый и востребованный (при жизни) в США, как учёный и консультант, Деминг У. Эдвард на уровне фирм активно противопоставлял конкуренции сотрудничество [76], однако переломить менталитет англо-сакского бизнеса не смог. Практическая реализация его идей происходила в основном в Японии, а не в США. В мире развитой экономики пока доминирует жёсткая борьба за деньги потребителей. Первичным критерием деятельности компаний является не создание общественных благ, а рост прибылей (при новых методологических подходах – рост стоимости компаний, что, в сущности, тождественно). В какой мере российской экономике хотя бы внутри удастся добиться превалирования сотрудничества и кооперации над конкуренцией, в особенности недобросовестной, во многом зависит от укоренения традиционного национального мировосприятия в деловой среде и принятия парадигмы существования на всех уровнях организационных систем.

Попытки использовать недобросовестные способы удовлетворения своих потребностей и достижения ценностей (в более узком смысле – ожиданий), очевидно, порождают угрозы. Например, стремление к материальному достатку может мотивировать человека, как на более производительный труд и саморазвитие для эффективного экономического использования своего потенциала (знаний, умений, навыков, способностей, таланта), так и недобросовестные действия в целях получения незаконного или(и) незаработанного (незаслуженного) дохода (вознаграждения).

Для своевременного выявления угроз необходимо наблюдать и анализировать также вызовы, которые могут являться источниками угроз. Аналогично и вызовы целесообразно соотносить с деятельностно-пространственно-временным континуумом существования предприятия в целях выявления последствий их влияния.

Моделирование деятельностно-пространственно-временного континуума направлено на выявление возможностей использования (неиспользования) ресурсов предприятия в личных (узко групповых)

интересах при помощи деловых процессов предприятия или вследствие их отсутствия.

Координата деятельности описывает различные деловые процессы, например, оценка качества продукции, организация и проведение закупок, использование информационных фондов предприятия и т. д. В различных элементарных операциях по реализации таких процессов могут возникать условия для злоупотреблений или экономии личностного ресурса, если не созданы инструменты предотвращения разрешения конфликта интересов личности с интересами предприятия в ущерб предприятию. Так, при организации закупок может быть реализована коррупционная схема и выбран нелучший, а то и вовсе негодный поставщик. Повышение квалификационного уровня и аттестация работников может проводиться формально и создавать угрозы потери качества труда с вытекающими отсюда последствиями, например, авариями, браком.

Пространственная координата предполагает объектовую и региональную декомпозицию причин возникновения угроз.

Временная - связана с особенностями различных этапов, которые может переживать предприятие на протяжении своей сколь угодно долгой истории, реализацией определённых этапов длительных жизненных циклов сложной продукции, сезонным характером работ. Например, предприятие может находиться в состоянии подготовки к процессу слияния-поглощения, реализации процесса объединения, формирования единой корпоративной культуры, пересмотра структуры использования интеллектуального потенциала в связи с изменением конъюнктуры спроса. Оно может быть занято растениеводством (весной сеет, осенью жнёт) или выполнять полный объём работ по созданию космического орбитального научно-производственного комплекса (создание компонент, транспортировка на орбиту, сборка и запуск в эксплуатацию).

Для выявления угроз, главным образом, при решении задач первого типа (устранение рассогласования требуемых уровней удовлетворения интересов (в т. ч. новых) и возможностей предприятия) удобно использовать диаграммы К. Исикавы. Структура этой диаграммы

моделирует структуру скелета рыбы. На её основных рёбрах можно откладывать возможные наиболее укрупнённые группы источников угроз, на крупных «костях», примыкающих к рёбрам – более точные группы источников угроз и т. д. Двигаясь по «рёбрам», «костям» и «косточкам», специалисты могут постепенно «докапываться» до первопричин рассогласования должного (желаемого) и сущего. Этот метод К. Исикавы с успехом применяется на промышленных предприятиях для выявления причин аварий, неисправностей и т. п.

Устойчивость системы обеспечивается как наличием ресурсов, так и возможностью их адаптивного использования. Последнее характеризуется управляемостью, т. е. способностью компенсировать отклонения от заданной траектории с задержкой и скоростью, сохраняющими устойчивость. Одними из условий обеспечения управляемости является своевременное и адекватное выявление воздействий, т. е. угроз, замеры качества и наличия ресурсов, а также их своевременное пополнение.

Таким образом, организация мониторинга угроз должна опираться на решение научно-методической задачи информационного моделирования проблематики обеспечения безопасного существования, включая моделирование деловых процессов, уязвимостей, создание моделей реализации угроз с учётом структуры мотивации действующих лиц. В качестве инструментов могут быть использованы когнитивные модели, сценарное моделирование, теория игр, ситуационный анализ, инфологические модели и структурно-функциональное моделирование.

Реализация механизма стратегического управления предприятием, а также интегративными структурами на основе парадигмы существования позволяет органично реализовать современные тенденции развития и черты корпоративного управления [77, 78], в частности:

- гибкость, адаптируемость к постоянным изменениям внешней среды;
- использование наработок теории систем, позволяющих содержательно рассматривать организацию в единстве её составных

частей, находящихся во взаимодействии между собой и с внешней средой;

- использование ситуационного управления, позволяющего выделять конкретный набор обстоятельств, которые оказывают решающее влияние на функционирование предприятия в текущий момент и в перспективе;

- смещение акцентов в управлении с лидерства и централизованной регламентации на самоорганизацию, мотивацию, совершенствование взаимоотношений в коллективе, развитие корпоративной культуры, предполагающей сотрудничество и взаимопонимание;

- защита прав акционеров (учредителей) хозяйствующего субъекта, а также интересов всех лиц, благоденствие и социальная значимость которых зависит от его существования;

- разработка миссии предприятия (корпорации), его стратегии, программ и планов, как единый творческий и управленческий процесс.

Основная тематика деятельности по предотвращению нецелевого использования ресурсов предприятия (парирования угроз) представлена на рисунке 5.

Очевидно, что направления деятельности, указанные на рисунке 5, выходят за рамки традиционного функционала подразделений обеспечения безопасности (экономической безопасности) или защиты ресурсов предприятия. Безусловно, в ряду целевых задач обеспечения безопасного существования предприятия находится также задача управления рисками. В контексте монографии «управление рисками» является синонимом «противодействие субъектам угроз». На практике предметная область обеспечения безопасности, обычно, существенно уже, представленной на рисунке 5.

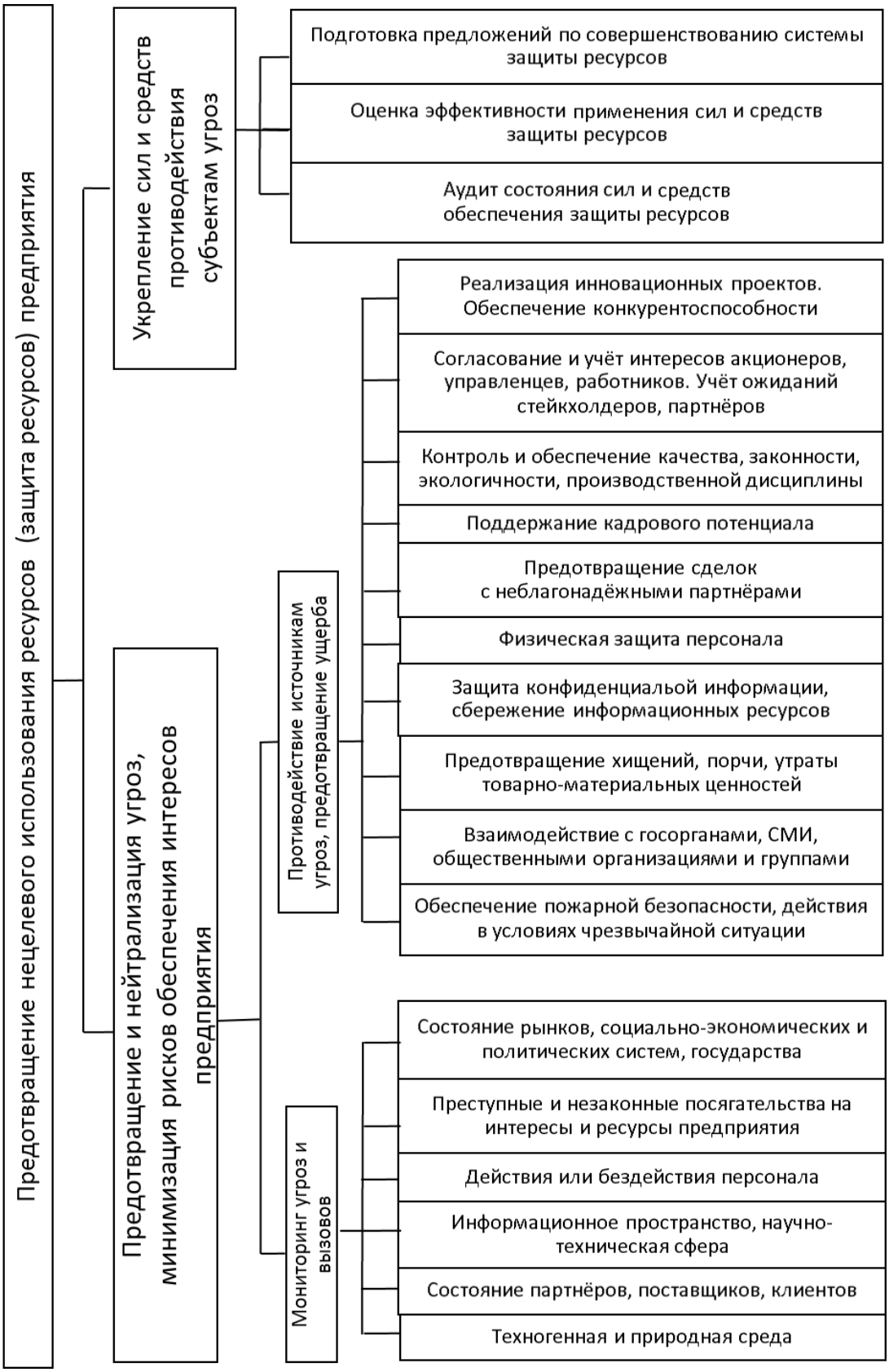

Рисунок 5 – Тематика деятельности по обеспечению безопасного существования предприятия

Это вынуждает руководство предприятия наряду с задачами защиты ресурсов отдельно рассматривать задачи управления рисками. В организационном аспекте «под задачи» управления рисками в большом бизнесе, как правило, создаётся специальное подразделение в составе органов управления компанией. Организационная сторона этого вопроса здесь не рассматривается, а с методической точки зрения задачи противодействия субъектам угроз и управления рисками являются тождественными.

Важное значение в составе задач обеспечения безопасного существования имеет оценка эффективности соответствующей деятельности. Выше было отмечено, что состояние безопасности отражает интегральный риск, однако установить однозначные корректные отношения между параметрами деятельности по обеспечению безопасности и уменьшением рисков далеко не всегда возможно. Особенно трудно это сделать при решении задач предотвращения ущербов.

В данном случае невозможно оценить эффективность деятельности по числу предотвращённых или выявленных фактов неблаговидных деяний, поскольку хорошо поставленная предупредительная работа существенно сокращает возможности и мотивацию нанесения ущерба. Задача оценки эффективности системной работы по обеспечению безопасности аналогична задаче выбора решения за что платить семейному доктору: за лечение или за те дни, которые пациенты провели в здравии. Для решения этой задачи целесообразно использовать методы оценки эффективности и активности защиты ресурсов.

Есть некоторые особенности рассмотрения безопасности отрасли промышленности.

Отрасль представляет собой совокупность предприятий и управляющих органов, объединённых сферой экономической деятельности, особенностями и направленностью производственных циклов. Особенностью существования отрасли является отсутствие прав собственности на предприятия, ограниченность возможностей административного влияния на операционную деятельность предприятий, в особенности негосударственных, ограниченность собственных ресурсов для нейтрализации угроз.

Интересы отрасли отражают интересы государства и олицетворяются её руководством. К ним можно отнести:

- выполнение государственных и отраслевых научно-технических, инновационных, производственных стратегий, программ, планов и т. п.;
- обеспечение прибыльности предприятий на заданном уровне;
- обеспечение технологического уровня отрасли на заданном уровне;
- обеспечение заданного научно-технического потенциала отрасли;
- реализация социальных программ отрасли.

Третий, четвёртый и пятый интересы являются обеспечивающими для первых двух, однако имеют и самостоятельное значение.

Не все предприятия некоторых, например, оборонных отраслей являются источниками прибыли, однако с необходимостью должна быть обеспечена их безубыточность. В противном случае, их безопасность в экономическом аспекте не может быть обеспечена.

Угрозами для безопасности отрасли является состояние безопасности предприятий, в том числе их технологическая и кадровая деградация, нарушение предприятиями контрактной дисциплины, невыполнение ими программ, планов, стратегий, в том числе инновационного развития, социальных программ. Кроме того, к угрозам относятся неблагоприятные изменения макроэкономической ситуации, изменения конъюнктуры международных рынков, сокращение финансирования государственных программ, сбои в работе и выполнении контрактных и договорных обязательств со стороны не входящих в отрасль субъектов хозяйственной деятельности.

Фактически угрозы предприятиям через них транслируются на безопасность отрасли. При этом угрозы предприятиям на уровне отрасли могут усиливаться и видоизменяться. Так, нарушение технологического цикла на предприятии может привести к ущербу на уровне предприятия, а невыполнение производственных планов предприятия может нарушить работу отраслевой кооперации.

ПОС отрасли включает, прежде всего, предприятия. К нему также относится уровень вариативности кооперационных цепочек, различные резервные, страховые фонды, созданные при участии управляющих органов отрасли, кадровый потенциал управляющих органов отрасли, информационные системы обеспечения взаимодействия предприятий отрасли, система обеспечения инновационного развития отрасли,

потенциал отечественной промышленности по выпуску комплектующих, материалов, узлов и агрегатов для производства и эксплуатации продукции, техническая инфраструктура.

Оценка безопасность отрасли не сводится к сумме оценок безопасностей предприятий, входящих в неё. Она должна оцениваться по интегральному ущербу отрасли, а он является следствием нелинейных взаимодействий между предприятиями и с окружающей средой.

1.4. Угрозы безопасному существованию предприятия

В разделе 1.3 задача мониторинга угроз определена в качестве одной из ключевых в проблематике обеспечения безопасного существования. Результаты решения этой задачи формируют исходные данные для других задач обеспечения безопасного существования.

Примерный перечень угроз для организации мониторинга в качестве информации к размышлению выглядит следующим образом:

- сокращение спроса на продукцию предприятия;
- снижение качества продукции;
- рост себестоимости продукции;
- дефицит сырьевой базы, энергии, комплектующих, материалов;
- предъявление предприятию исков и штрафных санкций;
- неправовые действия в отношении предприятия со стороны государственных органов;
- арест активов предприятия;
- дефицит финансовых ресурсов (финансовая неустойчивость предприятия);
- хищения и другие потери материальных и финансовых ресурсов, в том числе дебиторская задолженность, брак, двойное предпринимательство сотрудников;
- утечка конфиденциальной информации;
- утрата информационных ресурсов;
- рост цен на продукцию поставщиков;
- неудовлетворительная платежеспособность (банкротство) контрагентов (потребителей и поставщиков);
- монополизация поставщиками рынков сырья, энергии, материалов, комплектующих;

- нарушение договорных обязательств со стороны поставщиков;
- активизация маркетинговой деятельности конкурентов (рекламные акции, снижение цен, реализация новых эффективных схем логистики и сбыта);
- монополизация рынков сбыта конкурентами за счёт слияния, поглощения и т. п.;
- рост налоговой нагрузки;
- удорожание кредитных ресурсов;
- неблагоприятное изменение соотношения интересующих валют;
- протестная активность работников;
- недобросовестные действия конкурентов на рынке;
- попытки неконтролируемой скупки акций предприятия;
- деловые контакты с недобросовестными юридическими и физическими лицами, а также лицами, связанными с ОПГ;
- проникновение представителей ОПГ и(или) конкурентов в состав сотрудников предприятия (штатных, работающих по гражданско-правовым договорам или оказывающих услуги на регулярной основе);
- саботаж;
- террористический акт;
- диверсия;
- шантаж работников или акционеров;
- посягательство на жизнь и здоровье персонала в связи с выполнением трудовых обязательств или бизнес-деятельностью;
- неблагоприятный образ предприятия в СМИ и Интернет;
- дискредитация продукции предприятия, в том числе в СМИ и Интернет;
- утрата позиций среди исполнителей государственных и муниципальных заказов;
- предвзятость к деятельности предприятия на политическом и бюрократическом уровнях в регионах деловых интересов;
- социальная и(или) политическая нестабильность в регионах деловых интересов предприятия;
- неблагоприятные правовые изменения в регионах деловых интересов;
- экономическая стагнация или рецессия в регионах сбыта продукции;

- неразвитость промышленной, технической, рыночной инфраструктуры в регионах деловых интересов;
- сокращение трудовых ресурсов требуемой квалификации в регионах деловых интересов;
- появление конкурентоспособных центров притяжения трудовых ресурсов требуемой квалификации в регионах деловой активности;
- природные катаклизмы в регионах деловых интересов;
- авария;
- производственный травматизм и профессиональная заболеваемость;
- конфликты между работниками и их группами;
- низкий уровень трудовой дисциплины;
- загрязнение окружающей среды.

Последняя угроза при превышении допустимого уровня, кроме имиджевых потерь, ведёт к искам, санкциям, вплоть до закрытия предприятия.

Среди перечня угроз нет часто упоминаемых специалистами в качестве таковых «потеря конкурентоспособности», «снижение (недостаточность) производственного и технологического потенциала», «сокращение (деградация, недостаточность) кадрового потенциала». Последние в соответствии с подходом, представленном в предыдущих подразделах, относятся к ПОС, а конкурентоспособность требует небольшого комментария.

Конкурентоспособность – комплексный показатель, отражающий способность предприятия удерживать некоторую долю рынка. Она определяется объективными аспектами продукции: качество продукции, цена, послепродажное обслуживание, а также субъективными: реклама, авторитет бренда, включая страну-производителя. В связи с этим падение конкурентоспособности является не угрозой, а следствием реализации других угроз, которые легко обнаружить в предложенном перечне. В свою очередь конкурентоспособность не является и конечным показателем, характеризующим удовлетворение интересов предприятия, например, объём продаж. Конкурентоспособность является трудно формализуемым обобщённым параметром, выполняющим вспомогательную функцию в системе принятия управленческих решений. Зачастую эта категория служит фигурой речи

при обобщённых, вербальных оценках состояния и перспектив развития хозяйствующего субъекта.

В качестве вызовов следует рассматривать появление на рынке новых товаров, которые могут служить товарами-заместителями. С точки зрения стратегической перспективы к вызовам могут относиться тенденции изменения культуры потребления, научные открытия.

В информационном аспекте постановка задачи мониторинга угроз безопасности предприятию может быть представлена пятиуровневой моделью, полностью соответствующей уровням управления предприятия, представленным на рисунке 3. Каждый уровень имеет относительную автономность. Для него могут быть определены ответственные руководители и сотрудники за решение соответствующих задач анализа и парирования угроз. По мере возрастания уровня увеличивается масштабность решаемых задач с точки зрения учёта влияния внешней среды. Соответственно, акцент ответственности смещается от подразделения, обеспечивающего безопасность на уровне непосредственной защиты наличных ресурсов в сторону высшего руководства и подразделений, отвечающих за производство, предпринимательство и стратегическое развитие предприятия.

Угроза, включённая в приведённый перечень для мониторинга состояния безопасного существования предприятия, определяет некоторый вид неблагоприятных условий, идентифицируемый по специфическому содержанию физических процессов и действий, характерных для него. В каждом отдельном случае она воплощается в конкретные действия (рисковые события) и принимает ту или иную форму.

I уровень. Обладание

Уровень обеспечения безопасности работников, сохранности активов предприятия, включая информационные, и защиты коммерческой тайны.

На этом уровне фактически обеспечивается материальная и информационная основа жизнедеятельности хозяйствующего субъекта.

Характер угроз

Прямое нанесение ущерба предприятию путём сокращения его ресурсов непосредственно после рискового события. На этом уровне

носителями угроз являются либо конкретные источники угроз в виде физических лиц или организаций, либо техногенных аварий, стихийных бедствий или социальных потрясений.

Виды ущерба и некоторых рисковых событий:

- нанесение вреда здоровью, в т. ч. психического, работникам, акционерам;
- нанесение материального ущерба работникам, акционерам;
- потери материальных активов (товарно-материальных ценностей, финансовых средств, производственных фондов, недвижимости и т. п.);
- потери информационных ресурсов (документов или образцов товаров в виде «твёрдых» копий или на оптических и магнитных носителях);
- утечка сведений, составляющих коммерческую тайну.

Объекты защиты:

- жизнь и здоровье работников и акционеров в связи с их отношением к предприятию;
- материальные активы;
- нематериальные активы.

Источники угроз:

- конкурирующие структуры;
- криминальные элементы и ОПГ;
- экстремистские организации;
- недобросовестные работники предприятия и контрагентских организаций;
- безответственные сторонние лица;
- заинтересованные чиновники правоохранительных и контролирующих государственных органов;
- ангажированные (заказанные) СМИ и отдельные журналисты;
- технические устройства;
- Природа.

Субъекты обеспечения защиты ресурсов

Основным субъектом защиты ресурсов на уровне «Обладание» является традиционная служба безопасности или защиты ресурсов.

II уровень. Выживание

Уровень обеспечения внутренних процессов жизнедеятельности предприятия, прежде всего решения производственных задач в рамках

текущих условий и краткосрочной перспективы (квартального и годового планирования).

Характер угроз

Нанесение ущерба интересам бизнеса на уровне нарушения производственных процессов и дестабилизации обстановки в трудовых коллективах. Субъекты угроз чаще всего находятся внутри бизнеса, однако не исключается внешнее воздействие, в том числе в форме рефлексивного управления с целью дезорганизовать обеспечение производственных циклов.

Виды ущерба и некоторых рисковых событий:

- сокращение (невыполнение планов) производства;
- утрата технологического потенциала;
- сокращение кадрового потенциала;
- нарушение условий охраны труда и качества окружающей среды.

Объекты защиты:

- технологические и производственные циклы;
- механизмы хозяйственной деятельности;
- основные и вспомогательные производственные фонды;
- информационные ресурсы, в т. ч. интеллектуальные ресурсы, защищённые патентами или в режиме секретов производства («ноу-хау»);
- кадровый потенциал.

Источники угроз:

- конкурирующие структуры;
- криминальные элементы и ОПГ;
- недобросовестные работники предприятия и контрагентских организаций;
- недальновидные менеджеры бизнеса, отвечающие за обеспечение производственных циклов, сохранение и развитие технологического и кадрового потенциалов;
- заинтересованные чиновники правоохранительных и контролирующих государственных органов.

III уровень. Развитие

Уровень обеспечения благополучного существования бизнеса в пространстве рыночных отношений.

Характер угроз

На рыночном уровне угрозы, главным образом, возникают вследствие объективно возникающих условий на рынке, деятельности конкурирующих структур, неэффективного управления предприятием на рынке и неэффективного управления в компаниях-партнёрах. Угрозы также могут возникать в результате неправомерного или необоснованного вмешательства государственных органов в предпринимательскую деятельность.

Угрозы на рассматриваемом уровне могут носить как безадресный характер, так и направленный на ослабление рыночных позиций конкретного предприятия.

Источник угроз в основном находится вне предприятия.

Виды ущерба и некоторых рисковых событий:

- закрытие предприятия в результате банкротства;
- сокращение (невыполнение планов) прибыли;
- подрыв репутации бизнеса в обществе, государственных органах, предпринимательских структурах.

Объекты защиты:

- интересующих видов сырья, энергии, материалов, услуг, оборудования и комплектующих;
- внешние инвестиционные ресурсы;
- рынок сбыта продукции предприятия;
- акции предприятия;
- деловые связи, внешнее окружение;
- деловая репутация предприятия.

Источники угроз:

- конкурирующие структуры;
- криминальные элементы и структуры;
- недобросовестные работники предприятия и контрагентских организаций;
- недальновидные управленцы предприятия, отвечающие за обеспечение входных потоков ресурсов для производственных циклов, сбыт продукции, обеспечение качества продукции, разработку и реализацию рыночной стратегии;
- заинтересованные чиновники государственных органов.

IV уровень. Процветание

Уровень обеспечения благополучного существования бизнеса в условиях существующей и прогнозируемой социально-экономической и политической среды.

Характер угроз

Нанесение ущерба интересам предприятия на уровне изменения социально-экономических и политических условий в регионах деловой активности, изменения законодательства, политической конъюнктуры.

Угрозы в данном случае носят безадресный для бизнеса характер, за исключением случаев спекулятивного ущемления его интересов в политических целях.

Источники угроз находятся за «периметром» предприятия.

Виды ущерба и некоторых рисковых событий:

- закрытие предприятия;
- сокращение (невыполнение планов) прибыли;
- подрыв репутации бизнеса в обществе, государственных органах, предпринимательских структурах.

Объекты защиты:

- рынок сырья, энергии, материалов, оборудования и комплектующих;
- внешние инвестиционные ресурсы;
- рынок сбыта;
- акции бизнеса;
- внешнее деловое окружение предприятия;
- деловая репутация бизнеса.

Источники угроз:

- политические структуры;
- общественные структуры, профсоюзы;
- протестные социальные группы;
- заинтересованные чиновники государственных органов;
- актуальная социально-экономическая ситуация в регионах присутствия или деловых интересов.

V уровень. Предназначение

Уровень обеспечения благополучного существования предприятия в метастратегической перспективе.

Характер угроз

Нанесение ущерба интересам предприятия на уровне изменения глобальных цивилизационных процессов.

Угрозы в данном случае носят исключительно безадресный по отношению к предприятию характер. Они определяются процессами изменения общественных отношений, культуры, в частности отношений в системе потребления, на уровне стран, цивилизаций и Мира.

Виды ущерба и некоторых рисковых событий:

- ликвидация предприятия.

Объекты защиты:

- предприятие в целом.

Источники угроз:

- глобальные политические структуры, в том числе гегемонистские, фашистские и экстремистские;
- научно-технические структуры;
- большие социальные структуры и группы;
- неизвестные ныне, принципиально новые источники и причины.

Следует отметить, что одни и те же угрозы могут проявляться на различных уровнях. Их распределение по описанным уровням носит относительный характер и определяется удобством организации решения практических задач. Разные угрозы, в том числе находящиеся на различных уровнях, могут иметь одни и те же проявления через рисковые события. Например, угрозы «хищения и другие потери материальных и финансовых ресурсов» и «недобросовестные действия конкурентов на рынке» могут иметь одно и то же проявление – например, порча торговой точки. В первом случае это может быть следствием банального хулиганства или разбоя, во втором – спланированной акцией конкурентов в целях выдавить предприятие с рынка или вынудить его на какие-либо уступки. Очевидно, что серьёзность ситуации и требуемые действия в этих случаях различны. Идентификация угроз по их проявлениям – задача аналитической работы.

При реализации различных проектов может быть более конкретный перечень угроз, связанных с реализацией проекта. Например, для инновационных проектов такой перечень могут составлять следующие угрозы:

- ошибки прогноза получения научных, технических, технологических результатов; недостижение ожидаемых результатов НИР, получение отрицательных экспериментальных данных, использование ложных знаний или неверное использование знаний;

недостижение запланированных тактико-технических характеристик; невозможность при разумных затратах создать (подготовить) технологию промышленного производства новой продукции;

- изменения конъюнктуры рынка, не позволяющие либо предложить новую продукцию в принципе, либо добиться ожидаемого коммерческого успеха с её помощью; опережение конкурентами при патентовании аналогичных результатов интеллектуальной деятельности (далее – РИД);

- увеличение затрат по сравнению с первоначальным прогнозом;

- неготовность, недоступность иных звеньев технической или технологической среды (единой технологии, агрегата, технической системы, машины, материалов и т. п.), в которой предполагалось использовать РИД;

- утечка секрета производства и его использование конкурентами на рынке, в том числе патентование;

- нарушение планов финансирования; отказ от проекта венчурных фондов, государственных структур, инновационных фондов и т. п.;

- нецелевое использование внешнего финансирования инновационного проекта;

- развал кооперации разработчиков и производителей по выполнению инновационного проекта.

Все угрозы по характеру проявления можно разделить на три группы:

- статистические,

- вероятностные,

- уникальные.

Статистические угрозы реализуются с некоторой достаточно высокой и устойчивой по значению частотой. Этот ущерб присутствует практически всегда. Сам факт его появления – достоверное событие, а величина, естественно, может колебаться. Наносимый ущерб может быть описан статистически – средне ожидаемым значением и доверительным интервалом. Путём совершенствования системы управления безопасным существованием его можно снижать и в идеале переводить в разряд вероятностных.

Проявления вероятностных угроз на рассматриваемом интервале времени осуществляется с некоторой вероятностью, установленной расчётным, опытным (например, имитационное моделирование) или

экспертным путём. Наибольшей достоверности анализ может достичь, если для вероятности реализации угрозы установлен закон распределения. Реализация вероятностных угроз не является достоверным событием.

Уникальные угрозы носят, главным образом, гипотетический характер. Они мыслятся, имели единичные реализации или вовсе никогда не реализовывались. Уникальные угрозы связаны с проявлением неизученных, плохо (или не) наблюдаемых явлений или проявлением воли людей. Они характеризуются низкой априорной вероятностью реализации через рисковые события. Как правило, оценка этой вероятности мала и не имеет естественно научных строгих обоснований, т. е. выносится на субъективном интуитивном уровне экспертами или другими лицами, готовящими и принимающими решения.

Уникальные угрозы, обычно, несут значимый, а порой катастрофический, ущерб, иначе в силу их редкости они бы не замечались и не рассматривались. В то же время увлечение учётом уникальных угроз может служить свидетельством повышенной тревожности, высоким субъективным требованием к безопасности и приводить к контрпродуктивной затрате ресурсов на обеспечение безопасности.

В процессе подготовки к осуществлению, в ходе «созревания» вероятностные и уникальные угрозы могут приобретать более ощутимые и объяснимые вероятностные оценки. Формированию адекватного отношения к уникальным угрозам способствует выявление и изучение вызовов, которые могут быть предвестниками таких угроз. По терминологии Н. Таллеба, подобные уникальные угрозы и, соответственно, рисковые события называют «чёрными лебедями» [79][7]. Примером здесь может служить появление товаров, реализующих новые физические принципы удовлетворения потребности. Динамика перехода от катушечных магнитофонных лент до оптико-электронных дисков огромной ёмкости заняла не более двух десятков лет. Пейджеры только мелькнули на рынке и были полностью вытеснены мобильными телефонами.

[7] До открытия Австралии европейцы считали, что лебедей чёрного цвета не бывает. Даже этимология слова «лебедь» в разных языках отражает «белый», «искрящийся» и т. п.

Особое значение имеет выявление угроз, рисковых событий, последствия которых способны масштабироваться, т. е. распространяться без (или почти без) ограничений не пропорционально затратам источника угроз. К таким угрозам может относиться, например, проведение конкурентом успешной информационной компании.

Для осуществления мониторинга и выявления угроз, а также оценки их актуальности и возможного риска необходимо определить признаки (показатели) угроз. По возможности это должны быть измеряемые величины, непосредственно описывающие угрозы. В этом случае можно существенно уменьшить субъективизм в оценках угроз. По крайней мере, «вкусовые» трактовки динамики угроз и их сравнительных описаний в отношении различных объектов и направлений деятельности предприятия будут сведены к «нулю». Однако не всегда удаётся использовать количественные объективно измеряемые показатели. В этих случаях приходится прибегать к экспертным оценкам и использовать формализованные лингвистические шкалы, которые помогают экспертам точнее разобраться в своих ощущениях и передать их ЛПР, а также оставляют возможность строить математические модели и применять вычислительную технику для анализа состояния безопасности.

Составить универсальный, единственно верный перечень угроз и их показателей невозможно не только потому, что предмет и условия предпринимательства существенно отличаются для разных хозяйствующих субъектов и в разных условиях, но и потому, что эта задача носит сугубо творческий характер. Здесь отсутствуют какие-либо строго обоснованные правила решения. Полагаться можно лишь на культуру мышления, кругозор, опыт и добросовестность составителей.

Для построения информационной модели указанные категории элементов – интересы, угрозы, проявления, показатели, источники угроз, виды ущерба и некоторых рисковых событий, объекты угроз должны быть объединены системой отношений. В особенности это касается угроз и интересов, поскольку между ними существуют перекрёстные связи влияния.

1.5. Задачи информационно-аналитического обеспечения

В основе решения задач информационно-аналитического обеспечения лежит мониторинг угроз и аудит ПОС, осуществляемые в регламентном режиме, а также информационное изучение и аналитическое осмысление возникающих ситуаций, к числу которых относятся появление новых участников рынков, появление или прогноз появления новой продукции, изменение структуры интересующих рынков, изменения социально-экономической, политической, деловой обстановки в регионах деловых интересов, назначения в государственных органах и органах местного самоуправления, готовящиеся сделки, приём на работу на предприятие новых сотрудников, чрезвычайные ситуации различного характера.

Задачи «контроля…» включают:

- анализ и сопоставление финансовых и экономических документов (бюджетный план, бюджет движения денежных средств, бюджет расходов и доходов, анализ рентабельности), документов бухгалтерского и налогового учёта, а также учёта расходования и эксплуатации материальных ценностей, движение финансовых средств на банковских счетах предприятия, договоров с контрагентами, смет, обоснований цен, бизнес-планов и т. п.;
- осмотр, исследование, измерение материальных ценностей, в том числе с использованием необходимых приборов, инструментов и препаратов, а также непосредственное или с помощью технических средств, в том числе в отложенном режиме, наблюдение порядка расходования, использования и движения материальных ценностей;
- добывание информации о вызовах, угрозах и рисковых событиях из общедоступных и эксклюзивных источников, под которыми понимаются, прежде всего, люди, их знания и мнения, рабочие записи, автоматическое документирование работы технических систем, электронная переписка по служебным каналам связи, а также поступки и взаимоотношения различных лиц, имеющие отношение к жизнедеятельности предприятия.

К числу информационно-аналитических задач относится также подготовка докладов и информационно-аналитических справок об удовлетворении интересов предприятия и состоянии его ПОС для

акционеров и исполнительных руководящих органов. Опыт практической работы показывает, что для полного охвата требуемого информационного пространства необходимо на регулярной основе решение следующих частных задач сбора и обработки информации:

- сбор регламентных данных о вызовах, угрозах и рисковых событиях в форме стандартизированных внутренними правовыми актами докладов и сообщений;
- анализ социально-экономической обстановки в регионах деловых интересов предприятия;
- анализ рынка труда в регионах деловых интересов предприятия;
- анализ тенденций потребления в интересующих секторах экономики;
- анализ структуры и предложений в интересующих секторах рынков;
- анализ тенденций развития науки, техники, технологий;
- изучение состояния и деятельности конкурентов;
- анализ производственных и других деловых процессов на предприятии;
- оценка и прогноз финансовой устойчивости предприятия;
- анализ социальной ситуации на предприятии;
- анализ хода судебных разбирательств с участием предприятия;
- анализ хода, направленности и результатов проверок предприятия, осуществляемых уполномоченными государственными органами;
- анализ добросовестности контрагента – поставщика, заказчика, партнёра; ведение реестра недобросовестных поставщиков;
- оценка финансовой устойчивости контрагента;
- оценка финансовой устойчивости кредитных коммерческих организаций (банков), с которыми планируется или осуществляется сотрудничество;
- изучение кандидата на работу на предприятие или на заключение гражданско-правового договора о сотрудничестве.

Важно отметить, что информационно-аналитическая работа должна быть организована таким образом, чтобы результаты всех перечисленных выше задач дополняли друг друга.

2. Формализованные подходы к анализу безопасного существования предприятия

Содержание задачи обеспечения безопасного существования в основных чертах на вербальном уровне было рассмотрено в разделе 1.3. Здесь предлагается конкретизация логики и формализованные подходы к оценке безопасного существования.

2.1. Методический подход к интегральному оцениванию безопасности предприятия

Оценка уровня безопасности хозяйствующего субъекта является одним из краеугольных камней деятельности по обеспечению его безопасности. С постановки и решения этой задачи следует начинать формирование или совершенствование системы обеспечения безопасности. Результаты этой работы фактически формируют мотивацию акционеров и руководства предприятия к построению и развитию системы обеспечения его безопасности, позволяют выявлять «тонкие» места в защите его ресурсов и интересов, прогнозировать ущерб, служат аналитической базой для рационального распределения средств на развитие системы обеспечения безопасности. При этом использование для оценивания формализованных числовых методов позволяет во многом «очистить» оценку от субъективизма и при разработке бюджета применять хорошо разработанные в теории и широко используемые в практике методы математического программирования.

Исходя из определения категории «безопасность», представленного в разделе 1.1, оценка уровня безопасности предполагает интегральную оценку потенциального ущерба хозяйствующему субъекту, который может быть ему нанесён в рассматриваемый период времени. Для этого необходимо каким-то образом сопоставить всю совокупность угроз предприятию, учитываемых в информационной модели безопасности предприятия и возможности по их парированию и(или) минимизации возможного ущерба.

Обобщённые структурные элементы механизма оценки безопасности предприятия следующие.

1. Составляется (идентифицируется) перечень угроз.

2. Определяется совокупность рисковых событий с учётом их возможного совпадения, повторения и т. п. Рисковые события определяются до уровня типов по отношению к объектам защиты и видам ущерба. Каждое рисковое событие идентифицируется триадой (объект защиты, вид ущерба, характер нанесения ущерба). Строится когнитивный граф рисковых событий. Для решения рассматриваемой задачи непосредственно важны не угрозы, а рисковые события.

3. Рассчитывается ожидаемый ущерб в результате рисковых событий с учётом их взаимного влияния. Другими словами, строится когнитивная графовая модель рисковых событий с учётом их взаимовлияния. В [80] подобная модель именуется «вирусной моделью рисков» или «моделью вирусного механизма распространения рисков».

4. Оценивается возможность ПОС предотвратить рисковые события или сократить ущерб, который они влекут.

5. Уточняется ожидаемый ущерб в результате рисковых событий с учётом их взаимного влияния и противодействия со стороны ПОС.

6. Рассчитывается интегральный риск как степень недостижения интересов.

Схема механизма оценки безопасности предприятия представлена на рисунке 6 [81].

Идентификация множества угроз

Перечень угроз задаёт тематику мониторинга неблагоприятных воздействий, позволяет организовать систематическую работу по совершенствованию методического обеспечения выявления угроз, отражению устойчивых связей в системе угрозы-ПОС-интересы в информационных моделях обеспечения безопасности, однако он не может быть единственно верным и исчерпывающим.

Во-первых, этот перечень может уточняться в соответствии с представлениями лиц, готовящих и принимающих решения, по месту и времени. Во-вторых, необходимо постоянно осуществлять анализ отношений внутри хозяйствующего субъекта и с внешней средой для

выявления новых (ранее невыявленных, неучтённых) угроз и вызовов. В отношении наукоёмких предприятий в числе последних особое место занимают научные открытия и технические прорывы, которые способны в считанные годы изменить всю технологическую систему производства, структуру рынка.

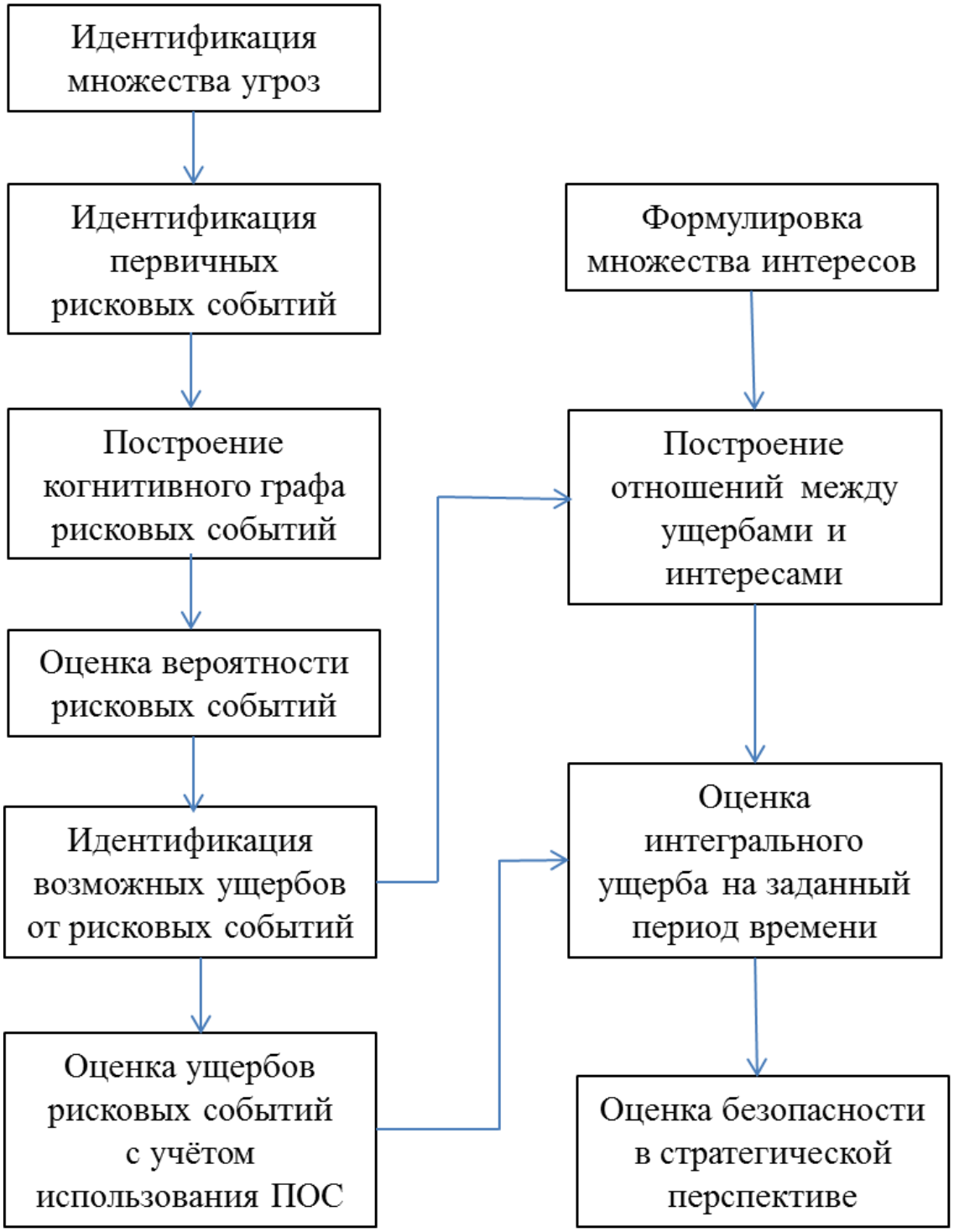

Рисунок 6 – Схема механизма оценки безопасности предприятия [81]

Идентификация первичных рисковых событий

Рисковое событие представляет собой деструктивное воздействие на какой-либо объект защиты. Одна и та же угроза из перечня угроз может приводить к различным рисковым событиям в зависимости от формы проявления угрозы. Рисковые события могут прогнозироваться, в том числе на основе статистики (для статистических угроз) и представляют собой свершившиеся факты.

Целесообразно установить отношения между множеством $\vec{U} = \|u_n\|$ угроз и множеством $\vec{S} = \|s_j\|$ рисковых событий, которые описываются матрицей вероятностей появления рискового события в результате актуализации угроз $\mathrm{P} = \|\rho_{nj}\| := \{\rho(s_j/u_n) \mid j \in J,\ n \in N,$ $0 \leq \rho \leq 1.$

Здесь $n=1,\ldots, N$ – условный порядковый номер угрозы из множества N, а $j=1, \ldots, J$ – условный порядковый номер рискового события из множества J.

Перечень рисковых событий так же, как и угроз, не является ни универсальным и незыблемым, ни исчерпывающим. В каждом конкретном случае может быть составлен перечень «по месту». При этом всегда надо предполагать возможность появления предварительно неописанных вариантов.

Рисковые события могут быть импульсными и приводить к разовому ущербу, а могут иметь продолжающийся характер. К первым, например, относится утрата ТМЦ, авария, ко вторым – повышение тарифов естественных монополий, снижение качества труда в результате деградации кадров или снижения зарплаты.

Построение когнитивного графа рисковых событий

Рисковые события могут порождать другие рисковые события неизбежно или с некоторой вероятностью, практически мгновенно или через некоторое время. В этих случаях возникает сценарий, совокупность сценариев или совокупность возможных сценариев развития ситуации возникновения ущерба.

В работе [80] предложена модель «вирусного» механизма распространения рисков на глобальном уровне, которая по сути

коррелирует с идеями в основании вирусной теории менеджмента [82], с «вирусной» теорией кадрового риска [83].

«Вирусный» механизм распространения рисков приводит к тому, что на конкретный объект защиты могут оказывать влияние риски, к которым он априори был нечувствителен. К рискам данного вида могут оказаться чувствительными другие объекты (или процессы для проектов), с которыми поддерживаются тесные связи. Если они находятся в состоянии близком к потере устойчивости, воздействие первичного рискового события может привести к формированию усиленной реакции всей интересующей системы, выражающейся в принципиальном изменении установившихся ранее связей.

«Вирусная» модель рисков, если её представить в виде графа, предполагает возможность контуров. Это означает, что в общем случае могут возникать ситуации лавинообразного развития кризиса за счёт процессов положительной обратной связи образования ущербов и существует возможность внешнего латентного управления путём формирования конкурентами или другими источниками угроз небольших воздействий в зонах повышенной чувствительности – выбор «слабого» звена в контуре, в котором воздействие можно осуществлять скрытно и рентабельно. С другой стороны, в контурах с учётом суперпозиции рисков могут возникать автоматические гашения деструктивной активности. Это означает, что объекты защиты, составляющие такой контур, находятся в надёжно стабильном состоянии. Следует иметь ввиду, что контуры в общей вирусной модели могут пересекаться.

Реализация вирусной модели механизма распространения рисков (когнитивной динамичной модели) требует:

- разработку моделей объектов защиты и их среды в виде графической модели взаимосвязи объектов защиты;
- разработку системы моделей влияния ущербов на одном объекте на риски для другого объекта (моделей передачи вируса, моделей заражения);
- разработку моделей динамики распространения ущербов;
- экспертные технологии для описания трудно формализуемых параметров и взаимосвязей.

Вирусный механизм демонстрирует необходимость использования развёрнутого описания сложных систем – итоговые результаты определяются не только исходным состоянием элемента, но и свойствами внешней среды, как глобальными, так и микроокружением элемента.

В настоящей работе предлагается интерпретация вирусной модели в виде графовой когнитивной динамической модели реализации угроз через рисковые события, учитывающей нелинейный характер накопления ущербов.

Когнитивная модель рисковых событий описывается взвешенным ориентированным графом. В узлах графа расположены рисковые события. Его рёбра соответствуют отношениям рисковых событий между собой, т. е. каждое ребро описывает влияние рискового события (реализации угрозы) в основании ребра на появление рискового события (возникновение и реализацию угрозы), которое находится в вершине ребра.

Учёт влияния имеет большое значение, т. к. от того, в какой степени угроза является причиной генерации рисковых событий, должен быть оценен приоритет действий по её предупреждению и (или) нейтрализации. Кроме того, взаимовлияние рисковых событий должно учитываться при прогнозировании нарастания угроз, которое может приобрести лавинообразный характер, как было отмечено выше. В монографии предлагается математическая модель описания такого влияния во времени.

Взаимное влияние рисковых событий описывается отношениями между ними, которые определяются величиной ущерба v и вероятностью его появления $\rho(v)$.

На множестве рисковых событий задаются отношения взаимовлияния, описываемые вероятностью появления i-го рискового события, если произошло j-ое. Взаимовлияние рисковых событий описывается матрицей $G = \|g_{ij}\| := \{g(s_i/s_j) | j \in J,\ i \in J, 0 \le g \le 1\}$, в которой каждый элемент $g(s_i/s_j)$ представляет собой условную вероятность наступления i-го события, если произошло j-ое.

В общем случае возможны альтернативные варианты сценариев развития последствий рисковых событий, т. е. распространение ущерба

от *j*-го рискового события к *i*-му может быть несовместимым с распространением ущерба от *j*-го события к некоторому *i*`-му. В случаях безальтернативности путей распространения «заражения» ущербом для задачи анализа безопасности вероятности «заражения», как правило, имеют значения 0 или 1.

Размер ущерба v_i при *i*-ом событии, возникшем в результате *j*-го события, описывается функцией $f(v_j,\ \vec{q}\ )$, где $\vec{q}$ – вектор параметров, описывающих «передаточную» функцию. В простейшем случае его размерность может быть 1. Вместо значений ущербов *v*, как правило, следует рассматривать их математические ожидания, законы распределения или некоторые интервалы возможных значений. Подробней это рассмотрено ниже.

Воздействия рисковых событий, как было отмечено выше, могут иметь импульсный характер, т. е. однократное нанесение ущерба и перманентный (продолжающийся во времени). В цепочке сценариев могут быть рисковые события обоих типов. Так, импульсное событие – авария, может привести к сокращению оборотных средств, утрате доли рынка и т. д. С другой стороны, снижение качества труда может привести к аварии, задержке сроков выполнения заказа, в том числе государственного.

Оценка вероятности рисковых событий

Оценка вероятности рисковых событий может осуществляться либо на основе статистики, либо с помощью расчётов, либо экспертным путём.

Третий случай возникает, когда для оценки не хватает предыстории и суждения о вероятности приходится выносить на интуитивном уровне. Здесь уместно использование лингвистических шкал оценивания вероятности по 5–7 градациям с последующей оцифровкой этих значений. Вероятно, наиболее подходящей для этого является шкала Харрингтона (таблица 1).

Идентификация возможных ущербов от рисковых событий

Строго говоря, ущерб бывает разного вида и это следует учитывать в модели наиболее общего характера. Однако в контексте безопасности хозяйствующего субъекта часто можно ограничиться только ущербом,

исчисляемым в денежных единицах. Ущерб может определяться на непрерывной области или дискретном множестве.

Для каждого рискового события существует своя модель оценки ущерба. Как правило, величина ущерба носит вероятностный характер, поэтому может быть оценена математическим ожиданием или верхней границей некоторого доверительного интервала.

Таблица 1 - Шкала Харрингтона и точечные оценки

Лингвистическое значение	*Численный интервал*	*Точечная оценка*
Очень высокая	]0,8; 1,0]	0,9
Высокая	]0,64; 0,8]	0,72
Средняя	[0,36; 0,64]	0,5
Низкая	[0,2; 0,36[	0,28
Очень низкая	[0; 0,2[	0,1

На данном шаге механизма оценки безопасности ущерб оценивается как имманентно присущий рисковому событию и пока не сопоставляется с интересами объекта защиты – предприятия.

Средне ожидаемый ущерб при j-ом рисковом событии, определённый на дискретном множестве возможных значений, вычисляется по формуле

$$\overline{v}_j = \sum_{m_j=1}^{M_j} v_j^{m_j} \cdot p_j(v_j) \qquad (1)$$

где m_j – условный порядковый номер возможного значения ущерба при j-ом рисковом событии.

Для ущерба, определённого на непрерывном множестве, используется формула:

$$\overline{v}_j = \int_0^{v_j^{max}} p_j(v_j)\, dv_j \qquad (2)$$

Для оценки верхней границы ущерба предлагается использовать эквивалентный энтропийный интервал изменения величины, который не требует субъективных данных для вычисления доверительных

интервалов и может быть применён абсолютно для всех законов распределения случайной величины.

Далее для упрощения записи индекс j опущен там, где нет необходимости идентифицировать параметры j-го рискового события от какого-либо другого.

Пусть H – энтропия распределения случайной величины, вычисляемая по формулам из теории передачи информации.

Для дискретного случая, предполагая, что значения ущерба выстроены по возрастанию, используется следующая формула:

$$H = H^- + H^+$$

$$H = -\sum_{m=1}^{m^c,\ v(m^c)\le\overline{v}} p(v_m)\cdot lnp(v_m) - \sum_{m^c,\ v(m^c)\ge\overline{v}}^{M} p(v_m)\cdot lnp(v_m) \qquad (3)$$

Здесь m^c – условный порядковый номер величины ущерба, при котором величина ущерба не превышает среднее значение ущерба.

Для непрерывного случая

$$H = H^- + H^+ = -\int_0^{\overline{v}} p(v)\cdot lnp(v)dv - \int_{\overline{v}}^{\infty} p\,(v)\cdot lnp(v)dv \qquad (4)$$

Верхняя граница эквивалентного интервала возможных значений ущерба $v^{\text{пр}}$ вычисляется по формуле

$$v^{\text{пр}} = exp(H^+) + \overline{v} \qquad (5)$$

Для каждого из объектов защиты можно провести расчёт критичности нанесения ущерба, определив несколько состояний, позволяющих целостно описать проблемы и сформировать шкалу для их учёта с точки зрения интересов субъекта (предприятия). В тех случаях, когда даже грубые модели конкретных рисков отсутствуют и не могут быть созданы, для анализа ущерба подобно техническим системам можно оценивать вероятность рискового события и влекомый им ущерб в соответствии с таблицей 2, используя экспертные оценки по лингвистической шкале.

Поскольку, как было определено выше, оценка безопасности определяется оценкой риска, то в клетках таблицы внесены лингвистические значения оценки обеспечения безопасности.

Принципиально меняются пороги при суперпозиции и трансформации систем рисков. Это объясняет все многолетние неудачи построения систем анализа рисков и обеспечения безопасности: при превышении порога кризис не наступал или, напротив, появлялся «чёрный лебедь».

Таблица 2 – Оценка последствий действия рисковых событий

Правила принятия решения	*Вероятность рискового события*					*Уровень ущерба*
	НВ	*МВ*	*ВС*	*ВВ*	*Д*	
Уровень риска	П	Н	Н	Н	Н	*КУ*
	С	П	П	П	П	*БУ*
	В	С	С	С	С	*СУ*
	А	В	В	В	В	*НУ*
	А	А	А	А	А	*МУ*

Примечания:

НВ – незначительная вероятность, МВ – маловероятно, ВС – вероятно (~ 50/50), ВВ – высокая вероятность, Д – очень высокая вероятность (почти достоверно);

КУ – критичный (недопустимо высокий) ущерб – существование вряд ли возможно; БУ – большой ущерб (существование проблематично), СУ – средний ущерб (существование возможно, но в неблагоприятных условиях); НУ – незначительный ущерб (интересы удовлетворяются в целом, но не идеально), МУ – практически не значимый (мизерный) ущерб - фиксируется, но почти не влияет на удовлетворение интересов;

Н – не обеспечена (практически не обеспечена), П – плохо обеспечена, С – обеспечена на среднем уровне, В – обеспечена на высоком уровне, А – обеспечена практически абсолютно.

Оценка ущербов рисковых событий с учётом использования ПОС

Оценка безопасности определяется не только наличием и реализацией угроз, но и возможностью объекта защиты предотвращать и парировать их, т. е. наличием и эффективностью применения ПОС.

Пусть r=1, …, R – условный порядковый номер некоторого действия по использованию ПОС из множества возможных действий R (далее – мера защиты).

Каждому j-му рисковому событию сопоставляется r-ая мера защиты. Эти отношения описываются матрицей $Z_j = \|z_{jr}\|$.

Многочисленные методы защиты, т. е. снижения и предотвращения рисков описаны в специальной литературе (см., например, [22, 28, 31-37]). Полный её объём в настоящее время необозрим.

Использование различных методов приводит к следующим альтернативным вариантам результатов защиты:

- уменьшение величины ущерба при сохранении его вероятности;
- уменьшение вероятности ущерба при сохранении его величины;
- «сдвиг влево кривой» плотности распределения вероятности ущерба.

Первый результат, как правило, является следствием компенсации ущерба и соответствует методу компенсации, передачи или распределения риска. Это может происходить, например, в результате получения страховых выплат после аварии, утраты имущества, стихийных бедствий и т. д. В этом случае рисковое событие не предотвращается. Защита заключается в ликвидации (минимизации) последствий.

Два другие результата являются следствием противодействия угрозам, предотвращения (полное или частичное) рискового события. К таким событиям относятся, например, срыв договорных обязательств со стороны контрагентов перед предприятием или в рамках проекта, ухудшение макроэкономической ситуации (рост индекса цен, рост тарифов естественных монополий, изменение курса валют, рост ставки рефинансирования и т. п.), появление новых акторов на интересующих рынках, появление новых конкурирующих товаров. В этих случаях использование ПОС может быть направлено, как на ликвидацию или ослабление связи между рисковыми событиями (предотвращение «заражения» риском) – фактически на предотвращение рискового события, так и на ликвидацию (уменьшение) его последствий. Например, наличие возможности привлечения альтернативного поставщика предотвращает срыв выполнения проекта.

Для формализованного описания уменьшения ущерба в результате использования ПОС необходимо ввести некоторые допущения, имеющие практическое значение:

- существуют ресурсы, специально предназначенные (зарезервированные) для определённых рисковых событий, например, страховой полис, специальные подразделения в организационно-штатной структуре, должностные обязанности и инструкции, роли исполнителей проекта, предусмотренные штрафные санкции и т. п.;

- существуют общие ресурсы, объём которых в общем случае ограничен;

- общие ресурсы выделяются по мере появления необходимости в соответствии с вероятностным характером возникновения рисковых событий;

- для нейтрализации (минимизации), предотвращения ущерба от рискового события выделяется весь необходимый для этого объём нужных ресурсов из состава общих ресурсов, если их объём на протяжении заданного интервала времени (год) ещё не израсходован;

- назначаемый (он же с организационной точки зрения требуемый) для предотвращения ущерба ресурс не может превышать некоторую долю величины ущерба в эквивалентных единицах, в противном случае, предотвращение бессмысленно; рекомендуемое соотношение – 2/3 от величины ущерба.

Пусть:

r=1, ..., R – условный порядковый номер меры нейтрализации ущерба при *j*-ом рисковом событии из множества R предусмотренных мер;

$\overrightarrow{z_j} = \|z_{jr}\|$ – вектор, отражающий наличие специальных мер для нейтрализации ущерба от *j*-го рискового события;

k=1, ..., *K* – условный порядковый номер вида общего ресурса ПОС из множества общих ресурсов K;

$\vec{Q} = \|Q_k\|$ – вектор запасов общих ресурсов ПОС; для рассматриваемой задачи эти ресурсы представляют собой, как правило, финансовые и материальные ресурсы, в отдельных случаях может идти речь о трудовых и иных ресурсах.

В результате использования специальных ресурсов ПОС для нейтрализации *j*-го рискового события ущерб уменьшается на величину $\Delta v_j = \vartheta\left(\overrightarrow{z_j}\right)$. Остаточный ущерб вычисляется по формуле

$$v_j^{\text{ПОС}} = v_j - \Delta v_j \qquad (6)$$

Здесь под v_j подразумевается $\overline{v_j}$ или $v_j^{\text{пр}}$.

Если $v_j^{\text{пос}} > \varepsilon$, где ε – величина незначительного ущерба, т. е. специальных мер по предотвращению ущерба от j-го рискового события недостаточно, то требуется дополнительно выделение ресурсов из общих запасов. В этом случае выражение (6) усложняется:

$$v_j^{\text{пос}} = v_j - \left(\vartheta\left(\overrightarrow{z_j}\right) * \varphi\left(q_{jk}^{\text{тр}}\right)\right) \cdot \frac{Q_k^{\text{тр}}}{Q_k} + \vartheta\left(\overrightarrow{z_j}\right) \cdot \frac{Q_k - Q_k^{\text{тр}}}{Q_k} \quad (7)$$

Здесь:

знак «*» означает композицию функций, которая на практике, обычно, является суммой;

$q_{jk}^{\text{тр}}$ – требуемый дополнительный ресурс k-го вида для нейтрализации ущерба от j-го рискового события;

$Q_k^{\text{тр}}$ – общий объём требуемого k-го ресурса для нейтрализации всех рисковых событий.

$$Q_k^{\text{тр}} = \sum_{j=1}^{J} q_{jk}^{\text{тр}} \quad (8)$$

Выражение (7) представляет собой математическое ожидание остаточного ущерба в зависимости от вероятности наличия дополнительных ресурсов. Вероятность наличия дополнительных ресурсов определяется соотношением их запаса на начало рассматриваемого периода оценки и суммарных потребностей в масштабе рассматриваемого объекта защиты.

Для упрощения принято, что в качестве дополнительного ресурса используется один вид наиболее необходимого и продуктивного ресурса для устранения (предотвращения) ущерба.

Формулировка множества интересов

Процесс формулирования интересов предприятия рассмотрен выше. Здесь можно уточнить, что в процессе оценки безопасности в качестве интересов могут использоваться основные задачи, стоящие перед предприятием.

Интересы формулируются таким образом, что они должны быть независимы по полезности, другими словами, достижение одного из них не должно влиять на отношение к степени удовлетворения другого [84].

Для унификации описания степени достижения интересов целесообразно нормировать степень их достижения одним интервалом, например, [0; 1]. Степень достижения может описываться строго, например, достижение заданных значений прибыли, или задаваться на качественном уровне по лингвистической шкале, когда физическая шкала для оценки степени удовлетворения интереса не существует или её использование затруднительно. При нормировании отрезком [0; 1] минимально допустимому значению присваивается значение 0, а максимально желаемому (установленному владельцами или государственными планами и заданиями) или практически возможному присваивается значение 1.

Соответствие качественных и количественных значений может быть установлено как в таблице 3.

Таблица 3 – Соответствие качественных и количественных значений степени достижения интереса по нормированной шкале

Качественное значение	*Количественное значение*
Практически удовлетворяется – существование обеспечивает полностью	]0.9; 1]
Удовлетворяется в целом – существование обеспечивает полноценно	]0.75; 0.9]
Удовлетворяются в основном – существование обеспечивает в основном	]0.6; 0.75]
Удовлетворяется недостаточно – существование обеспечивает недостаточно	[0.4; 0.6]
Удовлетворяется на низком уровне – существование обеспечивает на низком уровне	[0.25; 0.4[
Удовлетворяется минимально – существование обеспечивает на минимальном уровне	[0.1; 0.25[
Практически не удовлетворяется – существование не обеспечивает	[0; 0.1[

Построение отношений между интересами и ущербами

Основная задача и трудность этого этапа механизма оценки безопасности заключается в определении тех ущербов, которые

непосредственно оказывают воздействие на интересы во избежание «двойного счёта». Например, задержка поставок со стороны контрагента непосредственно не влияет на интересы проекта или предприятия, однако это может привести к задержке следующих этапов жизненного цикла продукции, к штрафным санкциям со стороны заказчиков и т. д. Вся эта цепочка «заражения» ущербами уже формализована в когнитивном графе рисковых событий. Авария серийного образца может не привести к существенным финансовым потерям вследствие получения страховых выплат, однако приводит к потере доверия со стороны потребителей. С другой стороны, авария при проведении испытаний может привести к удорожанию стоимости проекта, затягиванию его сроков, однако может и не отразиться на безопасности, если подобная ситуация предусмотрена в системе финансирования и страхования работ проекта.

Фактически на рассматриваемом этапе к когнитивному графу рисковых событий необходимо подключить узлы, отражающие интересы.

Пусть:

m=1, …, M – условный порядковый номер интереса из множества M интересов,

y_m – степень достижения m-го интереса.

Формально отношения между ущербами и интересами описывается функцией:

$$y_m = f(\vec{v}, \Theta) \tag{9}$$

Здесь:

$\vec{v} = \|v_j\|$ – вектор значений ущербов в результате рисковых событий; под v_j понимается или $\overline{v_j}$, или $v_j^{\text{пр}}$ в зависимости от выбранного подхода со стороны ЛПР;

$\Theta = \|\theta_{jm}\|$ – матрица соответствия интересов и ущербов от конкретных рисковых событий,

$$\theta_{jm} = \begin{cases} 1, \text{если } j-\text{ый ущерб влияет на } m-\text{ый интерес}, \\ 0, \quad \text{в противном случае} \end{cases}$$

Выражение (9) отражает влияние ущербов на интересы в наиболее общем виде, когда результат может быть описан композицией различных ущербов или какими-либо аналитическими выражениями,

однако в соответствии с природой ущербов в действительности, как правило, функция *f(·)* может представлять собой суммы финансовых потерь, суммы временных задержек. В других случаях, например, если в числе интересов «авторитет производителя», степень удовлетворения интереса может быть установлен на основе экспертного опроса. В целом количество вариантов функции *f(·)*, не сводимых к финансовым или временным потерям, может быть сколь угодно разнообразным. Если экспертные методы не удовлетворяют, в каждом конкретном случае необходимо разрабатывать модель оценки степени удовлетворения интереса от ущербов.

Для оценки удовлетворения интересов, имеющих финансовое (или временное) содержание может быть использована следующая модель.

Пусть:

Y_m^{max}, Y_m^{min} – максимальное и минимальное допустимые значения удовлетворения m-го интереса (например, размер дохода или прибыли).

В этом случае y_m можно рассматривать как нормированное значение:

$$y_m = 1 - \frac{Y_m^{max} - Y_m}{Y_m^{max} - Y_m^{min}} = 1 - \frac{Y_m^{max} - \sum_{j \in J^{\phi}} v_j}{Y_m^{max} - Y_m^{min}} \qquad (10)$$

Здесь J^{ϕ} – множество рисковых событий, которые приводят к прямому финансового ущербу, который ведёт к сокращению дохода (или прибыли).

Целесообразно при оценке безопасности (степени удовлетворения интересов) учитывать затраты на её обеспечение. В соответствии с парадигмой существования на обеспечение безопасного существования в сколь угодно продолжительной перспективе работает вся система менеджмента и реализации инновационных проектов предприятия. В связи с этим в рассматриваемой в этом разделе задаче для оценки затрат на обеспечение безопасности имеет смысл учитывать только те средства, которые зарезервированы или специально потрачены на предотвращение или компенсацию ущербов в результате возникших рисковых событий на рассматриваемом временном периоде – «специальное» задействование ПОС.

Пусть q^0 – нормированное значение затрат на обеспечение безопасности – «специальное» задействование ПОС, тогда уточнённое

нормированное значение финансового интереса y_m будет вычисляться по формуле

$$y'_m = y_m - q^0 \quad (11)$$

Разница $y_m - y'_m$ отражает факт существования угроз и необходимость их предупреждения. Она является основой для разработки решений о развитии сил и средств обеспечения безопасности в соответствии с экономической целесообразностью.

Оценка интегрального удовлетворения интересов на заданном периоде

Оценку интегрального удовлетворения интересов целесообразно осуществлять с использованием моделей теории полезности [70, 84].

В упрощённой форме допустимо использование средневзвешенной суммы удовлетворения совокупности интересов. Вычисление весовых коэффициентов целесообразно осуществлять с использованием моделей, предложенных в работах [70].

Интегральный нормированный показатель удовлетворения интересов (уровня безопасности) *y* вычисляется по формуле

$$y = \sum_{m=1}^{M} l_m \cdot y_m \quad (12)$$

Здесь l_m – коэффициент важности (замещения).

Оценка безопасности в стратегической перспективе

Предыдущие этапы механизма оценки безопасности описывают процедуры оценки на некоторый заданный период времени. Однако для стратегической оценки необходимо прогнозировать безопасность на достаточно длительную временную перспективу с учётом предпочтений к уровняю её обеспечения на различных этапах в будущем.

В качестве модели оценки используется аддитивная форма, объединяющая уровни безопасности на каждом интересующем этапе в будущем (по аналогии с функциями полезности). Расчёт коэффициентов, описывающих предпочтения ЛПР к обеспечению

безопасного существования в перспективе, проводится при следующих исходных посылках:

- предпочтения убывают по экспоненциальному закону;
- перспектива ограничивается 12 годами (два периода стратегического планирования, предусмотренного Федеральным законом от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации»);
- единичный период – 1 год.

Исходя из этого, коэффициенты рассчитываются по формуле

$$\varphi^t = e^{-\sigma \cdot t} \tag{13}$$

Параметр σ определяется по формуле

$$\sigma = -\frac{ln(1 - d_0)}{12} \tag{14}$$

Здесь d_0 – доля «внимания» эксперта при рассмотрении перспективы, которую он уделяет на принятую выше перспективу 12 лет.

Если принять, что d_0=0,99, то σ = 0,384.

Далее необходимо рассчитать значения φ^t для рассматриваемых моментов времени ($t \in [0; T]$). Практически целесообразно рассматривать t=0, 1, 2, 3, 6, 12.

Для того чтобы выдержать требование по согласованности шкал (здесь используются шкалы [0; 1]), рассматриваемые значения приоритетов φ^t необходимо нормировать также по шкале [0; 1]:

$$\varphi_n^t = \frac{\varphi^t}{\sum_{t \in [0:T]} \varphi^t} \tag{15}$$

Интегральное значение функции, отражающей оценку безопасности на временной перспективе от текущего года до года T, вычисляется по формуле

$$y^T = \sum_{t \in [0:T]} \varphi_n^t \cdot \sum_{m=1}^{M} y_m(t) \tag{16}$$

Ранжирование угроз

Ранги угроз определяют приоритетность деятельности по их предупреждению и парированию. В соответствии с целевым подходом ранг определяется тем, в какой степени соответствующая угроза снижает интегральную оценку безопасности. Для его определения необходимо сравнить значения интегральных оценок безопасности, получаемые для всей совокупности угроз и значения безопасности при отсутствии каждой из них. Разность значений является рангом угрозы, поскольку характеризует её «негативный вклад». Значения рангов могут быть отнормированы на каком-либо удобном для восприятия интервале.

Также как и оценки безопасности, ранги могут быть определены на текущий момент (единичный интервал анализа, например, год) и в масштабе стратегической перспективы.

Задача распределения ресурсов для противодействия угрозам является задачей дискретного программирования и может быть решена методом ветвей и границ для определения пакета угроз, подлежащих нейтрализации в рамках имеющихся для этого ресурсов. При существующих вычислительных мощностях даже ПЭВМ эта задача может быть решена методом простого перебора.

2.2. Оценка ущерба при «вирусной» модели его распространения в условиях аналитической неопределённости

Под аналитической неопределённостью понимается отсутствие объективной с точки зрения обоснования естественными закономерностями модели описания ущерба при *j*-ом рисковом событии, возникшем в результате некоторых других рисковых событий. При этом ущерб может накапливаться в соответствии с динамикой распространения («заражения»), отражаемой с выбранной тактовой частотой в изменениях состояний узлов направленного когнитивного графа рисковых событий. В случаях, если ущерб заключается в прямых финансовых потерях, он может элементарно суммироваться. Однако, если речь идёт о снижении уровня мотивации персонала, переменах во внешнеполитической обстановке, изменениях платёжеспособности потребителей и т. п., то влекомые подобными обстоятельствами ущербы не очевидны и могут быть оценены экспертным путём.

Предлагаемая в настоящем подразделе модель является экспертно-аналитической, позволяющей отразить общее состояние, прогноз и, главное, направленность динамики уровня безопасности в условиях множества разнохарактерных угроз и последствий их реализации при приемлемых трудозатратах на аналитическую и экспертную работу. Она использует универсальную эвристическую модель распространения и накопления ущерба и допускает высокую степень автоматизации в рамках информационной технологии и диалоговой экспертной работы, в том числе в режиме распределённого и удалённого доступа. С её помощью возможно определить критичные узлы в сети распространения рисков. Эти данные необходимы для планирования рационального развития ПОС и совершенствования механизмов его использования. Эта задача относится к задачам синтеза.

Область применения модели определяется наличием множества разнохарактерных трудноформализуемых угроз и, следовательно, рисковых событий и в наибольшей степени относится, с объектной точки зрения, к большим интеграционным хозяйствующим (социально-экономическим) образованиям, а с временно*й* – к моделированию состояния безопасности на продолжительном периоде. Такая модель используется, как правило, не для текущих оценок в конкретных ситуациях, а для выявления складывающихся тенденций.

Для построения модели приняты следующие посылки и допущения:

- ущерб накапливается с насыщением; накопление ущерба описывается логистической кривой;
- ущерб в результате каждого рискового события количественно описывается нормированным отрезком [0; 1], а численные значения интерпретируются по лингвистической шкале, примеры которой представлены выше;
- взаимное влияние угроз происходит с некоторой тактовой частотой; для настоящей модели целесообразно принять, что такт равен одной-двум неделям для проекта, месяцу для предприятия;
- воздействие нескольких рисковых событий на некоторое *i*-ое описывается как сумма их «вкладов» с учётом логистического характера накопления ущерба (см. первое допущение).

Выбор логистической кривой объясняется следующими соображениями. Распространение риска в общем случае аналогично процессу размножения в условиях ресурсных ограничений, который происходит по логистическому закону. В рассматриваемой задаче в результате воздействия исходного рискового события размножаются негативные микрособытия, или ущербы, формирующие производное рисковое событие, а в качестве ограниченных ресурсов выступают физически объективные возможности роста ущерба – не может быть ущерб более чем, например, стоимость объекта защиты, или сокращения выручки в результате потери сектора рынка, или увольнения всех работников и т. п.

Допущения, принятые в предлагаемой модели, позволяют учесть нелинейность характера влияния одного рискового события на другое и описывать накопление ущерба более адекватно, чем это позволяют линейные аддитивные структуры.

На основе изложенного может быть предложена следующая математическая модель взаимовлияния рисковых событий, которая позволяет прогнозировать значения ущербов в узлах когнитивного графа рисковых событий в различные будущие моменты времени с учётом взаимовлияния рисковых событий.

В модели используются следующие обозначения:

$\tau = 0, 1, \ldots, T$ – условный порядковый номер такта (единичного, элементарного временного интервала) изменения состояния пространства рисковых событий в интересующей предметной сфере – проект, предприятие; нулевой такт введён для последующей удобной записи исходного значения ущерба;

v_i^τ – значение ущерба в результате i-го рискового события, полученное на такте τ;

v_j^τ – значение ущерба от j-го рискового события после τ тактов;

β_{ji} – параметр, описывающий влияние j-ого рискового события на i-ое; этот параметр отражает корреляцию изменения ущерба при i-ом событии, которое произошло вследствие j-го рискового события; другими словами, β_{ji} отражает интенсивность наращивания ущерба;

$v_i^{\tau+1}(v_j^\tau;\ v_i^\tau;\ \beta_{ji})$ – величина ущерба при i-ом рисковом событии в результате воздействий на него j-го в (τ+1)-ом такте, распределённое по логистическому закону

$$v_i^{\tau+1}(v_j^\tau;\ v_i^\tau;\ \beta_{ji}) = \left(\frac{2exp(v_j^\tau \cdot \beta_{ji})}{exp(v_j^\tau \cdot \beta_{ji}) + 1} + 2v_i^\tau - 1\right) \cdot \frac{1}{1 + 2v_i^\tau} \qquad (17)$$

Параметр β_{ji} вычисляется, исходя из следующих условий:

если при значении v_j равном трети от максимума ущерб v_i достигает двух третей от максимума, то степень «передачи» ущерба – очень высокая и $\beta_{ji} = 4{,}83$;

если при среднем значении v_j ущерб v_i достигает три четверти от максимума, то степень «передачи» ущерба – повышенная и $\beta_{ji} = 3{,}89$;

если при среднем значении v_j ущерб v_i достигает также среднего значения (0,5), то степень «передачи» ущерба – средняя (прямая) и $\beta_{ji} = 2{,}19$;

если при среднем значении v_j ущерб v_i достигает значения в половину среднего, то степень «передачи» ущерба – пониженная и $\beta_{ji} = 1{,}02$;

если при среднем значении v_j ущерб v_i достигает значения в четверь среднего, то степень «передачи» ущерба – низкая и $\beta_{ji} = 0{,}39$;

Для учёта одновременного влияния на i–ое рисковое событие множества событий используется формула

$$v_i^{\tau+1}(v_j^\tau;\ v_i^\tau;\ \beta_{ji};\ J_i) = \left(\frac{2exp(\sum_{j\epsilon J_i} v_j^\tau \cdot \beta_{ji})}{exp(\sum_{j\epsilon J_i} v_j^\tau \cdot \beta_{ji}) + 1} + 2v_i^\tau - 1\right) \cdot \frac{1}{1 + 2v_i^\tau} \qquad (18)$$

где J_i – подмножество множества J, которое составляют рисковые события, воздействующие на i-ое, т. е. $J_i = \{j \mid \beta_{ji} \neq 0\}$.

Для прогнозирования рисков на заданную временную перспективу используется итерационная процедура. Этап процедуры (итерация) соответствует такту распространения ущерба. На каждом этапе процедуры рассчитываются значения всех ущербов, которые становятся исходными для расчёта значений на следующем такте с учётом импульсного или перманентного характера последствий и т. д.

При работе такой модели значения ущербов на каждом шаге следует уточнять по результатам их прогнозирования в зависимости от всей совокупности факторов, включая известные плановые.

2.3. Частные модели оценки основных проектных рисков

В настоящее время существует множество вариантов классификации рисков, включающих десятки позиций. В соответствии с принятой методологией (см. раздел 1.3) классифицировать следует не столько риски, сколько рисковые события, которые определяются угрозами. При этом сама классификация в практическом аспекте имеет смысл для организации мониторинга состояния безопасности и создания библиотеки моделей оценки рисков в результате рисковых событий.

Модели оценки рисков можно разделить на три класса: нормативные, экспертные и статистически-математические. Возможны комбинации классов. Например, изложенная выше модель оценки рисков с учётом взаимодействия рисковых событий предполагает, как математическую модель, построенную на эвристиках, так и экспертные оценки частных параметров, используемых в математических структурах.

Представить все модели частных рисков в рамках настоящей работы невозможно и нецелесообразно. Их большое количество можно найти в специальной литературе, например, [31-37, 85, 86]. Для практических целей следует разрабатывать различные модели и методики в рамках реализации информационной технологии оценки безопасности конкретного хозяйствующего субъекта в конкретных условиях его функционирования и пополнять библиотеку моделей и методик в процессе эксплуатации этой технологии. Ниже в качестве иллюстрации рассмотрены наиболее актуальные математические модели частных рисков применительно к проектам. Методы экспертного оценивания описаны в соответствующей тематической литературе, например, [87, 88].

Для наукоёмких, новаторских проектов высока степень неопределённости успешности результатов, объёма затрат и других проектных параметров. Это приводит к тому, что проекты, как правило, осуществляются поэтапно. По результатам выполнения каждого из

этапов принимается решение о возможности и целесообразности дальнейших работ. Возникшие проблемы реализации проекта, включая те, которые вызваны внешними угрозами, в том числе макроэкономического характера, рассматриваются как рисковые события, которые можно считать факторами реализации проекта. В зависимости от этих факторов может быть оценена функция распределения ущерба, который в зависимости от принятия решения по проекту и требований к его выполнению может описываться следующими показателями [35]:

- величина потерь, т. е. зря потраченный объём финансов, или недополученное финансирование на следующие этапы в случае прекращения проекта;
- увеличение затрат на проект;
- увеличение сроков реализации проекта, что может вести и к штрафным санкциям, и к имиджевым потерям (административным наказаниям), и к потере выручки (по коммерческим проектам).

Ниже будут рассмотрены частные модели оценки ущерба за счёт зря потраченных средств, потери финансирования при прекращении проекта, оценки увеличения затрат и оценки увеличения сроков.

Оценка риска зря потраченных средств

Пусть процесс выполнения проекта разбит на N этапов, а n – условный порядковый номер этапа n = 1, 2, …, N).[8]

Если вероятность успешного выполнения каждого из этапов равна p_n, то очевидно, что вероятность успешного выполнения проекта P равна:

$$P = \prod_{n=1}^{N} p_n$$

Вероятность срыва выполнения проекта $P_{ср}$ равна:

$$P_{\text{ср}} = 1 - \prod_{n=1}^{N} p_n$$

[8] Все обозначения в разделе 2.3 введены и используются исключительно в пределах этого подраздела монографии. Совпадения с обозначениями в других подразделах – непроизвольны, смыслом и ассоциациями не нагружены.

Вероятность срыва выполнения проекта после l этапов вычисляется по формуле

$$P(l) = \begin{cases} (1 - p_l) \cdot \prod_{n=1}^{l-1} p_n \text{ , если } l > 1 \\ (1 - p_l) \text{ , если } l = 1 \end{cases} \quad (19)$$

В случае финансирования выполнения проекта за счёт внутренних ресурсов математическое ожидание потерь в результате прекращения проекта вычисляется по формуле

$$\bar{Y} = \sum_{l=1}^{N} P(l) \cdot \sum_{n=1}^{l} (y_n - c_n) \quad (20)$$

где y_n – затраты на выполнение n-го этапа проекта, c_n – возможный положительный результат за счёт капитализации или реализации РИД (частичных или косвенных), полученных на каждом этапе.

Это оценка риска до начала проекта.

В действительности необходимость оценки возможного ущерба может возникать после некоторого (n-1)-го этапа в результате возникновения новых факторов вследствие рискового события. Тогда оценка возможного ущерба из-за срыва проекта на следующем этапе оценивается по формуле

$$Y(n) = \sum_{l=1}^{n-1} (y_l - c_l) + p_n \cdot (y_n - c_n) \quad (21)$$

Переоценка вероятностей p_n в результате рискового события приводит к переоценке ожидаемого ущерба на рассматриваемом периоде оценки безопасности. Если в этот период укладывается N* этапов проекта, начиная с n-го, то среднеожидаемый ущерб за счёт зря потраченных ресурсов, оцениваемый после (n+k)-го выполненного этапа ($n + k \leq N^*$), вычисляется по формуле

$$Y(n,\ n+k,\ N^*) = \sum_{l=n}^{n+k-1} (y_l - c_l) + \sum_{l=n+k}^{N^*} P(l) \cdot \sum_{m=n+k}^{l} (y_m - c_m) \quad (22)$$

Здесь $P(l)$ вычисляется по формуле

$$P(l) = \begin{cases} (1 - p_l) \cdot \prod_{m=n+k}^{l-1} p_m \ , & \text{если } l > n + k \\ 1 - p_l \ , & \text{если } l = n + k \end{cases} \qquad (23)$$

Оценка риска потери финансирования

Если финансирование осуществляется из внешних источников, то срыв проекта приводит к прекращению дальнейшего финансирования и сокращению входного денежного потока. В этом случае ущерб в период оценивания безопасности вычисляется по формулам, аналогичным (22) и (23):

$$Y(\, n + k, \ \ N^*) = \sum_{l=n+k}^{N^*} P(l) \cdot \sum_{m=l}^{N^*} y_{m+1} \qquad (24)$$

Здесь y_m – финансирование проекта на m-ом этапе. Значение y_{N^*+1} для вычислений по формуле (24) принимается равным 0, поскольку этот этап выходит за рассматриваемый период оценки безопасности.

Оценка риска удорожания проекта

Пусть:

Δy_n – удорожание проекта на n-ом этапе;

n=1, …, N – условный порядковый номер этапа проекта, каждый из которых планируется выполнять в период, на котором оценивается безопасность.

Если факторы, влияющие на удорожание, механизм и степень их влияния, достаточно детерминированы, то удорожание может быть вычислено путём прямого пересчёта. В более сложных случаях, когда выделяются варианты действия факторов, удорожание может быть вычислено как математическое ожидание результатов действия таких вариантов или их верхняя граница.

Когда имеет место аналитическая неопределённость воздействия рискового события, повлекшего факторы удорожания, подходящей аналитической структурой удорожания на некотором n-ом этапе может быть экспоненциальный закон распределения величины удорожания:

$$f(\Delta y_n) = 1 - e^{-\sigma_n \cdot \Delta y_n} \quad (25)$$

где σ_n – параметр, закона распределения роста затрат на проект на каждом n-ом этапе.

Выбор экспоненциального закона распределения объясняется следующим. Удорожание проекта в общем случае неопределённости определяется удорожанием различных работ, услуг, продукции поставщиков по различным причинам, в том числе в результате ошибок прогнозирования их стоимости, т. е. в результате некоторых первичных причин. Общее удорожание определяется набором таких первопричин. Предполагая их появление независимым друг от друга, можно считать, что их количество распределено по закону Пуассона. Соответственно, по этому же закону будет распределено значение удорожания, если полагать, что каждая первопричина влечёт некоторое усреднённое значение удорожания.

Математическое ожидание удорожания в этом случае равно $1/\sigma_n$.

Параметр σ_n и соответственно математическое ожидание удорожания можно вычислить из следующего условия

$$1 - e^{-\sigma_n \cdot y_n} = p_n^0 \quad (26)$$

где p_n^0 – некоторое значение вероятности, с которой затраты на n-ый этап выполнения проекта удвоятся. Аналогично можно задать условия, что затраты возрастут на четверть, в полтора раза, утроятся и т. д. в зависимости от удобства восприятия.

Из выражения (26) получается, что риск удорожания всех этапов проекта, т. е. проекта в целом, может быть вычислен по формуле

$$\Delta\bar{Y} = -\sum_{n=1}^{N} \frac{y_n}{ln(1 - p_n^0)} \quad (27)$$

Оценка риска задержки выполнения проекта

Среднеожидаемая задержка выполнения проекта вычисляется аналогично. Эти расчёты проводятся, если существует возможность рассчитать конкретную задержку из-за конкретных факторов, например,

практически достоверно прогнозируемой задержки поставок. В ситуации аналитической неопределённости можно использовать формулу аналогичную (27), подставив в неё вместо y_n величину задержки *n*-го этапа $\Delta\tau_n$.

$$\Delta\bar{T} = -\sum_{n=1}^{N} \frac{\tau_n}{ln(1-p_n^0)} \tag{28}$$

Если задержка выполнения проекта влечёт какие-либо потери *u*, например, недополученная прибыль, дополнительные расходы (аренда, зарплата, др.), штрафы и т. п., то среднеожидаемый ущерб $\bar{Y}$ в финансовом измерении равен:

$$\Delta\bar{Y} = \Delta\bar{T} \cdot u = -\sum_{n=1}^{N} \frac{\tau_n \cdot u}{ln(1-p_n^0)} \tag{29}$$

Здесь *u* должно вычисляться с учётом дисконтирования. При этом ставка дисконтирования может назначаться в соответствии с банковской кредитной ставкой, нормативной рентой на капитал предприятия или исходя из других соображений, вытекающих из финансовой политики предприятия.

2.4. Механизм оценки безопасности предприятия в режиме использования автоматизированной информационной технологии

Схема общего механизма оценки безопасности, представленная на рисунке 6 в разделе 2.1 для иллюстрирования структуризации проблемного поля разработки методологии, требует интерпретации и детализации некоторых аспектов с точки зрения реализации методологии оценки и её внедрения в практику деятельности.

Отличительной особенностью предложенной методологии является её ориентация на учёт конкретной специфики деятельности, отказ от простых, обобщённых до примитивности подходов в пользу более тонких многоаспектных моделей и методик, учитывающих взаимосвязи объектов онтологии проблематики безопасности, позволяющих осуществлять прогноз, использующих глубинные особенные знания экспертов по множеству узких вопросов и, в конечном итоге, учитывать нелинейность процессов, влияющих на

обеспечение безопасности, их масштабируемые и немасштабируемые результаты, выявлять «чёрных лебедей», учитывать вероятностную и невероятностную недетермированность различных явлений и взаимосвязей. Применение такой методологии ввиду необходимости оперирования большим количеством исходных данных и алгоритмов их обработки предполагает использование автоматизированной информационной технологии, снабжённой дружественным интерфейсом, системой управления знаниями, банком данных и знаний, библиотекой моделей, прецедентов и ситуаций, имеющей разнообразные возможности адаптации к конкретному объекту защиты, предлагающей возможность анализа и оценки состояния безопасности в режиме сценариев.

Автоматизированная информационная технология позволяет реализовать имитационное моделирование воздействия угроз, образования ущербов и их распространения в соответствии с «вирусным» механизмом.

Имитационное моделирование

Имитационная модель позволяет использовать всю доступную информацию вне зависимости от формы представления и степени формализации, что приобретает особую значимость при отсутствии надёжной статистической базы и достоверных знаний о структуре исследуемых объектов, а также когда они не могут быть адекватно описаны только с помощью аналитических математических моделей. Имитационное моделирование позволяет исследовать сложные производственные системы, подверженные разным угрозам. Не существует аналитических моделей поиска оптимальных структурных решений, поскольку структура – это форма, а форма принципиально не может быть описана числом. Ввиду уникальности подобных решений для крупных предприятий и их интегративных структур не может здесь помочь и статистика. В связи с этим для анализа влияния реструктуризации на различные аспекты функционирования отрасли, предприятия, включая их безопасность, невозможно найти достойную замену имитационному моделированию.

Для имитационного моделирования широко применяются потоковые модели, представляющие функционирование предприятия в

виде схем финансовых и материальных потоков, а также потоков рисковых событий и их последствий. Имитационные потоковые модели предприятия, включая технологические и финансовые потоки, могут быть разработаны в одной из широко используемых ныне программных сред структурно-функционального или потокового моделирования.

Имитационная модель может воспроизводить динамику функционирования хозяйствующего субъекта за несколько базовых периодов и генерировать многочисленные варианты реализации для каждого периода. При этом имитация может осуществляться по принципу фрактальных структур – от частных реализаций некоторого рискового события до уровня исследования статистических параметров состояния безопасности хозяйствующего субъекта любого масштаба.

После того, как модель построена, происходит генерирование сценариев развития системы для различных неблагоприятных событий. На этом этапе вычисляются численные оценки, как отдельных видов риска, так и интегрального значения по всему предприятию.

Имитационная модель безопасности предприятия позволяет получать интегральные оценки риска методом статистических испытаний Монте-Карло. Все необходимые функции для генерирования матриц случайных чисел с заданной структурой ковариации имеются в любом статистическом пакете или в специализированном пакетах для анализа рисков.

На основе имеющихся ретроспективных, расчётных и экспертных данных, а также информации о характере функционирования системы предприятие-среда можно задать основные факторы риска – рисковые события и ущербы в виде псевдослучайных величин с заданным распределением. Затем в результате многократного применения модели на данном массиве данных получаются квазистатистические и (или) расчётные квазивероятностные распределения и их моменты значений частных и интегрального рисков на рассматриваемом временном интервале.

Уровень доверия (вероятности попадания значений риска в доверительный вариант) при этом выбирается исходя из предпочтений ЛПР по точности удовлетворения интересов предприятия.

Полученные в результате имитационного моделирования численные оценки риска могут служить критериями оценки эффективности управления рисками и выбора оптимальных решений.

Во многих ситуациях, характеризующихся сложностью исследуемых процессов и недостатком надёжной информации, имитационное моделирование, интегрированное с предлагаемой методологией оценки безопасности, является единственным действенным инструментом её оценки.

Идентификация угроз и рисковых событий

Идентификация угроз осуществляется в результате мониторинга угроз и рисковых событий. Мониторинг проводится на основе рубрикатора угроз и рисковых событий, который содержится в базе знаний угроз и рисковых событий. Этот перечень является тематическим рубрикатором для осуществления мониторинга. В каждом конкретном случае угроза и рисковое событие имеют конкретное содержание. Кроме того, следует учитывать, что указанный перечень не является исчерпывающим, поскольку невозможно априорно учесть все возможные обстоятельства и сценарии нанесения ущерба ресурсам крупного хозяйствующего субъекта.

При выявлении угроз или возникновении рисков, не предусмотренных рубрикатором, они индексируются и вносятся в базу данных.

Для оценки безопасности на некотором рассматриваемом интервале времени необходимо учитывать не только возникшие рисковые события, но и прогнозируемые с некоторой вероятностью.

Для мониторинга используются внутренние и внешние источники информации и данных.

К внутренним источникам относятся система плановой отчётности о состоянии различных объектов, ресурсов, отношений и процессов, а также оперативные сообщения, как регламентированные, так и нерегламентированные от ответственных лиц или любых лиц. Кроме того, при наличии технической возможности используются сигналы в различной форме, параметрическая, звуковая и видео информация от технических систем контроля, наблюдения, установленных на объектах,

встроенных в технологические циклы и внутренние телекоммуникационные системы.

Внешние источники информации, как правило, предоставляют сведения о состоянии экономики, глобальных и региональных рынках, достижениях научно-технического прогресса, действиях и решениях государственных регуляторов, социально-экономической обстановке в регионе деловых интересов, военно-политической обстановке, состоянии и намерениях поставщиков и потребителей. К внешним источникам относятся средства массовой информации, глобальные телекоммуникационные сети, деловые контакты, информация государственных и муниципальных органов, отраслевые издания, в том числе электронные. Для их обработки целесообразно использовать автоматизированные технологии обработки потоков неструктурированной информации.

Реализация механизма расчёта ущербов и их распространения с использование графовой модели воздействия на объект защиты

Первоначально целесообразно построить наиболее вероятный нагруженный, ориентированный граф распространения рисковых событий («вирусный» механизм распространения ущербов). Удобно это делать в диалоговом режиме, используя модель потоков ресурсов и отношений в системе предприятие – среда. Этот граф в дальнейшем может использоваться для прогнозирования и в качестве опорной модели при реализации каких-либо ситуаций возникновения рисковых событий.

Графовая модель строится поэтапно. Каждый узел графа представляет собой пару: объект защиты – рисковое событие. Таким образом, одному объекту (например, склад №…, или технологический участок №…) может соответствовать несколько узлов. С другой стороны, поскольку большинство рисковых событий может быть разбито по определённым типам, одному типичному событию также может соответствовать несколько узлов.

Вначале между узлами устанавливается сам факт связи. Связь означает, что одно рисковое событие влечёт за собой появление другого (не исключено, что на том же самом объекте). Далее связь нагружается кортежем: вид ущерба (возможно, несколько), вероятность и величина.

Последняя пара может задаваться в виде функции распределения или плотности распределения случайной величины – ущерб.

Для оценки размеров и вероятностей ущербов могут использоваться модели из библиотеки моделей, экспертные процедуры.

Для моделирования «вирусного» механизма распространения устанавливается длительность такта, определяется вид ущерба или рискового события в исходящем узле – одноразовое воздействие (склад сгорел) или продолжающееся (утрата сектора рынка, задержка выполнения проекта, снижение качества из-за сокращения зарплаты и ухудшения качестве кадров). Для каждого из входящих узлов определяется: сохраняется ли остаточный ущерб после предыдущего такта или нет. Далее для каждого входящего узла вычисляется новое значение ущерба экспертным путём, по специальной модели из библиотеки или с помощью расчётного алгоритма, предложенного в разделе 2.2.

Для каждого узла задаётся «сопротивление» ущербу со стороны ПОС и вычисляется остаточный ПОС для расходуемых видов ресурсов.

Описанные действия и выбор способов и методов получения численных данных проводится на первой итерации, включающей начальное задание рисковых событий и ущербов в какой-либо момент и их распространение через один такт. В дальнейшем алгоритм может повторяться столько раз, сколько тактов вмещает период времени, на котором оценивается экономическая безопасность.

Вероятности появления и распространения ущербов по сетевой модели объекта защиты при реализации имитационного моделирования могут задаваться для каждой многоитерационной процедуры с помощью датчиков случайных чисел.

Для формулировки интересов, построения отношений между ущербами и интересами, а также моделирования предпочтений для моментальных оценок безопасности на протяжении периода оценки целесообразно использовать встроенные инструментальные средства – коммерческие пакеты или специально реализованные – для оценки альтернатив при многих критериях и предпочтениях в условиях неопределённости, экспертного группового оценивания.

Общая структурная схема механизма оценки безопасности хозяйствующего субъекта с использованием информационной технологии представлена на рисунке 7.

Центральным звеном является ассоциатор, который управляет всей логикой и механизмами оценки. В Базе данных и знаний содержатся сведения об интересах, угрозах, рисковых событиях, ущербах, статистика, прецеденты, описания ПОС, история расчётов и оценок, промежуточные результаты анализа, выходные формы документов.

Кроме того, технология должна включать неуказанные на рисунке программные модули для реализации функций технического обеспечения сопряжения с другими программно-инструментальными средствами, конвертации файлов различных форматов и т. п.

Рисунок 7 – Общая структурная схема информационной технологии оценки безопасности [81]

2.5. Модель аудита потенциала обеспечения существования предприятия

Косвенно аудит ПОС отражает возможности обеспечения нейтрализации угроз, и поэтому он может быть использован для оценки безопасности в качестве более простой методологии, чем построение когнитивного графа и прямой учёт использования ПОС для снижения ущербов, когда применение таких методик и моделей по каким-либо причинам слишком затруднительно или невозможно.

Аудит ПОС должен ответить на три вопроса:

- какие силы и средства используются (привлечены) для обеспечения безопасности?
- достаточен ли уровень ПОС по отдельным составляющим (компонентам)?
- каков интегральный уровень ПОС?

Ответы на первые два вопроса могут служить как для анализа состояния безопасности хозяйствующего субъекта и подготовки предложений по её укреплению, так и при проведении Due Diligence.

Интегральная оценка состояния ПОС может быть использована в тех случаях, когда требуется рационально распределить ресурсы, выделенные на развитие сил и средств обеспечения безопасности. В этом случае интегральная оценка является целевой функцией, а ресурсы следует израсходовать (распределить между компонентами ПОС) таким образом, чтобы обеспечить её максимизацию. Кроме того, такая оценка может быть полезна для характеристики общей картины состояния сил и средств обеспечения безопасного существования, анализа её динамики и аргументации предложений по выделению средств для укрепления состояния безопасности.

Аудит ПОС предполагает объективное описание существующих реалий, для чего необходимо, прежде всего, составить полный перечень позиций, подлежащих рассмотрению, и скрупулёзно их заполнить. Для этого может быть использована «Карта обследования ПОС» (см. Приложение). Эта карта не может быть исчерпывающей, поскольку существует большое количество различных сил и средств для обеспечения безопасности и к каждому конкретному объекту защиты эти силы и средства должны быть соответствующим образом

адаптированы. Она является типовой и отражает наиболее полное множество распространённых компонент ПОС.

Карта служит для характеристики наличных сил и средств, для оценивания обеспечиваемого ими потенциала существования, а также для рекомендаций эксперту: каким образом лучше собрать сведения о ПОС. Аудит проводится по множеству показателей, которые отражают наличие организационных структур, регламентирующих документов, технических средств контроля и защиты и т. д. Для оценивания приведены ориентировочные значения по лингвистической (описательной) шкале и соотнесённые им численные значения из интервала [0; 1]. Последние нужны для того, чтобы в дальнейшем иметь возможность сопоставления различных компонент потенциала между собой и с требуемым уровнем обеспечения безопасности. При этом лингвистические значения ПОС сформированы с учётом целевого эффекта, на который направлено применение тех или иных сил и средств - компонент ПОС.

Приведённые в третьем столбце Карты значения целевых показателей носят рекомендательный характер и могут назначаться по усмотрению аудитора (эксперта).

Для достижения большей объективности целесообразно к оцениванию привлекать нескольких специалистов и затем выводить групповые экспертные оценки.

Для интегрального оценивания состояния ПОС можно использовать два вида оценок – абсолютные и относительные.

Абсолютная оценка отражает уровень оснащения предприятия силами и средствами обеспечения существования в сравнении с максимальным уровнем, когда все численные значения оценки компонент ПОС (см. третий столбец в «Карте обследования ПОС») принимают значения равные «1». Такая оценка не учитывает ни требования к ПОС, ни уровень угроз.

Относительная оценка, наоборот, призвана соотнести состояние ПОС с некоторым требуемым уровнем и поэтому имеет большее практическое значение.

Для определения требуемого уровня ПОС возможны три подхода:

- требования определяются на основе анализа угроз и рисков, в том числе с учётом их прогноза – объективный[9] подход;

- требования выдвигаются руководством предприятия (т. е. ЛПР); это субъективный подход;

- требования диктуются положениями правовой нормативной базы – нормативный подход.

Формулирование требуемого уровня ПОС при субъективном подходе предполагает выяснение и описание образа состояния обеспечения безопасного существования в представлении ЛПР. Сложность решения этой задачи зависит от того, насколько ясно ЛПР представляет себе этот образ, а также, с практической точки зрения, насколько оно доступно для интервьюирования специалистами, проводящими аудит. Если ЛПР имеет сложившееся мнение о качественных параметрах сил и средств обеспечения безопасности, то задача сводится к формализованному описанию этого мнения и сопоставлению ПОС с требованиями ЛПР. Для решения таких задач существуют хорошо разработанные методы, один из которых описан ниже. Корректность решения определяется тем, насколько адекватно представление ЛПР о требуемых параметрах ПОС объективному положению вещей.

На практике ЛПР не всегда имеет правильное представление об объективных потребностях обеспечения безопасности, соотносимых с необходимыми для их удовлетворения затратами. Следует отметить, что руководитель хозяйствующего субъекта зачастую выдвигает требования, руководствуясь аналогиями с подобными производственными объектами, соображениями имиджа и т. д., что не всегда хорошо отражает объективные потребности. В силу этого возникает непростая задача подготовки мнения ЛПР на основе, если не научной обработки, то хотя бы экспертного анализа имеющихся данных об уровне угроз.

Нормативный подход к определению требований к ПОС заключается в том, что уровень обеспечения безопасности и некоторая совокупность мер и способов диктуются требованиями нормативной

---

[9] Здесь наименование «объективный» достаточно условно, поскольку доля субъективизма при анализе угроз, конечно, присутствует всегда, но её размер обратно пропорционален глубине и строгости анализа.

правовой базы.[10] Это касается, в частности, предприятий, использующих радиоактивные, взрывчатые, сильнодействующие ядовитые вещества и т. п., работающих со сведениями, составляющими служебную и(или) государственную тайну, прибегающие к услугам вневедомственной охраны МВД России и др. Так, органы вневедомственной охраны МВД России берут под свою опеку лишь те объекты, которые оборудованы в соответствии с требованиями, установленными в нормативных документах об оказании услуг по охране коммерческим организациям. К предприятиям, участвующим в выполнении государственного оборонного заказа, предъявляются требования уполномоченных государственных органов, отраслевые требования в части, касающейся обеспечения защиты от несанкционированного доступа, защиты ТМЦ, финансовой устойчивости и т. д.

Выбор подхода к определению требуемого уровня ПОС осуществляется исходя из особенностей, присущих каждому конкретному случаю проведения аудита, и зачастую является комбинацией трёх указанных подходов, диктуемой конкретными условиями деятельности и уровнем информационно-аналитической проработки вопросов обеспечения его безопасного существования.

Для численной интегральной оценки ПОС используется показатель степени соответствия уровня защиты предъявляемым требованиям – *D*, вычисляемый по формуле:

---

[10] Методическое пособие «Порядок обследования объектов, принимаемых под охрану» (утв. Главным управлением вневедомственной охраны МВД России 16 декабря 1997 г.).

Руководящий документ МВД РФ РД 78.36.003-2002 «Инженерно-техническая укреплённость. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств» (утв. МВД РФ 6 ноября 2002 г.).

Приказ МЧС РФ от 3 марта 2005 г. N 125 «Об утверждении Инструкции по проверке и оценке состояния функциональных и территориальных подсистем единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций».

Приказ МЧС РФ от 18 июня 2003 г. N 313 «Об утверждении Правил пожарной безопасности в Российской Федерации (ППБ 01-03)».

«Типовые требования по технической укреплённости и оснащению средствами охранно-пожарной сигнализации помещений с хранением наркотических средств».

Федеральный закон от 21 декабря 1994 г. N 69-ФЗ «О пожарной безопасности».

Единые требования по технической укреплённости и оборудованию сигнализацией помещений касс предприятий (с изменениями от 26 февраля 1996 г.).

$$D = \sum_{h=1}^{H} \frac{d_h}{d_h^{\text{тр}}} \cdot k_h \qquad (30)$$

Здесь:

h=1, …, H – условный порядковый номер компоненты ПОС (показателя оснащённости сил и средств защиты) из множества компонент, приведённых в Карте;

d_h – значение h-го показателя оснащённости;

$d_h^{\text{тр}}$ – требуемое значение h-го показателя оснащённости;

k_h – коэффициент важности h-го показателя.

Коэффициент важности k_h отражает «цену вопроса» укрепления h-ой компоненты ПОС и в связи с этим должен определяться на основе риска, для предотвращения которого служит (предназначена) рассматриваемая h-ая компонента. Однако практически сопоставить все компоненты с оценками рисков весьма трудоёмко и зачастую невозможно. Во-первых, отношения между множеством рисков и множеством компонент ПОС, как уже было отмечено выше, не являются бинарными (парными) отношениями, т. е. один риск может быть связан с несколькими компонентами и, наоборот, состояние некоторой компоненты может повлечь несколько рисков. Во-вторых, ПОС по своей природе влияет на потенциальные риски, которые с трудом поддаются объективной оценке по финансовому показателю (или какому-либо другому универсальному физически измеряемому показателю).

В связи с этим для практических целей коэффициенты важности компонент ПОС могут быть определены по методикам, изложенным в [70], в том числе рассматриваться как коэффициенты замещения, используемые в теории полезности. Однако в виду большой размерности H целесообразно использовать метод попарного сравнения. Учитывая большое количество коэффициентов, практически целесообразно определить значения для 5–7 наиболее важных компонент. Для других компонент установить пороги и использовать сатисфакционный критерий превышения порога.

Требуемые значения $d_h^{\text{тр}}$ могут быть определены с использованием следующих рекомендаций.

В Карте в правом столбце указаны возможные значения состояния компоненты ПОС.

Пусть каждая h-ая компонента имеет W_h возможных значений d_h^w, где w=1, …, W_h, причём с возрастанием условного номера w возрастает значение d_h^w .

Каждому значению d_h^w соответствует некоторое множество $S_h^w \subset S_h$ возможных s_{jh}^w-ых рисковых событий, которое может быть с очень высокой (близкой к 1) вероятностью предотвращено с помощью h-ой компоненты, если она имеет w-ое значение.

Исходя из этого, состояние (уровень оснащённости) h-ой компоненты $d_h^{\text{тр}}$ должно быть таким, которое позволит нейтрализовать все рисковые события в сфере «ответственности» h-ой компоненты кроме тех, вероятность появления которых меньше некоторого заданного значения χ. В формальной записи это выглядит следующим образом: $p\left(\forall s_j \mid s_j \in S_h \backslash S_h^w\right) \leq \chi$.

Для помощи ЛПР в определении величины χ можно предложить ему сравнить неблокируемое надёжно рисковое событие с некоторым более привычным аналогом, вероятность которого может быть определена статистически или воспринимается интуитивно.

3. Оценка потенциала финансовых ресурсов предприятия

В некоторых случаях при нехватке времени, исходной информации, а порой и узости методологического взгляда на проблему оценки безопасности она подменяется экономической безопасностью, а эта в свою очередь – финансовой безопасностью или устойчивостью. Рациональное зерно в этом есть, поскольку финансовые ресурсы являются системообразующие в ПОС. Они с разной скоростью могут быть конвертированы по сути в любой вид ресурса. Их недостаток запускает механизмы сокращения других ресурсов, а наличие, наоборот, является необходимым условием развитие всего ПОС. Достаточность или дефицит финансовых ресурсов прямо связан с широко используемой категорией «финансовая устойчивость».

3.1. Подходы к анализу финансовой устойчивости предприятия

Общие методологические положения исследования финансовой устойчивости предприятия

Теоретический подход к определению категории «устойчивость» был рассмотрен в подразделе 1.2.

В настоящее время существует множество различных вариантов определения финансовой устойчивости (далее – ФУ) предприятия [89-91]. Однако ни один из опубликованных подходов к формулированию рассматриваемого объекта исследования не удовлетворяет полностью, поскольку не позволяет вывести искомую дефиницию как частный случай из общесистемного понимания, изложенного выше. Используемые исследователями формулировки отличаются избыточностью, как правило, явно не отражают эмерджентность и ингерентность предприятия как системы с точки зрения финансов, оперируют неоднозначными субъективными оценочными категориями, например, «нормальное функционирование».

Множественность подходов к определению понятия ФУ имеет как субъективное, так и объективное объяснение. Последнее связано с тем, что финансовый аспект существования и деятельности предприятия может рассматриваться под разными углами зрения, с разными целями, применительно к разной временной перспективе. На основании

обобщения различных позиций авторов Е.Г. Моисеева и М.А. Грязева провели классификация типов и видов ФУ по шестнадцати! основаниям [92]. Составленная типология позволяет глубже разобраться в содержании этой экономической категории, его разночтениях и более рационально организовать анализ и управление ФУ.

Авторы указанной работы предлагают ввести в типологию также понятие потенциальной ФУ в связи с тем, что существующие подходы основаны, в основном, на изучении бухгалтерской отчётности и не учитывают возможности предприятий по оптимизации и улучшению своей ФУ. Однако представляется, что использование понятия потенциальная ФУ и, как следствие, разработка методов её определения малопродуктивно. Известные методы оценки ФУ как раз предоставляют информацию именно о потенциале предприятия по расплате с кредиторами, контрагентами и персоналом. Этот потенциал в общем случае может быть увеличен, однако, видимо, не бесконечно. Верхняя граница улучшения ФУ определяется ёмкостью рынка потребления, производственными возможностями предприятия, а также задачами по развитию производства и бизнеса в целом. Стремление к предельному (потенциальному, согласно [92]) значению ФУ – антитеза развитию. Вычисление этого предела имеет, скорее, теоретический интерес, чем практическую ценность. Другое дело, что для оценки ФУ, тем более на уровне стратегического планирования деятельности, явно недостаточно оценивать ФУ по состоянию баланса. Такие оценки никак не учитывают динамичное влияние внешней среды.

Как уже отмечалось в главе 1, хозяйствующий субъект в целом и его финансовые ресурсы, в частности, следует рассматривать как открытую систему, функционирующую в условиях нестабильной внешней среды. При этом смысл поддержания устойчивости хозяйственной системы не в том, чтобы обеспечить устойчивость любой ценой, а связать её с эффективными хозяйственными механизмами [93].

Прогнозирование и моделирование этого влияния на финансы предприятия позволит оценить потенциал ФУ в ожидаемых условиях функционирования предприятия.

В работе [91] используется понятие финансовой гибкости. При этом вместо формулировки предлагается перечисление различных способностей компании по использованию и манипуляциям своими

финансовыми ресурсами, включая задачи инвестирования, т. е. развития. В сопротивлении материалов и инженерном деле гибкость является одним из свойств, обеспечивающих неразрушающее изменение и восстанавливаемость формы конструкции, изделия, материала, т. е. в конечном итоге живучесть – устойчивость. В сфере финансов в «гибкость» сложно ввести дополнительный по отношению к «устойчивости» смысл, кроме аспектов организации манипулирования ими. Гибкость в этом контексте можно рассматривать как потенциал системы управления финансами, включая локально нормированную «степень операциональной свободы», профессионализм, интеллект и мотивацию финансистов. Она, с одной стороны, является одним из средств обеспечения устойчивости, с другой, – её разновидностью.

Для целей моделирования в настоящей монографии под финансовой устойчивостью предприятия понимается состояние активов предприятия, позволяющее финансировать исполнение внутренних и внешних его обязательств в условиях заданных изменений макроэкономических показателей, конъюнктуры используемых секторов рынка, параметров региональных социально-экономических систем, а также при возникновении событий, наносящих прямой материальных ущерб предприятию. Под прямым ущербом понимается утрата ТМЦ в результате порчи, хищения, изъятия, уничтожения, а также недополученная прибыль (или дополнительные расходы) в результате нарушения производственных и хозяйственных циклов по различным причинам внутреннего и внешнего характера.

В приведённом определении не указаны источники обеспечения финансовой устойчивости. Дело в том, что состояние активов может быть непосредственным или косвенным источником финансовых ресурсов для исполнения обязательств. Непосредственное использование активов для исполнения обязательств здесь комментариев не требует. Роль активов, как косвенного источника реализуется, если состояние активов (структура и динамика) формирует положительный образ кредитоспособности предприятия. В этом случае для покрытия непредвиденных затрат и, следовательно, восстановления финансовых ресурсов для выполнения обязательств могут быть привлечены заёмные средства, и предприятие «выстоит» под натиском «финансовой непогоды».

Внешним проявлением ФУ является его платёжеспособность. Однако эта категория по смыслу уже. Обычно под платёжеспособностью понимается возможность осуществления немедленных платежей по контрактам.

Состояние активов в целях моделирования ФУ определяется стоимостной оценкой этих активов по бухгалтерскому учёту и их ликвидностью, т. е. способностью конвертации в средства платежа. В научной и учебной литературе ликвидность трактуется неоднозначно, а ряд авторов, хотя и использует его, но не приводит формулировок словарного образца [94-97]. Под ликвидностью актива часто понимается только скорость, с какой актив может быть конвертирован в деньги без заметной потери его стоимости. В настоящей работе используется более полное понимание ликвидности как потенциальной способности актива выступить средством платежа. В процессе хозяйственной деятельности могут возникать ситуации, когда деньги для расчётов требуются срочно, и тогда актив может быть продан или конвертирован по заниженной стоимости, но необходимое срочное пополнение ресурсов он обеспечит. В общем случае ликвидность, зависит от макроэкономической ситуации, конкретной рыночной и региональной конъюнктуры и меняется во времени.

Объём активов в ходе хозяйственной деятельности определяется динамикой входных и выходных потоков финансово-экономических ресурсов (денег в различной форме, других финансовых ресурсов и ТМЦ), а также динамикой капитализации и декапитализации. Однако для оценки ФУ интерес представляют, главным образом, оборотные средства, запасы, резервы, и денежные ресурсы. Последние используются при оценке платёжеспособности.

ФУ обеспечивается, прежде всего, наличием и адекватным управлением резервами, приобретением продуктов страхования, управлением соотношения входными и выходными финансовыми потоками (очевидно, что в основе этого лежит управление поставками со стороны контрагентов и сбытом готовой продукции), принятием превентивных мер по защите ТМЦ от порчи и утраты, созданием условий диверсификации производства и гибким использованием этого потенциала. Последние два инструмента взаимосвязаны и являются наиболее сложными и важными.

Таким образом, в изложенной трактовке финансовая устойчивость в парадигме безопасного существования тождественна понятию достаточность финансовых ресурсов.

Под управлением входными и выходными потоками понимается поддержание необходимого баланса кредиторской и дебиторской задолженностей, выбор надёжных поставщиков, диверсификация поставщиков, диверсификация рынков сбыта, хозяйственное планирование, минимизирующее угрозы кассовых разрывов. Одним из базовых условий ФУ является наличие достаточного объёма собственного оборотного капитала.

На рисунке 8 изображена типовая схема движения денежных потоков, предложенная в [92].

Основными направлениями управления входными потоками с точки зрения обеспечения ФУ являются:

- анализ условий привлечения финансовых ресурсов;
- изучение доступных финансовых каналов и оценка величины финансовых ресурсов, включая мероприятия по компенсации ущербов, в частности приобретение продуктов страхования;
- расчёт необходимых финансовых запасов;
- разработка инструментов и процедур трансформации финансовых запасов в эндогенные факторы производства: материальные, нематериальные и финансовые.

Основными направлениями управления выходными потоками с точки зрения обеспечения ФУ являются [98]:

- оценка эффективности трансформации эндогенных факторов производства в затраты;
- оценка ключевых финансовых показателей по результатам деятельности предприятия;
- оценка эффективности распределения доходов в соответствии со стратегическими планами и ожиданиями,
- выявление факторов успеха и проблем при обеспечении ФУ.

При управлении финансовыми ресурсами главная цель – обеспечение безопасного существования предприятия – может быть декомпозирована на три подцели финансового содержания:

- обеспечение самосохранения предприятия, как единого целого, которое достигается при наличии минимального денежного потока, достаточного для существования предприятия;

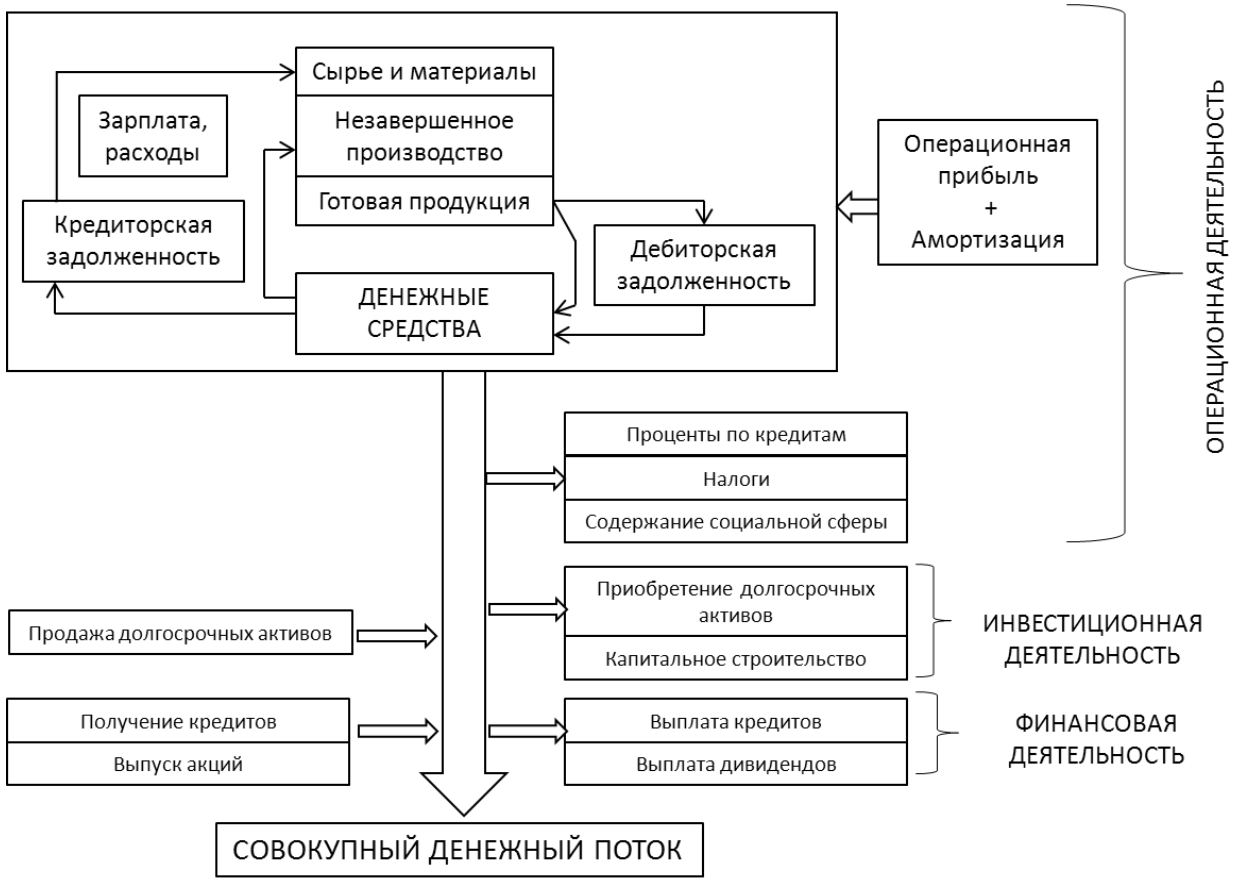

Рисунок 8 – Типовая схема движения денежных потоков [92]

- обеспечение адаптации предприятия к изменчивым рыночным условиям, достижение которой заключается в приспособлении предприятия к окружающей среде, что достигается дополнительными денежными потоками;

- установление баланса между вышеотмеченными подцелями, который необходим для обеспечения целостности предприятия и долгосрочной его устойчивости, что связано с выбором той или иной стратегии развития [99].

Для наукоёмких предприятий, выпускающих сложную продукции малой серии или уникальную (ракетно-космическая промышленность, атомная энергетика, кораблестроение и т. п.) важно выделить следующие особенности, осложняющие, как проведение анализа ФУ, так и процедуры её обеспечения:

- небольшая диверсификация рынка сбыта – по основной продукции практически отсутствует,

- дискретность финансирования, что ставит в зависимость от выплат авансов и за продукцию со стороны заказчиков; просроченная дебиторская задолженность одного потребителя основной продукции может ввергнуть предприятие в кризисное положение,

- небольшой спектр заказчиков и основных поставщиков комплектующих,

- большая доля в активах низколиквидных нематериальных активов,

- большая доля в оборотных активах низколиквидных запасов в виде комплектующих, деталей, материалов, не имеющих широкого спроса,

- сильная зависимость от надёжности изготавливаемой и используемой техники.

Подходы к анализу и оценке ФУ предприятий

Единый общепризнанный подход к математическому моделированию ФУ не существует.

В практике широко используется коэффициентный, факторный, динамический анализ. Здесь виды анализа указаны в порядке убывания частоты их использования.

Для оценки ФУ используются различные коэффициенты распределения и координации, рассчитанные на основе отношений абсолютных показателей, учитываемых в бухгалтерском балансе [96, 97, 100-103]. В основе подходов к расчёту коэффициентов лежит два основных критерия:

- обеспечение независимости от внешних источников финансирования;

- наличие резервов.

Как отмечают специалисты, на практике единая система коэффициентов, а главное, требуемых их пороговых значений не сложилась. Кроме того, даже названия одних и тех же идентичных по смыслу коэффициентов разнятся у разных авторов [104]. Вывод о ФУ по этим коэффициентам может быть сделан на основе изучения динамики данных баланса, сравнительного анализа различных предприятий или их

групп. Пороговые (базисные, нормативные) значения коэффициентов могут значительно отличаться для отраслей экономики, регионов, особенностей функционирования предприятий и т. п. Значения многих коэффициентов зависят от принятой учётной политики предприятий, в частности по методу отгрузки или методу оплаты.

Проблема использования коэффициентного анализа состоит в том, что он не вникает в операциональный смысл ФУ, а ограничивается поверхностной оценкой, которая оказывается мало содержательной без субъективного опыта аналитика в конкретном секторе промышленности.

Под факторным анализом в настоящей работе понимается сравнительный анализ абсолютных значений бухгалтерского баланса. Вывод о состоянии ФУ делается на основе сопоставления полученных равенств и неравенств с эталонными соотношениями статей баланса, которые выведены исходя из логики (здравого смысла) финансовой стороны функционирования предприятия. Состояния ФУ дифференцируются по градациям, каждой из которых соответствует предикат равенств и неравенств значений статей бухгалтерского баланса.

Содержание рассматриваемых показателей при факторном подходе может быть расширено за счёт более явного использования параметров входных и выходных денежных потоков, конвертации при необходимости приобретённых страховых продуктов, но суть подходов от этого не меняется.

Динамический анализ предполагает изучение не абсолютных значений параметров ФУ, а их дифференциалов. Достоинством метода является его направленность на рассмотрение процессов и, соответственно, вектора движения финансовых ресурсов предприятия, однако оно диалектически содержит и его главный недостаток. Динамический анализ не отражает фактического состояния ФУ в конкретный момент времени, в том числе в будущий. В принципе возможна ситуация, когда предприятие, имея «правильный» вектор изменения финансового состояния, оказывается банкротом сейчас – изменения идут, но не успевают исправить положение дел.

В числе широко распространённых методов также находятся экспресс-методы, в основе которых могут лежать коэффициентный, факторный, динамический анализ или их интеграция.

Некоторые исследователи используют интегральные балльные оценки, особенно для применения критерия банкротства [104]. В таких методиках и моделях для вычисления обобщённых оценок ФУ на основе коэффициентов используются различные свёртки, в которых значения балансовых коэффициентов складываются с некоторыми весовыми коэффициентами. Наиболее известными свёртками являются модели Альтмана, Таффлера, Тишоу, Лиса [105]. Однако они получены на основе уже устаревшей зарубежной статистики, не учитывающей российскую специфику.

В отечественной практике обычно для свёрток используются коэффициенты важности, определяемые экспертным путём. Для определения таких коэффициентов нет объективной базы, поэтому получаемую интегральную оценку нельзя считать надёжной. В целом недостатки примитивизации использования свёрток на основе, так называемых коэффициентов, важности и пути их преодоления рассмотрены в работе [70].

Особняком в арсенале моделирования ФУ предприятий расположены недостаточно разработанные методы и модели, так называемой, прямой оценки ФУ предприятия. Для таких моделей могут быть использованы показатели, описывающие вероятностные характеристики утраты предприятием способности выполнения своих обязательств по расчётам. Ниже в работе предложена имитационная модель прямой оценки достаточности финансовых ресурсов с учётом возмущений внешней среды. Однако следует отметить, что реализация такой модели и её использование довольно трудоёмкое занятие и требует сбора исходных данных, оперирование которыми не в традиции финансовых органов промышленных предприятий.

Общим недостатком рассмотренных методов непрямой оценки является то, что они не учитывают в явном виде влияние неопределённой внешней среды на потенциал платёжеспособности предприятия на некотором интервале времени, являются детерминированными. Однако эти модели, обладая несомненным преимуществом простоты и оперативности, важны для дополнения модели «прямой» оценки и при наличии статистики позволяют проводить грубую оценку и выявлять тревожные признаки в режиме ежедневного автоматического мониторинга. Результаты мониторинга

состояния активов, получаемые, например, в ситуационном центре, могут в режиме он-лайн в экранной форме предоставляться не только финансистам, но также руководителям предприятий, аналитическим службам обеспечения безопасного существования и, в частности, защиты ресурсов, членам правлений и советов директоров в качестве информации к размышлению.

3.2. Модели непрямого анализа финансовой устойчивости предприятия

Математические модели коэффициентного анализа ФУ предприятия

Для коэффициентного анализа могут быть использованы некоторые модели, получившие наибольшее распространение на практике.

Коэффициенты для обобщённой оценки ФУ предприятия

Для обобщённой оценки целесообразно использовать уточнённый коэффициент финансирования $К_{фу}$ и коэффициент манёвренности $К_м$, из которых можно вывести ряд других [100, 106].

$К_{фу}$ вычисляется по формуле

$$К_{фу} = З_{кк} / (С_к + З_{кд}) = (А - С_к - З_{кд}) / (С_к + З_{кд}) = А / (С_к + З_{кд}) - 1 \qquad (31)$$

где $З_{кк}$ – краткосрочные заёмные средства,

$С_к$ – собственный капитал,

$З_{кд}$ – долгосрочные заёмные средства,

А – стоимость всех активов.

Для расчёта $К_м$ используется формула

$$К_м = (С_к + З_{кд} - А_в) / С_к \ , \qquad (32)$$

где $А_в$ – балансовая стоимость внеоборотных активов.

Уточнённый коэффициент финансирования и коэффициент манёвренности рассчитываются по данным бухгалтерского баланса и отчёта о прибылях и убытках.

Частные коэффициенты оценки ФУ предприятия

Здесь представлены коэффициенты, получившие широкое распространение на практике [107].

1) Коэффициент автономии (коэффициент финансовой независимости, коэффициент концентрации капитала) – показывает удельный вес собственных средств предприятия в сумме средств

$$К_а = СК/ВБ = (КиР + РПР)/ВБ \quad (33)$$

где СК – собственный капитал,

ВБ – валюта баланса,

КиР – капитал и резервы,

РПР – резервы предстоящих расходов.

2) Финансовый леверидж (коэффициент финансовой зависимости) – показывает долю заёмных средств в валюте баланса заёмщика

$$К_л = ЗК/ВБ = (ФО + РПР)/ВБ \quad (34)$$

где ЗК – заёмный капитал,

ФО – финансовые обязательства.

3) Коэффициент соотношения заёмных и собственных средств (коэффициент финансового риска или коэффициент привлечения). Является разновидностью первых двух:

$$К_к = ЗК/СК \quad (35)$$

4) Коэффициент покрытия долгов собственным капиталом (коэффициент платёжеспособности) – обратный коэффициенту привлечения

$$К_п = СК/ЗК \quad (36)$$

5) Коэффициент обеспеченности собственными оборотными средствами – показывает, сколько оборотных средств финансируется за счёт собственных оборотных средств

$$К_с = (СК - ВнА)/ОА \quad (37)$$

где: ВнА – внеоборотные активы,

ОА – оборотные активы.

6) Коэффициент манёвренности собственных средств – доля собственных оборотных средств в собственном капитале

$$К_м = (СК - ВнА)/СК \quad (38)$$

7) Коэффициент обеспеченности запасов собственными средствами – показывает долю запасов, финансируемых за счёт собственных средств

$$К_з = (СК - ВнА)/З \quad (39)$$

где З – запасы.

8) Коэффициент покрытия активов собственными средствами

$$К_{п} = (СК - ВнА)/ВБ \quad (40)$$

9) Коэффициент структуры заёмного капитала

$$К_{сзк} = ДО/ЗК \ , \quad (41)$$

где ДО – долгосрочные обязательства.

Этот коэффициент отражает какую часть в обязательствах составляют долгосрочные займы. Низкое значение коэффициента говорит о зависимости от краткосрочных займов, а значит от сиюминутной конъюнктуры рынка.

10) Коэффициент структуры долгосрочных вложений

$$К_{сдв} = ДО/ВнА \quad (42)$$

Коэффициент предоставляет информацию о том, какая часть основных средств и других необоротных активов профинансирована внешними инвесторами.

11) Коэффициент покрытия краткосрочных обязательств потоком денежных средств

$$К_{пко} = (ЧП + А_{м})/КО \ , \quad (43)$$

где ЧП – чистая прибыль,

$А_{м}$ – отчисления на амортизацию;

КО – краткосрочные обязательства.

12) Интервал (длительность) самофинансирования [106].

$$Т_{сф} = (ДС + КФВ + КДЗ)/З_{д} \ , \quad (44)$$

где ДС – денежные средства,

$З_{д}$ – средние расходы на функционирование предприятия в день на рассматриваемом периоде; включают, в том числе управленческие и операционные расходы.

Выше было отмечено о невозможности установить общеприемлемые значения коэффициентов для любых предприятий без учёта специфики отрасли и особенностей функционирования предприятий.

Математическая модель факторного анализа финансовой устойчивости на основе исследования структуры активов и пассивов

Модель предусматривает оценку финансовой устойчивости предприятия на основе соотношения структуры активов и пассивов

[108]. При этом используются два нетрадиционных способа классификации активов.

В первом случае в составе имущества выделяется имущество в неденежной форме $И_{ндф}$ и имущество в денежной форме $И_{дф}$, а в составе пассивов – собственный и заёмный капитал [101].

$$И_{ндф} = ВнА + З + НДС + ДЗ + ПОА \quad (45)$$

где ВнА – внеоборотные активы,

З – запасы,

НДС – налог на добавленную стоимость по приобретённым ценностям,

ДЗ – дебиторская задолженность,

ПОА – прочие оборотные активы.

$$И_{дф} = ДС + КФВ \ , \quad (46)$$

где ДС – денежные средства,

КФВ – краткосрочные финансовые вложения.

В соответствии со вторым подходом к классификации активов предприятия активы делятся на финансовые (ФА) и нефинансовые (НФА) [109].

$$ФА = ДС + КФВ + ДФВ + КДЗ + ДДЗ \ , \quad (47)$$

где ДФВ – долгосрочные финансовые вложения или инвестиции,

КДЗ – краткосрочная дебиторская задолженность,

ДДЗ – долгосрочная дебиторская задолженность.

$$НФА = ВнА - ДФВ + З + ПОА \quad (48)$$

Капитал (пассивы) также разделяется на заёмный капитал (в т. ч. заёмный долгосрочный капитал (ДО) – итог по разделу IV баланса - и заёмный краткосрочный капитал (КО)) и собственный капитал (СК).

$$СК = КиР + ДБП + РПР \quad (49)$$

где КиР – капитал и резервы (итог по разделу III баланса),

ДБП – доходы будущих периодов,

РПР – резервы предстоящих расходов.

$$ЗК = ДО + КО$$
$$КО = ККЗ + КЗ - ДБП - РПР \quad (50)$$

где ЗК – заёмный капитал,

ККЗ – краткосрочные резервы и займы,

КЗ – кредиторская задолженность.

Расчёт индикаторов ФУ строится на экономически обоснованном соотношении активов и пассивов между собой с учётом удовлетворительной структуры баланса. Структура баланса считается удовлетворительной, если заёмный капитал разумно авансирован в покрытие более ликвидной части активов на случай необходимости срочного возврата долгов, поэтому самая низколиквидная часть оборотных активов (запасы) должна покрываться собственным капиталом. При этом образуется собственный оборотный капитал (СОК) [108].

При такой структуре баланса в соответствии с первым способом классификации активов индикатор ФУ, с одной стороны, показывает, хватит ли имущества в денежной форме для расчёта по обязательствам, а с другой – отражает, какая часть собственного капитала вложена в денежные активы.

Индикатором ФУ в этом случае выступает денежный капитал (ДК).

$$И^{1}_{фу} = ДК = СК - И_{ндф} = И_{дф} - ЗК, \qquad (51)$$

где $И^{1}_{фу}$ – индикатор ФУ при первом способе классификации баланса.

Здесь $И^{1}_{фу}$ выступает как платёжеспособность в денежной форме.

Для обеспечения финансовой устойчивости должно выполняться условие $И^{1}_{фу} > 0$.

Нарушение этого условия означает, что объём денег у предприятия меньше величины заёмного капитала, а собственный капитал меньше имущества в неденежной форме. Это свидетельствует, что все собственные источники в отчётном периоде были использованы полностью, их не хватило для финансирования активов, и поэтому были задействованы заёмные источники.

По второму способу индикатор ФУ рассчитывается по следующей форме:

$$И^{2}_{фу} = ФК = СК - НФА = ФА - ЗК \qquad (52)$$

Здесь величина ФК является оценкой достаточности покрытия активов предприятия финансово устойчивыми источниками их формирования и характеризует устойчивую возможность отвечать по своим обязательствам в любой момент времени.

При практическом применении оба способа расчёта $И_{фу}$ могут приводить к разным результатам, что объясняется различными подходами к классификации активов. В первом случае (деление имущества на денежную и неденежную формы) индикатор ФУ (денежный капитал) рассматривается как выражение реальных денежных средств, которые можно получить в любой короткий момент времени. Во втором случае финансовые активы классифицируются с точки зрения стоимостного выражения. Они представляют собой либо реальные денежные средства, либо денежные требования к другим контрагентам, а также вложения в долговые обязательства. Другими словами, второй подход шире с точки зрения охвата периода изучения ФУ [108].

Выбор подхода зависит от временного горизонта, для которого проводится анализ. Первый подход – краткосрочный период, второй - долгосрочный. Однако следует иметь в виду, что необеспеченность платёжеспособности (фактически это позволяет оценить первый способ) приводит к банкротству и делает бессмысленным долгосрочное планирование.

Преимуществом указанных подходов является то, что для оценки ФУ не требуется знание никаких пороговых значений. Достаточно оценить динамику индикаторов.

Их можно применять для оперативной оценки достаточности ресурсов предприятия для покрытия своих обязательств.

Динамическая нормативная модель ФУ

Для экспресс-диагностики динамического изменения ФУ любого предприятия может быть использована ординальная динамическая нормативная модель [89].

Модель построена на сравнении соотношения темпов изменения значимых показателей, рассматриваемых при анализе ФУ, с идеальным вариантом соотношения этих показателей. Чем ближе результат к идеалу (нормативному варианту) тем ФУ выше, поскольку деятельность предприятия, изменение структуры его баланса направлены к увеличению устойчивости. Строится эта динамическая модель следующим образом.

1) Определяется перечень наиболее важных для оценки ФУ показателей бухгалтерского баланса. В их число целесообразно включить:

- валюту баланса (ВБ),
- внеоборотные активы (ВнА),
- денежные средства и краткосрочные финансовые вложения (ДС),
- долгосрочные обязательства (ДО),
- заёмный капитал (ЗК),
- капитал и резервы (КиР),
- краткосрочные обязательства (КО),
- собственные оборотные средства (СОС),
- среднемесячную выручку (В).

2) Для совокупности выбранных показателей строится нормативная матрица соотношений темпов изменения значений показателей.

Правила заполнения таблицы следующие. В ячейку таблицы вносится 1, если показатель, расположенный в *i*-ой строке должен расти быстрее, чем показатель в *j*-ой строке, в противном случае вносится -1. В ситуации неопределённости в ячейку вносится 0. При этом для проверки на корректность и согласованность данных используется правило транзитивности отношений. Ячейка с одинаковыми номерами строки и столбца, естественно, не заполняется.

Для определения нормативного соотношения показателей в качестве логической поддержки могут использоваться модели коэффициентного анализа, которых в данном случае целесообразно привлекать как можно больше. Если два показателя используются в коэффициенте на разных уровнях отношения (один в числителе, а другой в знаменателе), то соотношение нормативных темпов их роста определяется исходя из требований увеличения или уменьшения значения коэффициента – значение коэффициента прямо пропорционально зависит от числителя и обратно пропорционально от значения знаменателя. Полученные результаты сведены в таблицу 4.

3) Для каждого показателя вычисляется нормативный рейтинг r_i^0, где *i* - условный порядковый номер показателя.

Пусть I – множество рассматриваемых показателей (в таблице 4 учитывается девять показателей), имеющее мощность I.

$$Для\ \forall i \in I\ и\ \forall j \in I \quad r_i^0 < r_j^0, \quad если \sum_{\substack{k=1 \\ k \neq i}}^{I} a_{ik} > \sum_{\substack{j=1 \\ k \neq j}}^{I} a_{jk} \qquad (53)$$

где a_{ik} – значение в таблице нормативных соотношений темпов изменения показателей, стоящее на пересечении *i*-ой строки и *k*-го столбца.

4) Показатели упорядочиваются (см. таблицу 4) в соответствии с их рейтингами.

5) По квартальной или годовой отчётности строится матрица реальных соотношений динамики изменения интересующих показателей.

Таблица 4 – нормативное соотношение темпов изменения основных показателей ФУ

Номер п/п	*Показатель*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1	В		1	1	1	1	1	1	1	1
2	ДС	-1		1	1	1	1	1	1	1
3	СОС	-1	-1		1	1	1	1	1	1
4	КиР	-1	-1	-1		1	1	1	1	1
5	ДО	-1	-1	-1	-1		1	1	1	1
6	ВнА	-1	-1	-1	-1	-1		1	1	1
7	ВБ	-1	-1	-1	-1	-1	-1		1	1
8	ЗК	-1	-1	-1	-1	-1	-1	-1		1
9	КЗ	-1	-1	-1	-1	-1	-1	-1	-1	

6) Динамический индикатор финансовой устойчивости *Y* вычисляется следующим образом.

$$Y = \left(1 - \sum_{i=1}^{I}\sum_{j=1}^{I} b_{ij}\right) \Big/ \left(I \cdot (I-1)\right),$$

$$b_{ij} = \begin{cases} 1, \text{если } r_i > r_j \text{ при } i < j \\ 1, \text{если } r_i < r_j \text{ при } i > j \\ 0, \text{в остальных случаях} \end{cases} \qquad (54)$$

где r_i и r_j – фактические рейтинги показателей, вычисляемые в соответствии с правилом (53).

b_{ij} – переменная, которая отражает наличие или отсутствие инверсии соотношения темпов изменения показателей между собой.

Чем ближе оценка Y к 1, тем большая доля требований, предъявляемых к ФУ предприятия, выполняется.

Представленный метод вычисления ФУ обладает рядом достоинств, в числе которых:

- независимость от состава показателей, что позволяет учесть особенности функционирования предприятия и предпочтения аналитика;
- вычислительная простота и ясный «физический» смысл;
- комплексное рассмотрение различных показателей состояния и динамики финансовых ресурсов предприятия;
- отсутствие эффекта компенсации положительных и отрицательных изменений отдельных показателей, т. е. бессмысленной для принятия решений агрегации;
- возможность получить прогноз ФУ, отражая прогнозируемые изменения в финансовых показателях в таблице фактических рейтингов показателей.

Статично-динамическая модель качественного оценивания ФУ

Выше предложена модель факторного анализа ФУ по структуре бухгалтерского баланса. Идея этой модели совместно с динамической оценкой ФУ позволяет построить простую модель комплексной качественной (в смысле неколичественной) оценки, которая может служить для экспресс-диагностики.

Таблица 5 – Градации оценки статичного состояния ФУ

Высокогарантированная устойчивость	(ЛОА=ДС+КВФ+КДЗ>КО+$КЗ_т$+РПР+ИП) & (ПОА≥ДО)
Устойчивость	(ЛОА≥КО+$КЗ_т$+РПР) & (ПОА≥ДО+ИП)
Неопределённость	(ЛОА=КО+$КЗ_т$) & (ПОА≈ДО+РПР)
Проблемы (дополнительные затраты на заёмный капитал или пени и штрафы)	(ОА=КО+$КЗ_Т$) ∨ (ОА>КО+$КЗ_Т$) & (ВБ<ДО+КО)
Кризис (угроза банкротства)	ОА<(КО+$КЗ_Т$)

Алгоритм работы модели заключается в следующем.

1) Задаётся 5 градаций статичного состояния ФУ на основе сопоставления абсолютных значений некоторых статей активов и пассивов баланса (см. таблицу 5). Для этого используется модификация классификации, предложенной в работе [110].

В таблице 5 использованы следующие обозначения при максимальной преемственности с предыдущими обозначениями настоящего раздела работы:

ОА – оборотные активы

ЛОА – высоколиквидные оборотные активы,

ПОА – (отличные от ЛОА) прочие оборотные активы,

ДС – денежные средства,

КВФ – краткосрочные вложения финансов,

КДЗ – краткосрочная дебиторская задолженность,

КО – краткосрочные обязательства (как внешние, так и внутренние),

$КЗ_Т$ – кредиторская задолженность, подлежащая погашению в анализируемом периоде,

ИП – плановые инвестиции,

ДО – долгосрочные обязательства,

ВБ – валюта баланса (в данном случае активы).

В таблице 5 приведены основные типовые ситуации для оценки по введённой лингвистической шкале реальных ситуаций.

2) Полученные в результате использования динамической нормативной модели численные значения преобразуются в лингвистические, приведённые в таблице 6.

Таблица 6 – Конвертация численных значений динамической нормативной оценки состояния ФУ в лингвистические

1	Усиление степени устойчивости
[0.8; 1[	Ослабление степени устойчивости
[0.5; 0.8[	Сильное ослабление степени устойчивости
[0; 0.5[	Катастрофическое ослабление степени устойчивости

3) Строится матрица ФУ, изображённая на рисунке 9.

В зависимости от сочетания статического состояния и тенденции его изменения делается вывод о состоянии ФУ с учётом его динамики на качественном уровне. Белые клетки соответствуют устойчивому состоянию; серые – неустойчивому состоянию, требующему принятие мер; тёмные клетки – кризисному состоянию.

Предложенная методика позволяет оперативно оценить состояния ФУ с учётом тенденции. Она даёт грубую оценку, поскольку реальное состояния дел зависит не только от знака направленности тенденции (улучшается/ухудшается), но и от скорости изменений.

	Усиление степени ФУ	Ослабление ФУ	Сильное ослабление ФУ	Катастро-фическое ослабление ФУ
Высокогарантированная ФУ				
Устойчивость				
Неопределённость				
Проблемы (неустойчивость)				
Кризис				

Рисунок 9 – Матрица статически-динамической оценки состояния ФУ предприятия на качественном уровне

3.3. Математическая модель прямой оценки достаточности финансовых ресурсов предприятия

Модель основана на сценарном расчёте платёжеспособности предприятия в каждый момент времени на некотором интересующем перспективном периоде в зависимости от входных и выходных потоков финансовых ресурсов, имеющихся активов с учётом возможности их перевода в средства платежа и различных внешних событий, требующих дополнительных затрат финансовых ресурсов.

Теоретически рассуждая, модель может быть построена в вероятностном пространстве внешних событий. Такая модель должна включать совместные функции распределения на множестве рассматриваемых событий, а также вероятностные модели конвертации активов в средства платежа за тот или иной период (т. е. вероятностные распределения значения ликвидности различных активов), математические ожидания и дисперсии дефицита платёжных средства в различные моменты рассматриваемого периода. Подобный полный и строгий учёт неопределённости значительно и неоправданно усложнит модель. Неоправданность связана с тем, что параметры функций распределения учитываемых величин априорно не известны. Для их ввода в модель придётся использовать экспертные оценки, которые в данном случае нельзя рассматривать как точные. Низкая объективность исходных данных нивелирует строгость математической модели. В то же время вероятностный характер воздействий среды может быть учтён при интеграции рассматриваемой модели в общий механизм вычисления рисков и имитационном моделировании (см. разделы 2.2 и 2.4).

В рассматриваемой задаче для моделирования прямой оценки достаточности финансовых ресурсов (далее – ДФР) предприятия целесообразно описать основные соотношения, отражающие платёжеспособность предприятия, и построить алгоритм расчёта платёжеспособности при тех или иных возмущающих воздействиях. Фактически предлагается имитировать бюджет движения денежных средств и корректировать оценку ДФР в соответствии с различными сценариями, реализующимися или гипотетическими.

Здесь необходимо привести важный комментарий. В практике реального планирования и деятельности предприятий, возможны кассовые разрывы, которые приводят к локальной потере платёжеспособности. Причины этого могут быть различными – несовершенство планирования, условия взаимодействия с потребителями и поставщиками, которые предприятие не в силах изменить и др. В такой ситуации могут оказываться также предприятия, работая по государственным заказам, когда динамика финансирования задаётся на уровне государственного планирования, а выполнение конкретных финансовых операций страдает из-за бюрократических барьеров. Однако, если задержки платежей не приводят к срыву

производственных планов (за счёт задержки выполнения работ или поставок, отключения от поставок естественных монополий (электроэнергия, газ), забастовок и т. п.), что чревато уже серьёзными последствиями, то предприятия без проблем переживают такие кассовые разрывы. В некоторых случаях менеджеры сознательно идут на формирование кредиторской задолженности, сопоставляя потери по пеням и штрафам с доходностью ликвидных активов, которые могли бы быть потрачены на текущие платежи. Подобные решения относятся к проблематике оптимального управления финансовыми ресурсами, что выходит далеко за рамки предмета настоящего исследования. В связи с этим в дальнейшем используется следующее методическое допущение.

В случае выявления на рассматриваемом временном интервале кассовых разрывов проводится оценка возможности привлечения различных активов для скорейшего выполнения обязательств предприятия вне зависимости от возможной стратегии финансового менеджмента.

Второе допущение связано с разной скоростью конвертации (ликвидности) активов в средства платежа. Исходя из этого, активы ранжируются по уровню ликвидности. В первую очередь для обеспечения платежей привлекаются наиболее ликвидные активы.

При сделанных допущениях оценка ФУ на рассматриваемом временном интервале получается более жёсткой, что с точки зрения оценки безопасности лучше.

В модели используются следующие обозначения.

t=1,…, (T+1) – условный порядковый номер элементарного отрезка рассматриваемого периода;

i=1,…, I – условный порядковый номер источника поступления финансовых средств в результате основной и неосновной производственной деятельности, финансовых вложений (проценты и возврат объёма (части) вложения), плановой реализации активов и т. п. Источник определяется исходя из удобства и возможности локализации соответствующей ему составляющей общего входного потока денежных средств. Под ним может пониматься конкретный контракт, сектор рынка потребления массовой продукции, депозит и т. п.;

v_i^t – объём поступления денежных средств из *i*-го источника в *t*-ом элементарном отрезке рассматриваемого периода[11];

j=1,…, *J* – условный порядковый номер направления платежа (адресата получения денежных средств, статьи расходов) предприятия;

z_j^t – объём платежа в *t*-ый момент в *j*-ом направлении; здесь учитываются практически все плановые расходы предприятия для расчётов с контрагентами, кредиторами, персоналом, налоги и сборы, пени и штрафы, различные обязательные взносы и т. п.;

τ – длительность интервала времени для конвертации актива в деньги; единицей измерения τ является элементарный отрезок рассматриваемого периода;

a=1, …, *A* – условный порядковый номер актива предприятия, который может быть конвертирован в средство платежа (ликвидный актив). В их число входят оборотные средства, резервный капитал, некоторые виды внеоборотных активов, а также страховые продукты, приобретённые по договорам страхования, которые могут быть использованы для погашения ущерба в случае необходимости. Основные производственные фонды в число *A* не включаются, исходя из позиции, что если дело дошло до их реализации в целях выполнения финансовых обязательств, то ФУ не обеспечена. А если для расчётов не хватит и основных производственных фондов, то это уже проблема не только и не столько предприятия, сколько его кредиторов. Множество ликвидных активов делится на абсолютно ликвидные активы (денежные средства), которые могут использоваться мгновенно (τ_a=0) и имеют номера по порядку $a \le a^*$, и менее ликвидные активы с номерами $a > a^*$, для конвертации которых требуется время ($0 < \tau_a \le \tau_a^{lim}$); денежным средствам, находящимся на расчётных счетах предприятия, присвоен порядковый номер 1 (*a*=1);

W^t – чистая прибыль в *t*-ый момент;

$$W^t = \sum_{i=1}^{I} v_i^t - \sum_{j=1}^{J} z_j^t = V^t + Z^t \qquad (55)$$

[11] В дальнейшем для лаконичности текста вместо фразы «элементарный отрезок рассматриваемого периода» будет использоваться слово «момент».

q_a^t – объём *a*-го актива, исчисленный в денежных единицах по балансовой стоимости, в *t*-ый момент;

Q^t – суммарный объём ликвидных активов в *t*-ый момент; $Q^t = \sum_{a=1}^{A} q_a^t$.

Обычно под ликвидностью актива понимается отрезок времени, за который актив может быть конвертирован в деньги без потери балансовой стоимости. Однако очевидно, что некоторые активы могут быть реализованы по балансовой стоимости за время практически неприемлемое (теоретически бесконечное). С другой стороны, даже высоколиквидный актив из-за срочности может быть реализован по заведомо заниженной цене. С учётом этого в модель введена величина τ_a^{lim} – минимальный срок, за который *a*-ый актив может быть реализован по балансовой стоимости (ликвидность актива, если использовать традиционную упрощённую трактовку этого понятия);

$s_a^{t+\tau}$ – выручка от реализации *a*-го актива к моменту (*t*+τ); $s_a^{t+\tau} = \varphi_a\left(q_a^t;\tau\right)$, где φ_a – некоторая функция, описывающая реальную стоимость *a*-го актива в зависимости от срочности конвертации. Её проще всего задать в табличной форме по экспертным оценкам, однако во многих случаях вероятность появления покупателя актива, готового приобрести его по той или иной цене, может быть описана экспоненциальным законом распределения, соответственно по аналогичному закону растёт со временем и реальная продажная цена. Кроме того, подобная зависимость справедлива для многих естественных процессов, для которых свойственно насыщение. При таком допущении зависимость между *s* и *q* может иметь следующий аналитический вид:

$$s_a^{t+\tau} = \left(1 - e^{-\lambda_a \cdot \tau}\right) \cdot q_a^t \qquad (56)$$

где λ_a – отражает эластичность спроса на *a*-ый актив,
или задаваться постоянным значением:

$$s_a^{t+\tau} = \begin{cases} q_a^t \text{ , если } \tau \geq \tau^{\lim} \\ 0 \quad \text{ , если } \tau < \tau^{\lim} \end{cases} \qquad (57)$$

где τ^{lim} означает операционную задержку, например, время, требуемое для оформления документов.

Очевидно, что для a=1 справедливо $s_1^{t+\tau} = q_1^t$ для $\forall\tau$ и $\forall t$. Здесь инфляция, а также различные процентные ставки не учитываются, поскольку речь идёт о номинальной стоимости актива (денежных средствах), который используется для выполнения необходимых платежей в номинальном исчислении.

Смысл выражения (56) в следующем – чем ниже цена, тем больше потенциальных покупателей и тем больше шансов продать актив быстрее. Кроме того, чем больше эластичность спроса, тем с падением цены быстрее растёт число заинтересованных потребителей.

Общая балансовая стоимость ликвидных активов в t-ый момент вычисляется по формуле:

$$Q^t = \sum_{a=1}^{A} q_a^{t-1} + W^t \ , \qquad (58)$$

Общий объём S^t (в денежных единицах) абсолютных ликвидов в t-ый момент вычисляется по формуле:

$$S^t = \sum_{a=1}^{a^*} s_a^t \qquad (59)$$

Дефицит средств платежа D^t в t-ый момент рассчитывается по формуле:

$$D^t = \begin{cases} Z^{t+1} - S^t, \text{если } Z^{t+1} > S^t \\ 0, \text{в противном случае} \end{cases} , \qquad (60)$$

Максимальный объём результата конвертации ликвидных активов в абсолютные активы, который был начат в t-ый момент и должен быть завершён в момент (t+τ), $S_+^t(\tau)$ вычисляется по следующей формуле:

$$S_+^t(\tau) = \sum_{a=a^*}^{A} \varepsilon_{ra} \cdot k_{ra} \cdot s_a^{t+\tau} = \sum_{a=a^*}^{A} \varepsilon_{ra} \cdot k_{ra} \cdot \varphi\left(q_a^t; \tau\right) \qquad (61)$$

где r=1, …, R – условный порядковый номер управленческого решения по конвертации ликвидных активов в абсолютно ликвидные; R – возможное количество таких решений;

ε_{ra} – индикаторная функция такая, что:

$$\varepsilon_{ra} = \begin{cases} 1, \text{ если при } r-\text{ом управленческом решении конвертируется } a-\text{ый ресурс;} \\ 0, \text{ в противном случае} \end{cases}$$

k_{ra} – коэффициент, описывающий долю a-го ресурса, подлежащего конвертации при r-ом решении.

Шкала значений ФУ имеет градации, описанные в таблице 7.

Для обеспечения ФУ в (t+τ)-ый момент должно выполняться условие:

$$S^{t+\tau} + S_{+}^{t}(\tau) \geq Z^{t+\tau+1} \qquad (62)$$

Алгоритм имитации движения денежных средств и оценки ДФР состоит в следующем.

1) Для каждого t=1,…, T в рамках составления бюджета движения денежных средств рассчитываются значения W^t и S^t.

2) Для каждого t=1,… T проверяется неравенство $s_1^t \geq Z^{t+1}$.

Если оказывается, что оно выполнено на всём рассматриваемом периоде, то ДФР обеспечена и работа алгоритма прекращается.

Если в некоторый t-ый момент выявлен кассовый разрыв $\left(s_1^t < Z^t\right)$, то требуются идентификация состояния ДФР, и коррекция оценок ДФР с момента t с учётом конвертации части ликвидных активов для погашения дефицита.

3) Вычисляется достаточность наиболее ликвидных активов.

Пусть все активы выстроены по номерам в порядке убывания их ликвидности (это предполагалось в предшествующем описании модели, хотя явно и не декларировалось).

3.1) Проверяется условие:

$d_1^t = D^t - s_1^t$, где левая часть – остаток дефицита после использования ресурса с номером a=1, т. е. денежных средств на расчётных счетах и в кассе предприятия.

Таблица 7 – Градации мгновенных значений ДФР предприятия

Состояние ресурсов	*Градация*	*Комментарий*
$s_1^t \geq \sum_{j=1}^{J} z_j^{t+1}$	Абсолютная достаточность финансовых ресурсов в момент t	Предприятие имеет положительный баланс движения денежных средств, принятие дополнительных мер для обеспечения выполнения платёжных обязательств не требуется
$\left(s_1^t < \sum_{j=1}^{J} z_j^{t+1} \right) \& \left(S^t > \sum_{j=1}^{J} z_j^{t+1} \right)$	ДФР обеспечена	Имеются признаки зарождения негативных процессов; требуется анализ
$\left(S^t \leq \sum_{j=1}^{J} z_j^{t+1} \right) \& \left(Q^t > \sum_{j=1}^{J} z_j^{t+1} \right)$	Состояние неопределённости	Вопрос о ДФР решается, исходя из возможности конвертации менее ликвидных активов в абсолютно ликвидные активы; выполнение обязательств приводит к сокращению ресурсной базы, возможно, повлечёт дополнительные затраты на обслуживание кредитов и займов, выплату пеней и т. п.
$Q^t \leq \sum_{j=1}^{J} z_j^{t+1}$	ДФР не обеспечена; кризис	Предприятие не имеет необходимого объёма ликвидных средств для выполнения платёжных обязательств

Примечание к таблице 7. Оценка состояния ДФР на основе баланса бюджета движения денежных средств осуществляется исходя из правила, что средства для выплат по обязательствам в каждом элементарном временном периоде должны быть сформированы к его началу, т. е. в предыдущие моменты, а выручка формируется на конец этого элементарного временного периода и будет доступна к использованию только в следующие моменты времени.

Если $d_1^t \le 0$, то актива с номером a=1 полностью достаточно, и следует только вычислить k_1, чтобы оценить потенциал ДФР для последующих моментов. Для вычисления k_1 решается уравнение:

$k_1 = D^t / s_1^t$.

Если $d_1^t > 0$, то k_1:=1 и осуществляется переход к оценке возможностей использования актива с номером a=2, т. е. к шагу 3.2) (здесь значок := означает оператор «присваивания»). Так продолжается до тех пор, пока не будет выполнено условие $d_{a^+}^t \le 0$ на некотором a^+-ом шаге.

На каждом шаге 3.а) ($a \le a^+$) проверяется условие:

$d_a^t = d_{a-1}^t - s_a^t = d_{a-1}^t - \varphi_a\left(q_a^1; (t-1)\right)$.

Если $d_a^t > 0$, то k_a:=1 и осуществляется переход к оценке возможностей использования актива с номером (a+1), т. е. к шагу 3.a+1).

В противном случае, рассмотренных активов достаточно и следует только вычислить k_a, чтобы оценить потенциал ДФР для последующих моментов.

Для вычисления k_{a^+} решается уравнение:

$k_{a^+} = d_{a^+}^{t'} / s_{a^+}^{t'}$.

4) Для каждого актива с номером $a<a^+$ справедливо s_a=0;

если $a^+ \le a^*$, то $s_{a^+} = k_{a^+} \cdot s_{a^+}^0$, где $s_{a^+}^0$ - первоначальный объём a^+-го актива;

если $a^+ > a^*$, то $q_{a^+} = k_{a^+} \cdot q_{a^+}^0$, где $q_{a^+}^0$ - первоначальный объём a^+-го актива по балансовой (или рыночной) стоимости.

5) Для последующих временных моментов (t+1), (t+2), …, T проводится расчёт бюджета движения денежных средств с учётом уменьшения доходности использованных активов, а также штрафов и пеней, если за счёт ликвидных активов не удалось полностью погасить платёжные обязательства, возникшие в t-ом году.

По анализу динамики мгновенных оценок ДФР можно делать выводы об интегральной ДФР на некотором интересующем временном интервале, руководствуясь правилами, сведёнными в таблицу 8.

Таблица 8 – Правила идентификации состояния ФУ при прямой оценке на интервале планирования или прогнозирования

ДФР абсолютна	Бюджет движения денежных средств имеет постоянный положительный баланс
ДФР обеспечена	Бюджет движения денежных средств имеет итоговый положительный баланс, общий объём ликвидных активов уменьшился, но не более чем вдвое
ДФР обеспечена не надёжно	Бюджет движения денежных средств имеет итоговый положительный баланс, общий объём ликвидных активов практически использован
ДФР не обеспечена	Бюджет движения денежных средств имеет итоговый отрицательный баланс (на конец рассматриваемого периода), но не превышает стоимость необоротных активов; запас ликвидных активов использован
Кризис, банкротство	Бюджет движения денежных средств имеет итоговый отрицательный баланс (на конец рассматриваемого периода) и превышает стоимость необоротных активов; запас ликвидных активов использован

Для учёта различных неблагоприятных факторов в модель могут вноситься возмущения в виде увеличения затрат и уменьшения прибыли. Для этих возмущений запускается выше описанный алгоритм, начиная с момента ввода возмущения. Если некоторые воздействия застрахованы, то для погашения затрат или компенсации потерянной прибыли используются страховые выплаты. С другой стороны, результаты использования описанной модели могут быть полезны для принятия решения о страховании.

3.4. Общая схема использования математической модели оценки потенциала финансовых ресурсов предприятия

Общая схема использования математической модели ФУ предприятия, объединяющей представленные в настоящем разделе модели и методики, отражена на рисунке 10.

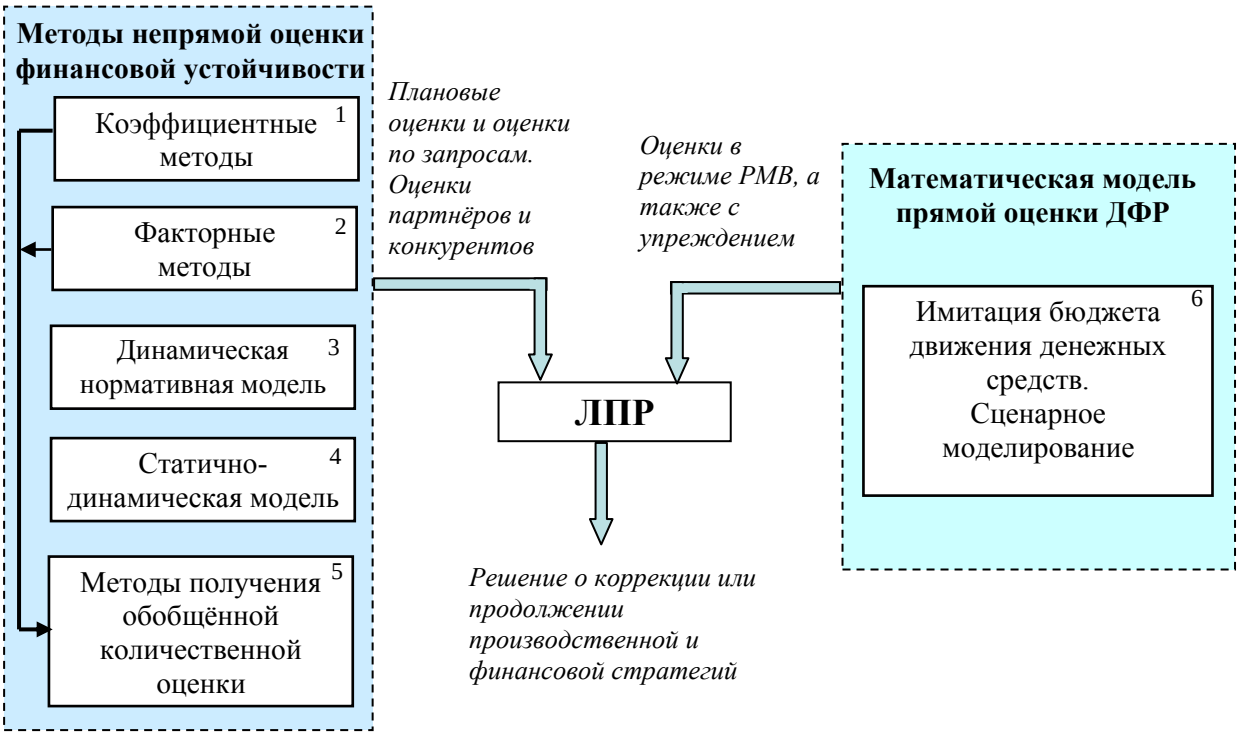

Рисунок 10 – Схема использования математической модели оценки потенциала финансовых ресурсов предприятия

Модели непрямой оценки носят между собой альтернативный характер. Их использование и интерпретация зависят от методологических предпочтений ЛПР и наличия статистики. Как правило, они применяются для периодической оценки по результатам отчётных периодов. Однако в целях более внимательного наблюдения над состоянием финансовых ресурсов предприятия, а также при наличии автоматизированных технологий анализа бухгалтерской отчётности и представления информации, расчёты могут проводиться еженедельно и ежедневно, а их результаты предоставляться ЛПР в регламентном режиме или по запросу.

Модели и методики непрямой оценки могут использоваться для анализа ФУ контрагентов, партнёров и конкурентов по общедоступной или предоставляемой ими информации о бухгалтерском балансе. Использовать для этих целей модели прямой оценки ДФР невозможно, поскольку недоступна оперативная и плановая информации других предприятий.

Для оценки ДФР предприятия (его способности платить по своим обязательствам) в реальном масштабе времени (далее – РМВ) используется модель, указанная на рисунке 10 в блоке 6. С помощью этой модели можно моделировать различные сценарии в полном пространстве входных и выходных потоков финансовых ресурсов, а также с учётом изменения различных условий внешней по отношению к предприятию среды.

Уязвимость предложенной в настоящей работе модели прямой оценки ДФР связана с неполным учётом возможных изменений внешних факторов. Философия моделей непрямой оценки по умолчанию требует наличия некоторого «запаса прочности» на никак неопределённые ситуации. Такой запас не предполагается в моделях прямой оценки. В связи с этим возможна ситуация, когда модель прямой оценки даёт положительный результат, а модели непрямой – напротив. Адекватность оценок в данном случае зависит от поведения внешней среды и того, насколько адекватно (с каким запасом) оно отражено в модели прямой оценки.

Рассмотренная модель прямой оценки может быть встроена в механизм оценки рисков для проектов и предприятий с учётом мер защиты (применения ПОС), предложенный в разделе 2.1.

На каждом такте выявляются рисковые события, связанные с задержками входного потока, а также другие аналогичные события, приведшие (могущие привести) к кассовым разрывам. С помощью указанной модели прямой оценки ДФР вычисляются возможности осуществления необходимых платежей и рассчитывается остаточный ущерб в финансовом измерении. При этом остаточный ущерб формируют следующие слагаемые:

- штрафы и пени за задержку платежей, если ликвидных активов предприятия или проекта не хватило для оплаты;
- потери из-за конвертации ликвидных активов в денежные средства по цене ниже их стоимости из-за срочности;
- потери доходности ликвидных активов, вследствие их использования для предотвращения задолженностей в платежах и кассовых разрывов (например, банковский процент, штрафы за досрочное снятие средств с депозита и т. п.);

- вероятность нарастания социальной напряжённости на предприятии и снижения качества труда, если речь идёт о недостатке денежных средств для выплаты заработной платы и различных социальных пособий;

- возможно и другое.

В заключение раздела важно отметить, что, вероятно, невозможно найти объективные основания для абсолютных оценок ФУ (потенциала финансовых ресурсов) предприятия и их однозначной интерпретации на уровне физических законов. Оценки и анализ ФУ осуществляются для определения перспектив выживаемости предприятия, его защиты от банкротства. В то же время результат выживания и шансы избежать банкротства во многом зависят от поведения заинтересованных акторов – терпения, доверия и лояльности кредиторов, поддержки органов государственного и муниципального управления, разворотливости управленцев по манипулированию финансовыми ресурсами, в частности, и производственным потенциалом предприятия, в целом, и т. п. Любые расчёты и оценки ФУ предоставляют лишь информацию о складывающихся или сложившихся тенденциях, неблагоприятных факторах для размышления и принятия решения о коррекции или сохранении финансовой политики и хозяйственной деятельности.

Если все методы дают положительные оценки, то проблем с оценкой ФУ нет. Высокая квалификация от ЛПР требуется, если оценки, полученные с помощью разных моделей, не совпадают.

Заключение

В настоящей монографии предпринята попытка найти объективное основание для методологических подходов к решению задач развития и обеспечения безопасности хозяйствующих субъектов и увязать единым механизмом процессы управления жизнедеятельностью предприятия на уровне повседневности и в стратегической перспективе. Это основание обнаружено в первичных мотивах деятельности живых систем, к которым относятся организационные системы и их разновидность – хозяйствующие субъекты, и заключается оно в стремлении к существованию в сколь угодно далёкой перспективе. При этом под существованием понимается полноценная реализация своего потенциала, удовлетворение интересов.

Использование этого основания позволяет эффективно реализовывать проектный подход при управлении предприятием, избавляться от симулякров в аналитической работе и фактически бесполезных и неиспользуемых практиками методических подходов и моделей.

Парадигма безопасного существования снимает проблему соотношения безопасности и развития, определяя, что развитие есть процесс, направленный на обеспечение безопасности (безопасного существования). При этом обеспечение конкурентоспособности, технологического лидерства, приобретение статуса социального ответственного предприятия и другие цели и задачи приобретают статус частных целей и задач в рамках обеспечения безопасного существования. Эта парадигма предполагает комплексное использование теории систем, теории живых систем, микроэкономики, аксиологии и других научных дисциплин. Она беспрепятственно может быть применена к исследованию и описанию безопасного существования региональных и глобальных социально-экономических систем. В этом случае потребуется уже привлечение теории катастроф, теории самоорганизации и некоторых других.

Деятельность по обеспечению безопасности должна предусматривать управление большой сложной (разнообразной) системой, подготовку и реализацию превентивных мер и, безусловно, оперативность. В полной мере невозможно реализовать эти требования

без технологичности в работе, без мониторинга состояния безопасности предприятия, без готовности к отражению угроз по наработанным сценариям, без чётких методик и инструкций, явно фиксирующих объективные грани порядка вещей в рассматриваемой проблематике. В то же время всё предусмотреть и полностью формализовать в проблематике стратегического управления, включая обеспечение безопасности невозможно. В связи с этим методическое и программно-инструментальное обеспечение этой деятельности должно предусматривать комплексное использование информационных технологий различного уровня формализации, обеспечивать эффективные организационные механизмы извлечения экспертного знания, поддержку творческого подхода.

Системная целостность, предметная универсальность и операциональная конкретность предложенной методологии позволяют рассматривать её как основу для разработки автоматизированной информационной технологии управления обеспечением безопасного существования предприятия.

В заключение целесообразно коснуться соотношения рассмотренной парадигмы безопасного существования и теории жизненного цикла предприятия, рассматривающей фазы его становления, развития, процветания и угасания. В более мягком и реальном варианте речь идет о жизненном цикле деловой активности предприятия. Сторонники теории жизненного цикла декларируют обязательность периодических (даже гармонических) колебаний деловой активности предприятия (см., например, [111-113]). Однако при эффективном управлении предприятие не обязательно должно остро переживать эти фазы, по крайней мере, заметно для стороннего наблюдателя. Оно может испытывать лишь в той или иной степени проявленности флуктуации на траектории существования. Крупное предприятие с диверсифицированным производством при умелом упреждающем руководстве, своевременном технологическом переоснащении по оптимизированной процедуре может сколь угодно долго существовать без заметных спадов. С другой стороны, и мелкий бизнес, удовлетворяющий естественные потребности людей, например, булочная-пекарня или парикмахерская, также может стабильно процветать, если не появятся конкуренты, но это уже другая история. В

то же время циклы хорошо описывают существование технологий, продукции, проектов, организационных форм. Эти циклы влекут перманентное обновление предприятия вплоть до замены всего его сущего через какое-то время. Предприятие постепенно становится другим фактически, сохраняя, возможно, название, бренды, отраслевую принадлежность, этические традиции, историю, гудвилл и т. п.

В этом случае можно провести аналогию с популяцией живых организмов. Организмы ведут борьбу за индивидуальное и популяционное (видовое) существование, сами тем не менее по очереди отмирая, но в процессе жизнедеятельности сохраняя популяцию и вид, возможно, с накоплением новых признаков и в других ареалах обитания. Кроме того, смысл существования предприятия, как было отмечено в главе 1, обнаруживается в интересах людей, имеющих отношение к предприятию. Способы и средства удовлетворения своих интересов для людей вторичны. Какая разница, что производить, если это полезный продукт (социальная значимость, нравственные императивы) и за него хорошо платят (материальное благополучие)? В этой связи носители интересов предприятия субъективно не воспринимают обновление предприятия в каких-то частях, как его переход из одной фазы существования (фазы цикла) в другую. Для них предприятие продолжает непрерывное существование с тем или иным успехом.

Автор идеи концепции жизненного цикла предприятия Дж. Гарднер, проводя аналогию предприятия с живым организмом, отмечал, что предприятие может просуществовать до ликвидации несколько лет или сколь угодно долго. На уровне математической абстракции любую прямую можно описать как кривую, отражающую колебательный процесс с бесконечным периодом. Остаются ли в этом случае объективные основания для концепции жизненного цикла предприятия (не технологии, не продукта)?

Парадигма существования фактически поглощает подходы к анализу деятельности предприятий, использующие категорию жизненного цикла предприятия (или деловой активности) и служит основанием для формирования механизмов управления предприятием, позволяющих избегать не только его ликвидации, но и глубоких спадов в деловой активности, как организационной системы-среды реализации интересов его стейкхолдеров.

Список использованной литературы

1 Литвиненко А.Н., Ковтунова С.Ю. Разработка типовой структуры механизма обеспечения экономической безопасности // Вестник Санкт-Петербургского университета МВД России. № 4 (48), 2010. С. 137-144.

2 Багдасарян В.Э. Витальный подход к сложным социальным системам // Витальный подход к сложным социальным системам. Материалы научного семинара. Вып. № 6. М.: Научная экспертиза, 2013. С. 7-70.

3 Клейнер Г.Б. Стратегия предприятия. 2008. –М.: Издательство «Дело» АНХ, 568 с.

4 Мусин М.М. Управление экономическими интересами : учебное пособие для вузов / VI. М. Мусин . – VI.: Гардарики. 2006. – 287 с.

5 Трошин Д.В. Проблемы обеспечения экономической безопасности хозяйствующих субъектов России в условиях глобализации // Национальные интересы: приоритеты и безопасность. № 12 (249), 2014 г. С. 52-66.

6 Лечиев А.С. Развитие концепта «Безопасность жизнедеятельности в истории философской мысли» // Электронный научный журнал «ГосРег», 2014, № 4.

7 Суглобов А.В., Хмелев С.А., Орлова Е.А. Экономическая безопасность предприятия. М., изд-во «Юнити-Дана». 2012 г. 272 с.

8 Лебедева Н.А. Экономическая безопасность предприятия. Цифровая книга. Изд-во «МАБИВ». 2012 г. 162 с.

9 Грунин О., Макаров А., Михайлов Л., Михайлов А., Скаридов А. Экономическая безопасность. М., изд-во «Дрофа». 2010 г. 272 с.

10 Основы экономической безопасности. Уч.-практ. пос. Под ред. Олейника Е.А. - М. : ЗАО Бизнес-школа «Интел-Синтез», 1997 г.

11 Грунин О.А., Грунин С.О. Экономическая безопасность организации – СПб. : «Питер», 2002.

12 Судоплатов А.П., Лекарев С.В. Безопасность предпринимательской деятельности. М.: «ОЛМА-ПРЕСС», 2001. С. 3.

13 Козанченко А.В., Пономарёв В.П., Ляшенко А.Н. Экономическая безопасность предприятия: сущность и механизм обеспечения / Монография.- Киев: Либра, 2003. – 280 с.

14 Гапоненко В.Ф., Беспалько А.А., Власков А.С. Экономическая безопасность предприятий. Подходы и принципы. – М.: Издательство «Ось-89», 2007.

15 Вдовина С.Б. Инструменты качественной оценки проектных рисков // Экономическая безопасность России: проблемы и перспективы: материалы Международной научно-практической конференции. Нижегородский государственный технический университет им. Р.Е. Алексеева. – Нижний Новгород, 2013. – 480 с.

16 Зимина Л.Е. Этическая безопасность предприятия как составная часть экономической безопасности // Экономическая безопасность России: проблемы и перспективы: материалы II Международной научно-практической конференции; Нижегород. гос. техн. ун-т им. Р.Е. Алексеева. – Нижний Новгород, 2014. – 492 с.

17 Чужмаров А.И. Обеспечение экономической безопасности предприятий как основной фактор эффективного функционирования отрасли промышленности // Вестник Научно-исследовательского центра корпоративного права, управления и венчурного финансирования. - М. 2007. – 63 с.

18 Басалай С.И. Экономическая оценка последствий реализации угроз и управление экономической безопасностью отрасли национальной экономики // Транспортное дело России. 2008. № 4. С. 13-15.

19 Илышева Н.Н., Каранина Е.В. Методологические аспекты формирования, оценки и совершенствования системы стратегического анализа и управления бизнес-рисками предприятия // Экономический анализ: теория и практика. 11 (362) – 2014. С. 23-30.

20 Власенко М.Н. Методология обеспечения экономически эффективности и безопасного функционирования хозяйствующих субъектов в условиях регионального рынка: системный подход // Национальные интересы: приоритеты и безопасность. 5 (146) – 2012. С. 40-47.

21 Разгонов С.А. Основные особенности системы экономической безопасности отрасли автомобилестроения в современных условиях // Transport Business in Russia. С. 87-80.

22 Машков Д.М. Инструменты управления рисками промышленных предприятий // Вестник Саратовского госагроуниверситета им. Н.И. Вавилова. 2015. № 2.

23 Ильин М.Е., Фёдорова Л.А. Модель оценки устойчивости развития наукоёмких производство авиационной промышленности // Экономический анализ: теория и практика. 4 (355) – 2014. С. 20-29.

24 Дадалко В.А., Питулько С.Ю. Экономическая безопасность аэрокосмической отрасли России. Минск: ИВЦ Минфина, 2010.

25 Инновационные преобразования как императив устойчивого развития и экономической безопасности России / под ред. В.К. Сенчагова. – М.: «Анкил», 2013 – 688 с.

26 Товстоношенко В.Н. Методологический подход к управлению рисками на предприятиях ракетно-космической промышленности // Вестник СибГАУ. № 1(53). 2014. С. 225-229.

27 Хрусталёв Е.Ю. Экономическая безопасность наукоёмкого предприятия: методы диагностики и оценки // Национальные интересы: приоритеты и безопасность. 13 (70) – 2010. С. 51-58.

28 Авдонин Б.Н., Стрельникова И.А., Хрусталёв Е.Ю. Механизмы снижения риска при создании высокотехнологичной наукоёмкой продукции // Аудит и финансовый анализ. 5’2011. С. 1-18.

29 Макаров Ю.Н., Хрусталёв Е.Ю. Экономическое обеспечение безопасного функционирования и развития ракетно-космических производств // Национальные интересы: приоритеты и безопасность. 5 (146) – 2012. С. 28-39.

30 Голощапова Л.В. Формирование механизма обеспечения безопасности экономического потенциала предприятия // Вектор науки ТГУ. Серия: Экономика и управление. 2012. № 4(11). С. 46-49.

31 Вишняков Я.Д. Общая теория рисков : учеб, пособие для студ. высш. учеб, заведений / Я.Д. Вишняков, Н. Н. Радаев. — 2-е изд., испр. — М. : Издательский центр «Академия», 2008. — 368 с 15ВЫ 978-5-7695-5396-7.

32 Качалов Р.М. Управление хозяйственным риском. – М.: Наука, 2002.

33 Моделирование рисковых ситуаций в экономике и бизнесе: М74 Учеб. пособие / А.М. Дубров, Б.А. Лагоша, Е.Ю. Хрусталев,

Т.П. Барановская; Под ред. Б.А. Лагоши. - 2-е изд., перераб. и доп. - М.: Финансы и статистика, 2001. - 224 с.

34 Чернова Г.В., Кудрявцев А.А. 4-45 Управление рисками: учеб, пособие. - М.: ТК Велби, Изд-во Проспект, 2005. - 160 с.

35 Шапкин А.С, Шапкин В.А. Экономические и финансовые риски. Оценка управление, портфель инвестиций. — 7-е изд. — М.: Издательско-торговая корпорация «Дашков и К°», 2009. — 544 с.: ил.

36 Дубров А.М., Лагоша Б.А., Хрусталёв Е.Ю. Моделирование рисковых ситуаций в экономике и бизнесе. – М.: Финансы и статистика, 2001.

37 Эльжбета Островская. Риск инвестиционных проектов М.: ЗАО «Издательство «Экономика» Москва 2004 - 269 с.

38 Поздеев В.Л. Анализ в системе экономической безопасности предприятия // Инновационное развитие экономики, № 2(19), 2014. С. 38-47.

39 Минаев Г.А. Безопасность организации. М., изд-во «КНТ». 2009 г. 440 с.

40 Минаев Г.А. Образование и безопасность: учеб. пособие / Г.А. Минаев. – М.: Университетская книга; Логос, - 2009. – 312 с. (Новая университетская библиотека).

41 Морозюк Ю.В. Индикативные составляющие экономической безопасности организации // Вестник Финансовой академии, № 4, 2006. С. 50-60.

42 Основы обеспечения безопасности России: Учеб. пособие / М.И. Дзлиев, А.Д. Урсул; Рос.гос. торгово-экон. ун-т, НИИ проблем безопасности и устойчивого развития. – М.: ЗАО «Издательство «Экономика», 2003.

43 Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. – М., МЦНМО, 2002.

44 Иващенко Г.В. Какие теоретические основания необходимы Концепции национальной безопасности // «Навигут». 2003. № 5. Приложение к журналу «Безопасность Евразии».

45 Артемьев Н.В. Экономическая безопасность как научная категория // Микроэкономика. № 2, 2015 г. С. 36-41.

46 Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. - 1994, - № 12, - с. 5.

47 Сенчагов В.К. Экономическая безопасность России // ЭКО. - 2007. - № 5. - С. 7.

48 Тамбовцев В.Л. Объект экономической безопасности России // Вопросы экономики. - 1994, - № 12, - с. 45.

49 Авдийский В.И., Безденежных В.М. Экономическая безопасность как системообразующий фактор устойчивости сложных социально-экономических систем // Безопасность бизнеса, № 1, 2014. С. 2-5.

50 Авдийский В.И., Безденежных В.М. Неопределённость, изменчивость и противоречивость в задачах анализа рисков поведения экономических систем // Эффективное антикризисное управление. – С.-П., № 3 (66) – 2011. С. 46-61.

51 Новиков Д.А. Теория управления организационными системами. М.: МПСИ, 2005. – 584 с.

52 Селиванов А.И., Трошин Д.В. О методологических основаниях реализации закона от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации» // Экономика. Налоги. Право. 3/2015. С. 18-23.

53 Трошин Д.В. Метафизика целеполагания в стратегировании // Национальные интересы: приоритеты и безопасность. № 46 (235) 2013 г. С. 57-66.

54 Селиванов А.И. Субъектные основания теории и методологии экономической безопасности // Экономическая безопасность России: проблемы и перспективы: материалы II Международной научно-практической конференции; Нижегород. гос. техн. ун-т им. Р.Е. Алексеева. – Нижний Новгород, 2014. – 492 с.

55 Урсул А.Д., Романович А.Л. Концепция устойчивого развития и проблема безопасности. [Электронный ресурс] URL: http://www.philosophy.nsc.ru/journals/philscience/11_01/05_ursul.htm. Дата обращения 23.01.2014 г.

56 Клайн М. Математика. Утрата определённости. – М.: Мир, 1984.

57 Смирнов П.И. Ценность: стимул деятельности и одно из основных понятий социологии // Теоретический журнал Credo new. 2011. № 1 (65). С. 139-157.

58 Смирнов П.И. Потребность: стимул деятельности и одно из основных понятий социологии. // Теоретический журнал «Credo new». - 2010. - № 4 (65). - с. 139-157.

59 Логунов А.Б. Региональная и национальная безопасность: Учебное пособие. – 3-е изд., перераб. и доп. – М.: Вузовский учебник: ИНФРА-М, 2014. – 457 с.

60 Трошин Д.В. Онтология безопасности: парадигма существования // Национальные интересы: приоритеты и безопасность, № 23 (260), С. 40-48.

61 Трошин Д.В. Имитационная модель состояния финансовой устойчивости хозяйствующего субъекта // Финансовая аналитика: проблемы и решения», 41 (179), 2013. С. 41-48.

62 Леонтьев Р.Г., Веретенников Н.П., Адаменя А.И., Орлов А.Л. Отраслевые корпорации и региональный бизнес: интеграция интересов. Научное издание. – М.: ВИНИТИ РАН, 2009. – 616 с. Ил.

63 Балацкий Е.В. Новые характеристики глобального капитализма // Общество и экономика, № 3, 2013, с. 59-80.

64 Салихов Б.В. Духовно-нравственные основы развития современной российской экономики: Монография. – М.: Издательство МГОУ, 2009. – 160 с.

65 Гринберг Р.С. Свобода и справедливость. Российские соблазны ложного выбора / - М.: Магистр : ИНФРА-М, 2012. – 416 с.

66 Андреев А.П., Селиванов А.И. Русская традиция. М., 2004 г.

67 Злоказов В.Б. Психология и религия глазами кибернетики / Ценностный дискурс в науках и теологии. // Рос. акад. наук, Ин-т философии, Рос. гос. гуманитар. ун-т; Отв. ред. И.Т. Касавин и др. – М.: ИНФРАН. 2009. С. 351.

68 Моисеев Н.Н. Восхождение к Разуму. М., 1993.

69 Арнольд В.И. «Жёсткие» и «мягкие» математические модели. URL: http://www.pseudology.org/state/katastropha_models.htm. [Электронный ресурс]. Дата доступа 13.04.2015.

70 Трошин Д.В. Скаляризация векторных предпочтений: преодоление примитивизации // Эффективное антикризисное управление: преодоление примитивизации. С.-П. № 3(78), 2013. С. 88-94.

71 Клейнер Г.Б. Ресурсная теория системной организации экономики // Российский журнал менеджмента, 2011, Т. 9, №. 3. С. 3-28.

72 Шаныгин С.И. Стратегическое управление организацией: теоретико-методологический подход. СПб.: Наука, 2011. – 187 с.

73 Иода Е.В., Ерусалимский В.М. Управление инновационной деятельностью в регионе на основе концепции «риск-ресурс». Монография. Тамбов: Никитина М.А., 2010. - 236 с.

74 Лепский В.Е. Исходные посылки совершенствования системы национальной безопасности России (субъектно-ориентированный подход) // Международный научно-практический междисциплинарный журнал «Рефлексивные процессы и управление». № 1, 2007, январь-июнь, том 7.

75 Кутахов Ю.Л., Явчуновская Р.А. Человек. Полиэтнический мир. Безопасность. СПб., 1998.

76 Деминг У. Эдвард. Новая экономика / Пер. с англ. Т. Гуреш. – М.: Эксмо, 2008. – 208 с. – (Библиотека ЭКСПЕРТА).

77 Пищулин О.В. Совершенствование корпоративного управления в условиях глобализации и инновационного развития (монография). – М.: Вольное экономическое общество Москвы, Этносоциум, 2014. – 313 с.

78 Воробей О. Новые принципы управления // Проблемы менеджмента в условиях глобализации информационного пространства: сборник докладов Международной научно-практической конференции. – СПб.: Издательство Санкт-Петербургский университет управления и экономики, 2012. – 216 с.: ил. – с. 182.

79 Таллеб Н.Н. Чёрный лебедь. Под знаком непредсказуемости / Пер. с англ. В. Сот, А. Бердичевского, М. Костионовой, О. Попова под редакцией М. Тюнькиной. — М.: Издательство КоЛибри, 2009. - 528 с.

80 Ворожихин В.В. Компьютерное прогнозирование рисков на основе вирусной теории рисков // Межотраслевая информационная служба (МИС) / № 2, 2015. С. 46-51.

81 Трошин Д.В. Методический подход к оцениванию безопасности хозяйствующего субъекта // Экономический анализ: теория и практика. № 29 (428), 2015 г. С. 47-60.

82 Майрон Трайбус. Вирусная теория менеджмента. [Электронный ресурс]. URL: http://www.deming.ru/TeorUpr/VirTeorMen.htm. Дата обращения 18.03.2015.

83 Семиков В.Л. Рискогенность руководителей в системе МЧС России. [Электронный ресурс]. URL: http://agps-2006.narod.ru/ttb/2007-5/05-05-07.ttb.pdf. Дата обращения 18.03.2015.

84 Кини Р.Л., Райфа Х. Принятие решений при многих критериях: предпочтения и замещения. М.: Радио и связь, 1981. 560 с.

85 Яковлева И.Н. Оценка финансовых рисков на базе бухгалтерской отчетности //Журнал «Справочник экономиста», № 5, 2008 год.

86 Гранатуров, В. М. Экономический риск: сущность, методы измерения, пути снижения : учебное пособие. — 3-е изд., перераб. и доп. — М.: Дело и Сервис, 2010. — 208 с.

87 Литвак Б.Г. Экспертные оценки и принятие решений. М.: «Патент», 1996. 271 с.

88 Губанов Д.А., Коргин Н.А., Новиков Д.А., Райков А.Н. Сетевая экспертиза / Под ред. чл.-кор. Д.А. Новикова, проф. А.Н. Райкова. – М.: Эгвес, 2010. – 168 с.

89 Погостинская Н.Н., Погостинский Ю.А., Павлюк Г.А. Инновационный подход к оценке финансовой устойчивости предприятия // Финансы, Деньги, Инвестиции, № 1/2013 (45).

90 Мельцас Е. Финансовая устойчивость – да, банкротство – нет! // РИСК: Ресурсы, информация, снабжение, конкуренция. 2011. № 3. –М. С. 403-406.

91 Абанин С.Л., Рязанцев Д.А. Финансовая устойчивость и финансовая гибкость как важнейшие характеристики финансового состояния компании // Финансы. Деньги. Инвестиции. № 4/2011 (40).

92 Моисеева Е.Г., Грязева М.А. Подходы к классификации финансовой устойчивости организации // Казанская наука, № 1, 2013. С. 61-64.

93 Мисхожев Э.Р., Кулебакина Л.Е. Формирование экономической устойчивости организации в условиях рыночной экономики // Вестник Государственной полярной академии. 2012, № 1(14), с. 96-99.

94 Бригхем Ю., Гапенски Л. Финансовый менеджмент / Пер. с англ. под ред. Ковалёва В.В. – СПб., Экономическая школа, 1997, Т.2.

95 Ковалёв В.В., Ковалев Вит.В. Анализ баланса или как понимать баланс – М.: Проспект, 2009.

96 Бернстайн Л.А. Анализ финансовой отчётности – М.: Финансы и статистика, 1996.

97 Шеремет А.Д. Комплексный анализ хозяйственной деятельности – М.: ИНФРА-М, 2009.

98 Гукова А.В., Киров А.В., Юдина Е.Н. Система управления финансовой устойчивостью фирмы в инновационной экономике // Дайджест-Финансы. 2012, № 11(215). С. 25-30.

99 Коряков А.Г. Управление предприятием на основе концепции устойчивого развития // Актуальные проблемы российской экономики и новые подходы к их решению: III Всероссийская научно-практ. конф., Москва, 29 марта 2012 г.: Сб. науч. тр. / НИЦ «Стратегия». – М.: МАКС Пресс, 2012. С. 53-56.

100 Крейнина М.Н. Финансовая устойчивость предприятия: оценка и принятие решений // Финансовый менеджмент. 2001. № 2. С. 15.

101 Грачёв А.В. Финансовая устойчивость предприятия: анализ, оценка и управление: Учебно-практическое пособие. М.: Изд-во «Дело и Сервис», 2004.

102 Бочаров В.В. Комплексный финансовый анализ. СПб.: Питер, 2005. 423 с.

103 Гиляровская Л.Т., Вехорева А.А. Анализ и оценка финансовой устойчивости коммерческого предприятия. СПб.: Питер, 2003. 256 с.

104 Смирнова Н.А. Методы анализа и оценки финансовой устойчивости предприятий / Контроллинг процессов: теория, практика: сборник научн. тр. – Н.Новгород: Изд-во Волго-Вятской академии государственной службы. 2011. С.133-147.

105 Финансы в нестабильной экономике / Под ред. проф. Н.Н. Погостинской. – СПб.: Изд-во МБИ, 2010. – 208 с.

106 Киров А.В. Информационно-аналитическая система управления финансовой устойчивостью фирмы // Финансовая аналитика: проблемы и решения 27(69) – 2011, с. 9-14.

107 Казакова Н.А., Федченко Е.А., Черепанова Л.А. Информационно-аналитическое обеспечение системы контроллинга финансовой устойчивости // Финансовая аналитика: проблемы и решения. 18(156) – 2013.

108 Кован С.Е., Кочетков Е.П. Финансовая устойчивость предприятия и её оценка для предупреждения банкротства // Экономический анализ: теория и практика, 15(144) – 2009, с. 52-59.

109 Гребенщикова Е.В. Финансовая устойчивость промышленного предприятия и способы её обеспечения: Дис…, Финансовая академия при Правительстве РФ, 2007.

110 Татаров С.В. Финансовая устойчивость фирмы как основа стратегии её развития // Известия Южного федерального университета. Технические науки. Таганрог. 2005. Т.52, № 8, с. 179-183.

111 Гарднер Дж. Жизненный цикл организации. М.: Бизнес-школа, 1991.

112 Никулина О.В. Управление предприятием по стадиям жизненного цикла в условиях инновационного развития // Экономический анализ: теория и практика. № 20 (227) – 2011. С. 29-40.

113 Линг В.В. Обзор основных концепций жизненного цикла предприятия // Экономика и предпринимательство, № 6 (ч.2), 2015 г. С. 735-739.

ПРИЛОЖЕНИЕ. Карта обследования потенциала обеспечения существования предприятия

№ п/п	*Компонента ПОС*	*Средства реализации компоненты ПОС*	*Порядок обследования компоненты ПОС*	*Оценка реализации компоненты ПОС*
1.	Финансовая устойчивость			
1.1.	Структура активов k_1=	1.1.1. Структура активов: 1.1.2. Динамика структуры активов: 1.1.3. Бюджет движения денежных средств:	Изучение документации. Изучение документации. Изучение документации.	*Оценивается по отдельным методикам с комплексным использованием статических и динамических методов.*
1.2.	Организационное и методическое обеспечение k_2=	1.2.1. Постоянный мониторинг состояния финансовой устойчивости: 1.2.2. Наличие методологии и информационных технологий анализа ситуации и синтеза решений: 1.2.3. Наличие квалифицированных финансистов, способных эффективно манипулировать ликвидами для обеспечения финансовой устойчивости. 1.2.4. Регламентация анализа финансовой устойчивости и манипулирования ликвидами:	Изучение практики работы. Изучение документации и практики. Изучение анкет. Беседы. Изучение практики работы. Изучение документации.	*1. Проведение постоянного мониторинга с использованием автоматизированных технологий, реализующих статические и динамические методы, оперативное манипулирование ликвидами – 1* *2. Проведение постоянного мониторинга офисными средствами, оперативное манипулирование ликвидами – 0,8* *3. Проведение периодического анализа офисными средствами, оперативное манипулирование ликвидами – 0,5* *4. Использование ограниченных экспресс-методов анализа – 0,2* *5. Ситуативное реагирование на кассовые разрывы – 0,1*
2.	Кадровый потенциал			
2.1.	Укомплектованность k_3=	2.1.1. Кадровая структура и укомплектованность:	Изучение кадровой документации.	*Оценивается от 0 до 1 в зависимости от процента*

		2.1.2. Система анализа качества труда: 2.1.3. Система комплектования:	Изучение документации и практики. Изучение документации и практики	*укомплектованности, уровня квалификации, среднего возраста, наличия системы анализа качества труда и системы комплектования.*
2.2.	Подготовка кадров k_4=	2.2.1. Организация подготовки и переподготовки кадров на предприятии: 2.2.2. Организация подготовки и переподготовки кадров в учебных заведениях и других внешних организациях:	Изучение документации и практики. Изучение документации и практики	*Оценивается от 0 до 1 в зависимости от удовлетворения потребностей в переподготовке кадров в заданные сроки.*
3.	Организация производства и уровень его оснащения			
3.1.	Технологи-ческая оснащённость k_5=	3.1.1. Степень износа оборудования и его структура по технологическим уровням: 3.1.2. Уровень автоматизации:	Изучение документации. Изучение документации	*Оценивается от 0 до 1 по отдельным методикам с учётом отраслевых требований к степени износа и уровню автоматизации.*
3.2.	Организация производства k_6=	3.2.1. Система мотивации труда и социальной защиты: 3.2.2. Система логистики: 3.2.3. Система анализа производственных процессов и взаимоотношений с поставщиками и потребителями:	Изучение документации и практики. Изучение документации и практики. Изучение документации и практики.	*Оценивается от 0 до 1 по отдельной методике.*
4.	Сеть партнёров и источников входных потоков			
4.1.	Структура кооперации k_7=	4.1.1. Вариативность системы поставщиков: 4.1.2. Вариативность системы потребителей:	Изучение документации и практики. Изучение документации и практики.	*1. Наличие надёжной кооперации и резервных вариантов – 1* *2. Наличие надёжной кооперации и*

				отсутствие резервных вариантов – 0,75 *3. Наличие ненадёжной кооперации и ограниченность резервных вариантов – 0,5* *4. Наличие ненадёжной кооперации и ограниченность резервных вариантов – 0,25* *5. Наличие ненадёжной кооперации – 0,1*
5.	Система страхования имущества, проектов и др.			
5.1.	Регламентация страхового обеспечения деятельности k_8=	5.1.1. Наличие внутренних правовых документов, определяющих порядок страхования деятельности и имущества: 5.1.2 Наличие методического обеспечения выбора страховых продуктов:	Изучение документации. Изучение документации.	*1. Документация полностью определяет порядок страхования, содержит методические положения по выбору страховых продуктов, страховых премий и других условий, а также выбору страховых компаний или участию в обществах самострахования– 1* *2. Порядок деятельности по страхованию регламентирован, однако методическое обеспечение утверждено на уровне общих рекомендаций 0,8* *3. Порядок страхования регламентирован полностью, методическое обеспечение отсутствует – 0,5* *4. Порядок страхования определен в общих чертах – 0,2* *5. Порядок*

				страхования на уровне локальных правовых актов не определён – 0
5.2.	Обеспечение этапов жизненных циклов продукции, имущества страховыми продуктами k_9=	5.2.1. Наличие договоров страхования или иных документов системы взаимного страхования.	Изучение договорной документации.	*Оценка определяется как процент застрахованных рисков в финансовом измерении, делённый на 100.*
6.	Система защиты интеллектуальной собственности			
6.1	Регламентация обеспечения защиты интеллектуальной собственности k_{10}=	6.1.1. Наличие внутренних правовых документов, определяющих порядок защиты интеллектуальной собственности:	Изучение документации.	*Оценка определяется по шкале от 0 до 1 в зависимости от полноты и качества локальной правовой базы по данному вопросу.*
6.2	Использование системы мониторинга неправомочного использования интеллектуальной собственности k_{11}=	6.2.1. Наличие организационных ресурсов для проведения мониторинга: 6.2.2. Наличие организационных ресурсов для правовой защиты интересов:	Изучение документации. Изучение документации. Беседы.	*1. Достаточные ресурсы для мониторинга и правовой защиты в мире – 1* *2. Ресурсы для мониторинга по миру и правовой защиты в России – 0,75* *3. Ресурсы для мониторинга по России и защиты по миру – 0,6* *4. Ресурсы для мониторинга и правовой защиты в России – 0,5* *5. Ресурсы для мониторинга в России – 0,3* *6. Ресурсы для правовой защиты в России – 0,15*
6.3	Патентование результатов интеллектуальной деятельности k_{12}=	6.3.1. Организационные ресурсы для патентования: 6.3.2. Финансовые ресурсы для патентования:	Изучение документации. Изучение документации, в т.ч. бухгалтерской.	*1. Квалифицированный штат, патентование РИД во всех странах потенциальных конкурентах -1* *2. Квалифицирован-*

				ный штат, патентования в странах – основных потенциальных конкурентах – 0,75 *3. Квалифицированный штат, патентование в наиболее вероятных странах конкурентах – 0,5* *4. Недостаточно квалифицированных штат патентование в наиболее вероятных странах конкурентах – 0,3* *5. Патентование исходя из ограниченных ресурсов на патентование – 0,15* *6. Отсутствие систематического патентования – 0*
7.	Инновационное развитие (научно-технический прогресс)			
7.1	Организация инновационной деятельности k_{13}=	7.1.1. Кадровые ресурсы реализации инновационных процессов: 7.1.2. Внутренняя регламентация инновационной деятельности: 7.1.3. Методическое обеспечение оценки РИД: 7.1.4. Практика проведения экспертных исследований и ситуационных анализов РИД:	Изучение документации. Беседы. Изучение документации. Изучение документации. Изучение документации. Беседы со специалистами	*1. Квалифицированный штат для реализации инновационных процессов, качественная регламентация в форме внутренних правовых актов, регулярная практика экспертных и сит. анализов – 1* *2. Штат для реализации инновационных процессов, внутренняя регламентация – 0,5* *3. Нештатные обязанности, регламентация в общих чертах – 0,1*
7.2	Программирование инновационной деятельности k_{14}=	7.2.1. Наличие программ развития производственных технологий:	Изучение документации.	*1. Обоснованные программы развития технологий, продуктовой линейки на основе все-*

		7.2.2. Наличие программ создания инновационных продуктов: 7.2.3. Систематический мониторинг и прогноз развития интересующих продуктовых секторов: 7.2.4. Оперативная организация исследований и разработка новшеств и инноваций:	Изучение документации. Изучение практики деятельности. Изучение практики деятельности.	*объемлющего мониторинга и прогноза с анализом рисков– 1* *2. Программы, обоснованные в общих чертах на основе периодического мониторинга основных секторов и конкурентов – 0,5* *3. Ситуативное реагирование – 0,1*
7.3	Мотивация инновационной деятельности и финансовое обеспечение k_{15}=	7.3.1. Финансовые ресурсы для создания инноваций: 7.3.2. Устойчивые взаимоотношения с кредитными организациями для финансирования инновационных проектов: 7.3.3. Система поощрения новаторов и инноваторов:	Изучение документации. Изучение договорной документации и практики работы. Изучение документации и практики применения.	*1. Эффективная система мотивации новаторов и инновационных менеджеров, устойчивое партнёрство с кредитными организациями и в рамках гос.-частного партнёрства – 1* *2. Формальная система мотивации новаторов и инновационных менеджеров, устойчивое партнёрство с кредитными организациями и в рамках гос.-частного партнёрства - 0,8* *3. Формальная система мотивации новаторов и инновационных менеджеров, ситуативный поиск партнёров для реализации инновационных проектов – 0,5* *4. Эффективная система мотивации новаторов и инновационных менеджеров, использование собственных средств – 0,3*

				5. Формальная система мотивации новаторов и инновационных менеджеров, использование собственных ограниченных средств – 0,1
8.	Информационное противоборство			
8.1.	Организационное обеспечение k_{16}=	8.1.1. Кадровые ресурсы для взаимодействия с общественностью и органами государственной власти и местного самоуправления: 8.1.2. Регламентация публичной деятельности и взаимоотношений с органами государственной власти и местного самоуправления:	Изучение документации. Изучение документации.	*1. Специальное штатное подразделение, укомплектованное квалифицированными специалистами, постоянный мониторинг – 1* *2. Специальное штатное подразделение, укомплектованное квалифицированными специалистами, ситуативное реагирование – 0,8* *3. Ответственный сотрудник, ситуативное реагирование – 0,5* *4. Отсутствие специально уполномоченных сотрудников, ситуативное реагирование – 0,2* *5. Отсутствие реакции – 0.*
8.2.	Материально-финансовое и коммерческое обеспечение k_{17}=	8.2.1. Финансовые и программно-технические средства для ведения мониторинга и подготовки информации для публичного пространства: 8.2.2. Система кооперации со СМИ и исполнителями печатных и медийных материалов:	Изучение документации и осмотр средств. Изучение документации и практики работы.	*1. Наличие современных средств обработки неструктурированных потоков информации, входного объёма популярных и специализированных СМИ в реальном режиме времени, наличие достаточной*

				статьи расходов на PR и устойчивых отношений со СМИ и другими партнёрами – 1 *2. То же, но без специальных средств обработки – 0,8* *3. То же, но при ограниченных объёмах СМИ – 0,5* *4. То же, но при ограниченных объёмах финансирования – 0,2*
9.	Предотвращение несанкционированного пересечения периметра территории (или проникновения в здание), а также провоза (проноса) ТМЦ			
9.1.	Инженерно-техническая защита периметра k_{19}=	9.1.1. Ограждение *(материал, высота, толщина, заглубленность основания, (не)сплошное, конструкция, дополнительное ограждение (козырек, «Спираль АКЛ» и т. п.), др.)*. 9.1.2. Предупредительное ограждение *(высота, конструкция (колючая проволока), ширина зоны отчуждения, контрольно-следовая полоса, др.)*. 9.1.3. Система охранного телевидения *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум,*	Внешний осмотр (ВнОсм). Изучение технической документации (ТехДок)[12] ВнОсм. Изучение ТехДок. ВнОсм. Изучение ТехДок. Проверка	*1. Пересечение периметра скрытно[13], а также без приспособлений, технических средств или инструментов (далее - снаряжение) невозможно - 1* *2. Пересечение периметра скрытно невозможно. Пересечение периметра затруднено - 0,85* *3. Пересечение периметра не представляет трудностей, но сделать это скрытно невозможно – 0,6* *4. Возможно скрыт-*

[12] Везде далее - в случае если охрана объекта (предприятия) осуществляется по договору с подразделением вневедомственной охраны МВД России, в ходе аудита изучается документация, относящаяся к работам по устранению недостатков и выполнению рекомендаций, отмеченных в акте последнего профилактического или внепланового обследования.

[13] «Скрытно» в данном случае означает, что действие может быть совершено в условиях, когда отсутствуют, в том числе на отдельных участках периметра, технические средства фиксации этого действия или караульные, непосредственно отвечающие за наблюдение (охрану) периметра. Другими словами, фраза «пересечь периметр скрытно невозможно» отражает не факт воспрепятствования проникновению на охраняемую территорию (или эвакуации с неё) со стороны охраны, а наличие средств и(или) сил, с помощью которых потенциально любой факт пересечения периметра фиксируется.

		тип видеонакопителя, поле наблюдения, др.). 9.1.4. Средства охранной сигнализации пересечения периметра *(прожектора, сирена, извещатели, шлейф сигнализации, сигнал на пульт охраны, др.)*. 9.1.5. Караульные собаки *(обученность, активность (агрессивность), место нахождения и степень свободы перемещения, количество на 100 м длины периметра, др.)*. 9.1.6. Посты охраны периметра *(количество на 100 м периметра и топология размещения, выучка охранников, средства оповещения (тревожной сигнализации), специальные средства и вооружение охранников, др.)*.	системы гарантирован. электропитан. (СГЭ) Проверка видеозаписей. Изучение ТехДок. Проверка срабатывания и СГЭ ВнОсм. ВнОсм. Выборочная проверка функциональной готовности охранников. Проверка средств связи и сигнализации. Изучение личных дел.	*ное пересечение периметра, но требуется снаряжение – 0,4* *5. Пересечение периметра затруднительно, но возможно совершить это скрытно – 0,25* *6. Возможно скрытное без затруднений пересечение периметра, но только пешим порядком - 0,1*
9.1.а.	Инженерно-техническая защита здания (сооружения) k_{20}=	9.1.а.1. Стены *(материал, толщина, др.)*. 9.1.а.2. Перекрытия пола первого этажа *(материал, толщина)*. 9.1.а.3. Потолочные перекрытия верхнего этажа *(материал, толщина)*. 9.1.а.4. Оконные проемы *(ударопрочность стекол, решетки, ставни (куда открываются, засовы, запоры), высота расположения окон первого этажа, возмож-*	ВнОсм. Изучение ТехДок. ВнОсм. Изучение ТехДок. ВнОсм. Изучение ТехДок. ВнОсм. Изучение ТехДок.	*1. Проникновение в здание или эвакуация из него скрытно, а также без приспособлений, технических средств или инструментов (далее - снаряжение) невозможны - 1* *2. Проникновение в здание или эвакуация из него скрытно невозможны. Проникновение в здание и эвакуация из него несанкционированны*

		ность проникновения в окна с пожарных лестниц, др.). 9.1.а.5. Двери *(материал, толщина, конструкция, петли, торцевые крюки, тамбуры, средства сигнализации, др.)*. 9.1.а.6. Запоры дверей *(тип замков, др.)*. 9.1.а.7. Система охранного телевидения по периметру здания, крыши *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*. 9.1.а.8. Средства охранной сигнализации проникновения в здание через окна, крышу, запасные двери, в т.ч. наружные двери в подвальные помещения *(прожектора, сирена, извещатели, шлейф сигнализации, сигнал на пульт охраны, средства раннего обнаружения, др.)*.	ВнОсм. Изучение ТехДок. ВнОсм. Изучение ТехДок. Проверка работоспособности замков. ВнОсм. Изучение ТехДок. Проверка СГЭ. Проверка видеозаписей. Осмотр аппаратуры. Изучение ТехДок. Проверка срабатывания (выборочно). Проверка СГЭ	*м (необычным) образом затруднены - 0,85* *3. Проникновение в здание и эвакуация из него не представляют серьезных трудностей, но сделать это скрытно невозможно – 0,6* *4. Возможно скрытно проникнуть в здание или покинуть его, но для этого требуется специальное снаряжение – 0,35* *5. Проникновение в здание затруднительно, но возможно совершить это скрытно и без специальной подготовки – 0,15*
9.2.	Инженерно-техническая защита контрольно-пропускных пунктов, ворот, служебных проходов (далее - КПП) k_{21}=	9.2.1. Въездные ворота (КПП для проезда транспорта) *(высота, оборудование средствами дополнительного ограждения, запирающие и блокирующие устройства, жесткая фиксация в закрытом состоянии, средства автоматического открывания, устойчивость к механическому*	ВнОсм. Изучение ТехДок.	*1. Перемещение грузов и проход людей через КПП находится под постоянным наблюдением, в т.ч. с использованием технических средств. Несанкционированный проход и проезд физически затруднён.*

		воздействию, устройства для ограничения скорости движения автотранспорта, противотаранные устройства, конструкции и заграждения, шлюзовая система, глазок, средства охранного телевидения и сигнализации, освещение, др.). 9.2.1.а. Шлагбаум *(средства автоматического открывания, устойчивость к механическому воздействию, средства охранного телевидения и сигнализации, др.)*. 9.2.2. Технические средства контроля вывоза грузов *(весы, эстакады (для осмотра железнодорожного транспорта – вышки с площадками), средства ДОСмотра, электронные пропуска (электронные маркировки ТМЦ), средства передачи и отображения данных о вывозе груза, поступающие на КПП в автоматизированном режиме из мест отгрузки и учета вывозимых грузов, др.)*. 9.2.3. Служебный проход *(помещение для хранения и оформления пропусков, помещение для сотрудников охраны, характеристика двери на КПП, решетки на окнах, средства охранного телевидения обстановки на КПП, средства охранной сигнализации)*. 9.2.4. Система контроля и управления доступом *(преграждающие устройства, устрой-*	ВнОсм. Изучение ТехДок. Изучение ТехДок. Проверка работоспособности путём наблюдения ВнОсм. Изучение ТехДок. Проверка средств сигнализации на	*Имеются средства надёжной идентификации личности и грузов – 1* *2. Провоз грузов и проход людей через КПП находится под постоянным наблюдением, в т.ч. с использованием технических средств. Имеются технические средства надежной идентификации личности и грузов – 0,8* *3. Провоз грузов и проход людей через КПП находится под постоянным контролем, в т.ч. с использованием технических средств. Несанкционированный проход и проезд физически затруднен. Технические средства идентификации личности и грузов отсутствуют – 0,6* *4. Технические средства контроля провоза грузов и прохода людей через КПП отсутствуют. Несанкционированный проход и проезд физически затруднен. Технические средства идентификации личности и грузов отсутствуют – 0,3*

		ства ввода идентификационных признаков, устройства управления доступом, защита от несанкционированного проникновения к программным средствам УУ, автономное электропитание, выдача сигналов тревоги, протоколирование, др.):	срабатывание. Проверка СГЭ. Изучение документации. Проверка работоспособности. Натурное испытание системы защиты от несанкционированного доступа. Проверка СГЭ	
9.3.	Инженерно-техническая защита водопропусков, воздушных трубопроводов, подземных коллекторов k_{22}=	9.3.1. Средства предотвращения проникновения *(решетки, дополнительные ограждения)*. 9.3.2. Средства охранной сигнализации на разрушение и открывание *(прожектора, сирена, извещатели, шлейф сигнализации, сигнал на пульт охраны, др.)*.	ВнОсм. Изучение ТехДок. Осмотр аппаратуры. Изучение ТехДок. Проведение эксперимента на срабатывание (выборочно). Проверка СГЭ.	*1. Скрытное приближение к водопропускам, воздушным трубопроводам, подземным коллекторам невозможно, также невозможно помещение в предметов, в том числе мелких (имеющих по каждому из, хотя бы, двух измерений длину менее 50 мл), без специальных средств взлома инженерной защиты-1* *2. Скрытное приближение к водопропускам, воздушным трубопроводам, подземным коллекторам невозможно, проникновение в них взрослого человека, а также помещение не мелких предметов (имеющих по каждому из, хотя бы, двух измерений длину более 50 мл) без специальных средств взлома средств инженерной*

				защиты невозможно - 0,8 *3. Скрытное приближение к водопропускам, воздушным трубопроводам, подземным коллекторам невозможно; проникновение в них взрослого человека, а также помещение не мелких предметов (имеющих по каждому из, хотя бы, двух измерений длину более 50 мл) не требует специальных средств взлома инженерной защиты - 0,7* *4. Возможно скрытное приближние к водопропускам, воздушным трубопроводам, подземным коллекторам, однако проникновение в них взрослого человека, а также помещение не мелких предметов (имеющих по каждому из, хотя бы, двух измерений длину более 50 мл) невозможно без взлома инженерной защиты с использованием специальных средств- 0,4* *5. Возможно неконтролируемое приближение к водопропускам, воздушным трубопроводам, подземным коллекторам, однако проникновение в них взрослого человека, а также помещение не мелких предме-*

				тов (имеющих по каждому из, хотя бы, двух измерений длину более 50 мл) невозможно без взлома инженерной защиты с использованием специальных средств – 0,2
9.4.	Оснащение, вооружение и боевая готовность охраны на КПП и постах охраны периметра (постовых «грибках») k_{23}=	9.4.1. Количество охранников на КПП: 9.4.2. Оснащение охранников спецсредствами *(травматическое оружие, газовое оружие или баллончики, дубинки, др.)*. 9.4.3. Вооружение охранников *(типы огнестрельного оружия и его количество на смену)*. 9.4.4. Средства связи охранников *(спецификация, количество на смену, связь с резервной группой, связь с милицией, др.)*. 9.4.5. Резервная группа *(количество охранников, средняя удаленность размещения резервной группы от КППов, постовых «грибков», др.)*. 1.4.6. Квалификация охранников *(владение оружием (меткость стрельбы) и спецсредствами,*	Изучение регламентирующей документации. Проверка описей спецсредств. Выборочная проверка работоспособности. Проверка описей вооружения. Выборочная проверка боеготовности вооружения. Изучение документации. Выборочная проверка работоспособности. Изучение документации. Проверка. Изучение анкетных данных. Беседы.	*1. Охрана имеет возможность дать отпор групповому нападению, в т.ч. вооружённому, и оказывать сопротивление до прибытия сотрудников милиции – 1* *2. Охрана имеет возможность сообщить о групповом нападении в правоохранительные органы, а также пресечь агрессивные действия отдельного вооружённого лица или предотвратить нарушения режима со стороны группы невооружённых лиц, воздерживающихся от насильственных действий в отношении сотрудников охраны – 0,85* *3. Охрана имеет возможность предотвратить нарушение режима со стороны отдельного лица, воздерживающего от насильственных действий в отношении сотруд-*

		владение приёмами рукопашного боя, средний возраст).		*ников охраны, и вызвать милицию – 0,35* *4. Охрана не в состоянии своими силами противостоять активным действиям нарушителя режима, но имеет возможность вызвать милицию – 0,15* *5. Охрана не в состоянии своими силами противостоять активным действиям нарушителя режима, и не имеет прямой (оперативной) связи с органами внутренних дел – 0,05*
10.	Обеспечение личной безопасности руководства бизнеса			
10.1.	Защита рабочего места руководителя k_{24}=	10.1.1. Дверь в рабочий кабинет *(материал, толщина, замки, электронный ключ (проксимити-карта), петли, торцевые крюки, другие конструктивные особенности).* 10.1.2. Окна в рабочем кабинете *(прозрачность и ударопрочность стёкол, решётки, защитные щиты и ставки, запоры, др.).* 10.1.3. Охранная сигнализация рабочего кабинета *(сирена, извещатели, шлейфы сигнализации, сигнал на пульт централизованной охраны).* 10.1.4. Система охранного телевидения *(спецификация и количество камер,*	ВнОсм. Изучение ТехДок. Проверка работоспособности электронного ключа. ВнОсм. Изучение ТехДок. ВнОсм. Изучение ТехДок. Проведение эксперимента (выборочно). Проверка СГЭ. Изучение ТехДок. Проведение натурных	*1. Скрытный[14] и без специальных приспособлений и(или) средств взлома несанкционированный доступ к рабочему месту руководителя невозможен. Охрана способна предотвратить нападение на руководителя непосредственно на рабочем месте – 1* *2. Скрытный и без специальных приспособлений и(или) средств взлома несанкционированный доступ к рабочему месту руководителя невозможен. Защита руководителя от нападения непос-*

[14] Присутствие секретаря в приёмной не учитывается.

		разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения (вход, рабочий стол, сейф и т. п.), др.). 10.1.5. Тревожная сигнализация в кабинете и(или) приёмной: 10.1.6. Охрана в приёмной *(количество охранников, оснащение и вооружение, связь с центральным постом охраны, правоохранительными органами, навыки телохранителя)*.	испытаний. Проверка системы гарантирован. электропитан. Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ. Проверка описей вооружения. Изучение анкетных данных. Беседы с персоналом (руководителями СБ и подразделения управления персоналом, охранниками и сотрудниками СБ).	*редственно на рабочем месте отсутствует – 0,9* *3. Скрытный доступ к рабочему месту руководителя невозможен, однако препятствия для этого отсутствуют; существует возможность тревожного вызова охраны – 0,70* *4. Возможен скрытный доступ к рабочему месту руководителя, средства тревожного вызова охраны отсутствуют, однако несанкционированный доступ к рабочему месту руководителя без специальных приспособлений и(или) средств взлома невозможен – 0,4* *5. Возможен скрытный доступ к рабочему месту руководителя без использования специальных приспособлений и (или) средств взлма, однако у руководителя или секретаря в приёмной имеется возможность тревожного вызова охраны – 0,15*
10.2.	Личная охрана (сопровождение) руководителя k_{25}=	10.2.1. Охрана *(количество охранников, оснащение и вооружение, связь с правоохранительными органами, навыки телохранителя)*: 10.2.2. Радиомаяк местоположения	Проверка описей вооружения. Изучение анкетных данных. Беседы. Изучение ТехДок. По	*1. Охрана способна защитить руководителя от нападения; его местоположение контролируется дистанционно– 1* *2. Охрана способна защитить руководителя от*

		(спецификация, радиус действия, продолжительность работы от автономного источника питания (батареи), др.):	возможности наблюдение работоспособности.	*хулиганских действий и оградить от неблагоприятных проявлений внешней среды – 0,7* *3. Охрана способна оградить руководителя от неприятностей в результате мелких происшествий – 0,35* *4. Руководитель не защищён; его местоположение контролируется дистанционно – 0,1*
10.3.	Защита руководителя при передвижении на автомобиле k_{26}=	10.3.1. Водитель *(стаж, квалификация, навыки экстремального вождения, др.)*. 10.3.2. Охрана *(количество охранников, оснащение и вооружение, связь с правоохранительными органами, навыки телохранителя)*: 10.3.3. Автомобиль *(марка, подушки и шторки безопасности, бронирование, противоугонные устройства, радиомаяк местоположения (спецификация), др.)*.	Изучение анкетных данных. Беседы. Проверка описей вооружения и оснащения. Изучение документации, регламентирующей действия охранников. Изучение анкетных данных. Беседы. Изучение ТехДок., в т.ч. подтверждающей техническую исправность.	*1. Охрана способна защитить руководителя от нападения; автомобиль имеет средства защиты от огнестрельного оружия и оборудован средствами защиты пассажиров (руководителя) на случай катастрофы; его местоположение контролируется дистанционно – 1* *2. Охрана способна защитить руководителя от нападения, однако автомобиль небронирован, но имеет средства защиты пассажиров (руководителя) на случай катастрофы; его местоположение контролируется дистанционно – 0,7* *3. Водитель и охрана способны*

				оградить руководителя от неприятностей от мелких происшествий; автомобиль не бронирован, но имеет средства защиты пассажиров (руководителя) на случай катастрофы; его местоположение контролируется дистанционно – 0,5 *4. Руководитель самостоятельно обеспечивает свою безопасность; водитель высококлассный; автомобиль не бронирован, но имеет средства защиты пассажиров (руководителя) на случай катастрофы; его местоположение контролируется дистанционно – 0,25* *5. Руководитель самостоятельно обеспечивает свою безопасность; водитель не имеет специальных навыков вождения; автомобиль не бронирован, но имеет средства защиты пассажиров (руководителя) на случай катастрофы; его местоположение не контролируется дистанционно – 0,1*

11.	Обеспечение безопасности работников и посетителей в рабочих помещениях и на территории предприятий			
11.1.	Инженерно-техническая защита работников и посетителей k_{27}=	11.1.1. Система охранного телевидения в рабочих помещениях, коридорах, холлах, на лестницах и т. д. *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*. 11.1.2. Система тревожной сигнализации *(сигнал на центральный пункт управления, вызов милиции, др.)*. 11.1.3. Система оповещения персонала и посетителей о чрезвычайной ситуации *(подача звуковых сигналов, аварийное освещение, световые указатели, др.)*. 11.1.4. Средства индивидуальной защиты *(количество, спецификация, сертификация, др.)*: 11.1.5. Запасные выходы *(пригодность к использованию).*	Изучение ТехДок. Проведение натурных испытаний работоспособности. Проверка СГЭ Изучение ТехДок. Проведение натурных испытаний работоспособности. Проверка системы СГЭ Изучение ТехДок. Проведение натурных испытаний работоспособности. Проверка СГЭ. Проверка описей. Изучение актов проверки пригодности. Выборочная проверка наличия. ВнОсм.	*1. Обстановка в рабочих помещениях и на территории предприятия контролируется в режиме постоянного мониторинга; обеспечена возможность своевременного оповещения работников и посетителей предприятия о чрезвычайных ситуациях (обстоятельствах) (далее – ЧС) и их эвакуация с использованием запасных выходов, а также применения в случае необходимости средств индивидуальной защиты – 1* *2. Обеспечена возможность своевременного оповещения работников и посетителей предприятия о ЧС и их эвакуации с использованием запасных выходов, а также применения в случае необходимости средств индивидуальной защиты – 0,85* *3. Обеспечена возможность своевременного оповещения работников и*

				посетителей предприятия о ЧС и их эвакуации с использованием запасных выходов – 0,65 *4. Обеспечена возможность своевременного оповещения работников и посетителей предприятия о ЧС, однако их эвакуации с использованием запасных выходов затруднена – 0,4* *5. Обстановка в рабочих помещениях и на территории предприятия контролируется в режиме постоянного мониторинга, однако возможность оперативного оповещения работников и посетителей отсутствует; существует возможность эвакуации с использованием запасных выходов – 0,25* *6. Обстановка в рабочих помещениях и на территории предприятия контролируется в режиме постоянного мониторинга, однако возможность оперативного оповещения работников и*

				посетителей отсутствует; эвакуация с использованием запасных выходов затруднена – 0,1
11.2.	Нормативное правовое обеспечение k_{28}=	11.2.1. Внутренние документы, регламентирующие действия персонала по сигналам системы оповещения *(полнота и ясность инструкций, др.)*. 11.2.2. Схемы и планы эвакуации *(полнота, доступность, наглядность)*:	Изучение документации. Изучение документации.	*1. Действия персонала по сигналам системы оповещения регламентированы внутренними документами, а также поддержаны наглядными схемами и планами эвакуации – 1* *2. Действия персонала по сигналам системы оповещения не регламентированы внутренними документами, однако поддержаны наглядными схемами и планами эвакуации – 0,5* *3. Действия персонала по сигналам системы оповещения регламентированы внутренними документами, однако не поддержаны наглядными схемами и планами эвакуации – 0,25*
12.	Обеспечение сохранности финансовых средств и драгоценностей			
12.1.	Оборудование помещения кассы k_{29}=	12.1.1. Размещение кассового помещения *(этаж, изолированность от других помещений юридического лица, изолированность от соседних помещений других организаций)*. 12.1.2. Стены,	ВнОсм. Изучение	*1. Проникновение в кассовое помещение или эвакуация из него скрытно, а также без приспособлений, технических средств или инструментов*

		перекрытия, перегородки *(материал, толщина, конструктивные особенности, укрепление металлическими решетками не капитальных стен, перекрытий и перегородок, др.)*. 12.1.3. Буферное помещение (пространство) *(площадь)*. 12.1.4. Дверь в буферное помещение *(толщина, материал, петли, торцевые крюки, конструктивные особенности, замки, проксимити-карта, др.)*. 12.1.5. Дверь в кассовое помещение *(направление открывания, полнотелость, толщина и, материал дверного полотна, обивка стальными листами, дополнительные средства усиления прочности, петли, торцевые крюки, глазок, цепочка, другие конструктивные особенности, количество и типы замков, обрамление дверного проема (усиление дверных коробок стальным уголком, др.)*. 12.1.6. Дополнительная дверь в кассовое помещение *(направление открывания, конструктивные особенности, прочностные характеристики, замки, ушки для навесных замков, засовы, обрамление дверного*	документации. ВнОсм. ВнОсм. ВнОсм. Изучение ТехДок. Проверка электронного ключа. ВнОсм. Изучение ТехДок. ВнОсм. Изучение ТехДок.	*(далее - снаряжение) невозможны - 1* *2. Проникновение в кассовое помещение или эвакуация из него скрытно невозможны. Проникновение в кассовое помещение и эвакуация из него несанкционированным (необычным) образом затруднены - 0,85* *3. Проникновение в кассовое помещение не представляет серьёзных трудностей, но сделать это скрытно невозможно – 0,6* *4. Возможно скрытное проникновение в кассовое помещение или эвакуация из него, но для этого требуется специальное снаряжение – 0,35* *5. Проникновение в кассовое помещение затруднительно, но возможно совершить это скрытно – 0,15*

		проема, др.).		
		12.1.7. Оконные проемы в кассовом помещении *(размер (в том числе окна выдачи), прочностные характеристики решеток, защитных щитов или ставень, конструктивные особенности, засовы, запоры, др.)*.	ВнОсм. Изучение ТехДок.	
		12.1.8. Вентиляционные шахты, короба и дымоходы *(размеры, прочностные характеристики решеток, укрепление решетками по внутренней поверхности, др.)*.	ВнОсм. Изучение ТехДок.	
		12.1.9. Охранное телевидение входа в кассовое помещение *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*.	Изучение ТехДок. Проведение натурных испытаний работоспособ-ности. Проверка СГЭ.	
		12.1.10. Охранная сигнализация кассового помещения *(на открывание, пролом, удар, датчики и извещатели контроля объема, вывод сигналов тревоги, прокладка шлейфов сигнальных устройств, др.)*.	Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ.	
		12.1.11. Система тревожной сигнализации *(вывод сигнала на пульт централизованной охраны, в милицию, др.)*: 12.1.11. Хранилище денег (сейф) *(тип и марка, толщина стенок, масса, замок,*	Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ. Изучение ТехДок. ВнОсм. Проведение	

		сигнализация, крепление к конструкциям здания, др.).	натурных испытаний. Проверка СГЭ.	
12.2.	Защита денежных средств, иных финансовых ценностей и драгоцен-ностей при их перемещении k_{30}=	12.2.1. Автомобиль *(марка, бронирование, дверные замки, сигнализация по радио каналу об открывании дверей, противоугонные устройства, радиомаяк местоположения (его спецификация), средства связи, др.)*. 12.2.2. Сопровождение кассира *(количество охранников, оснащение и вооружение, навыки инкассатора, др.)*. 12.2.3. Страхование рисков, связанных с ограблением *(размер страховой премии, страховая компания, др.)*. 12.2.4. Привлечение инкассации на условиях аутсорсинга *(юридическое лицо, др.)*.	Изучение ТехДок., в т.ч. подтверждаю щей техническую исправность. Проверка описей вооружения и оснащения. Изучение документации, регламентиру ющей действия охранников. Изучение анкет. Беседы. Изучение договорной документации. Изучение договорной документации. Беседы с руководителем СБ и финансового органа.	*1. Обеспечена возможность отразить (предотвратить) нападение на кассира (или другого лица, осуществляющего перемещение ценностей во внешнем пространстве); риски застрахованы – 1* *2. Обеспечена возможность отразить (предотвратить) нападение на кассира; риски не застрахованы – 0,9* *3. Обеспечена возможность отразить (предотвратить) нападение на кассира со стороны преступников-дилетантов (невооружённых огнестрельным оружием и т. п.); риски не застрахованы – 0,75* *4. Обеспечена возможность отразить (предотвратить) нападение на кассира со стороны преступников-дилетантов (невооружённых огнестрельным оружием и т. п.); риски не застрахованы – 0,5* *5. Обеспечена*

				возможность предотвратить утрату ТМЦ в результате спонтанных преступных посягательств или возникновения непредвиденностей; риски застрахованы – 0,25 *6. Обеспечена возможность предотвратить утрату ТМЦ в результате спонтанных преступных посягательств или возникновения непредвиденностей; риски не застрахованы – 0,1*
12.3.	Нормативное правовое обеспечение сохранности финансовых ценностей и драгоцен-ностей k_{31}=	12.3.1. Внутренние документы, регламентирующие порядок доступа в кассовое помещение, а также обеспечения сохранности ценностей в кассовом помещении и при их перемещении *(полнота, ясность, др.)*.	Изучение документации.	*1. Внутренние документы разработаны качественно в полном объёме – 1* *2. Внутренние документы не чётко регламентируют некоторые аспекты сохранности ТМЦ, что создаёт косвенные предпосылки снижения уровня защиты ТМЦ – 0,75* *3. Внутренние документы не регламентируют ряд аспектов обеспечения сохранности ТМЦ – 0,5* *4. Внутренние документы разработаны формально - 0,25*

13.	Защита товарно-материальных ценностей на складах			
13.1.	Инженерно-техническая защита склада в отдельном здании k_{32}=	13.1.1. Стены, перекрытия *(материал, толщина, конструктивные особенности, укрепление металлическими решетками не капитальных стен, перекрытий и перегородок, др.)*.	Изучение документации. ВнОсм.	*1. Проникновение в здание склада или эвакуация из него скрытно, а также без приспособлений, технических средств или инструментов (далее - снаряжение) невозможны - 1*
		13.1.4. Оконные проёмы (в т.ч. окна выдачи ТМЦ) *(размер (в т.ч. окон выдачи), прочностные характеристики решеток, защитных щитов или ставень, конструктивные особенности, засовы, запоры, замки, др.)*.	Изучение документации. ВнОсм.	*2. Проникновение в здание склада или эвакуация из него скрытно невозможны. Проникновение в здание склада и эвакуация из него несанкционированным (необычным) образом затруднены - 0,85*
		13.1.5. Двери *(толщина, материал дверного полотна, полнотелость, дополнительные средства усиления прочности, петли, торцевые крюки, глазок, цепочка, другие конструктивные особенности, количество и типы замков, кроксимити-карты, обрамление дверного проема (усиление дверных коробок стальным уголком), др.)*.	Изучение документации. ВнОсм.	*3. Проникновение в здание склада и эвакуация из него не представляют серьезных трудностей, но сделать это скрытно невозможно – 0,6*
		13.1.6. Вентиляционные шахты, короба и дымоходы *(размеры, прочностные характеристики решеток, укрепление решетками по внутренней поверхности, др.)*.	Изучение документации. ВнОсм.	*4. Возможно скрытно проникнуть в здание склада или покинуть его, но для этого требуется специальное снаряжение – 0,35*
		13.1.7. Система охранного телевидения по периметру здания,	Изучение ТехДок. Проведение	*5. Проникновение в здание склада затруднительно, но возможно совершить это скрытно и без специальной подготовки – 0,15*

		крыши *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*.	натурных испытаний. Проверка СГЭ.	
		13.1.8. Средства охранной сигнализации проникновения в здание через окна, крышу, запасные двери, в т.ч. наружные двери в подвальные помещения, вентиляционные шахты, короба и дымоходы *(прожектора, сирена, извещатели, шлейфы сигнализации, сигнал на пульт централизованной охраны или милицию, др.)*.	Изучение ТехДок. Проведение эксперимента на срабатывание. Проверка СГЭ.	
		13.1.9. Система охранного телевидения здания склада *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*.	Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ.	
13.2.	Инженерно-техническая защита складской территории (открытой площадки с материаль-ными ценностями)	13.2.1. Ограждение *(материал, высота, толщина, заглубленность основания, (не)сплошное, конструкция, дополнительное ограждение (козырек, «Спираль АКЛ» и т. п.), др.)*.	ВнОсм. Изучение документации.	*1. Пересечение периметра складской территории скрытно[15], а также без приспособлений, технических средств или инструментов (далее -*

[15] «Скрытно» в данном случае означает, что действие может быть совершено в условиях, когда отсутствуют, в том числе на отдельных участках периметра, технические средства фиксации этого действия или караульные, непосредственно отвечающие за наблюдение (охрану) периметра. Другими словами, фраза «пересечь периметр скрытно невозможно» отражает не факт воспрепятствования проникновению на охраняемую территорию (или эвакуации с неё) со стороны охраны, а наличие средств и(или) сил, с помощью которых потенциально любой факт пересечения периметра фиксируется.

	k_{33}=	13.2.2. Предупредительное ограждение *(высота, конструкция (колючая проволока), ширина зоны отторжения, контрольно-следовая полоса, др.)*. 13.2.3. Система охранного телевидения *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*. 13.2.4. Система охранной сигнализации периметра складской территории *(прожектора, сирена, извещатели, шлейфы сигнализации, сигнал на пульт централизованной охраны или полиции, др.)*. 13.2.5. Караульные собаки *(дрессура, активность (агрессивность), место нахождения и степень свободы перемещения, количество на 100 м длины периметра, др.)*. 13.2.6. Посты охраны периметра складской территории (постовые «грибки») *(количество на 100 м периметра и топология размещения, выучка караульных, средства оповещения (сигнализации), специальные средства и вооружение караульных, средства освещения периметра, др.)*.	ВнОсм. Изучение документации. Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ. Изучение ТехДок. Проведение эксперимента на срабатывание. Проверка СГЭ. ВнОсм. ВнОсм. Проверка функционирования технических и спец. средств. Проверка выполнения служебных обязанностей охранниками.	*снаряжение) невозможно - 1* *2. Пересечение периметра складской территории скрытно невозможно. Пересечение периметра складской территории затруднено - 0,85* *3. Пересечение периметра складской территории не представляет трудностей, но сделать это скрытно невозможно – 0,6* *4. Возможно скрытное пересечение периметра складской территории, но требуется снаряжение – 0,4* *5. Пересечение периметра складской территории затруднительно, но возможно совершить это скрытно – 0,25* *6. Возможно скрытное без затруднений пересечение периметра складской территории, но только пешим порядком - 0,1*

13.3.	Инженерно-техническая защита выделенных в здании складских помещений k_{34}=	13.3.1. Дверь в помещение склада *(толщина, материал дверного полотна, полнотелость, дополнительные средства усиления прочности, петли, торцевые крюки, глазок, цепочка, другие конструктивные особенности, количество и типы замков, кроксимити-карты, обрамление дверного проема (усиление дверных коробок стальным уголком, др.)*.	ВнОсм. Изучение документации.	*1. Проникновение в складское помещение или эвакуация из него скрытно, а также без приспособлений, технических средств или инструментов (далее - снаряжение) невозможны - 1*
		13.3.2. Средства дистанционного и автоматического управления дверными замками (запорами) в помещении склада:	Изучение документации. Проверка функционирования.	*2. Проникновение в складское помещение или эвакуация из него скрытно невозможны. Проникновение в складское помещение и эвакуация из него несанкционированным (необычным) образом затруднены - 0,85*
		13.3.3. Оконные проемы в складском помещении (в т.ч. окна выдачи ТМЦ) *(размер (в т.ч. окон выдачи), прочностные характеристики решеток, защитных щитов или ставень, конструктивные особенности, засовы, запоры, др.)*.	ВнОсм. Изучение документации.	*3. Проникновение в складское помещение не представляет серьёзных трудностей, но сделать это скрытно невозможно – 0,6*
		13.3.4. Стены, межэтажные перекрытия *(материал, толщина, конструктивные особенности, укрепление металлическими решетками не капитальных стен, перекрытий и перегородок, др.)*.	ВнОсм. Изучение документации.	*4. Возможно скрытное проникновение в складское помещение или эвакуация из него, но для этого требуется специальное снаряжение – 0,35*
		13.3.5. Система охранной сигнализации проникновения в	Изучение ТехДок. Проведение	*5. Проникновение в складское помещение затруднительно, но возможно совершить это скрытно – 0,15*

		складское помещение *(на открывание, пролом, удар, датчики и извещатели контроля объема, вывод сигналов тревоги, прокладка шлейфов сигнальных устройств, др.)*. 13.3.6. Система охранного телевидения входа в складское помещение *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*. 13.3.7. Система охранного телевидения обстановки внутри складского помещения *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*. 13.3.8. Система тревожной сигнализации *(вывод сигнала на пульт централизованной охраны, в милицию, др.)*.	эксперимента на срабатывание. Проверка системы СГЭ. Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ. Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ. Изучение ТехДок. Проведение эксперимента. Проверка СГЭ.	
13.4.	Средства контроля поступления и отгрузки ТМЦ k_{35}=	13.4.1. Система маркировки ТМЦ *(метки для автоматического дистанционного распознавания ТМЦ и срабатывания сигнализации при несанкционированном выносе)*. 13.4.2. Система автоматизированного учёта поступления и отгрузки ТМЦ *(спецификация контрольных*	Изучение документации. Проведение эксперимента на срабатывание сигнализации. Изучение документации. Наблюдение функционирования.	*1. Обеспечена возможность автоматизированного учёта поступления и отгрузки ТМЦ, в т.ч. контроля в режиме on-line, надёжно обеспечено хранение сведений в базе данных и предотвращение несанкционированного доступа к системе*

		устройств, датчиков и т. п., предотвращение несанкционированного доступа (использование электронных ключей, ПИН-кодов и т. п.), автоматическое протоколирование операций актуализации сведений о движении ТМЦ, резервное копирование базы данных о движении и наличии ТМЦ, удалённый контроль движения и наличия ТМЦ в режиме on-line).		*электронной маркировки и автоматизированного учёта поступления и выдачи ТМЦ – 1* *2. Обеспечена возможность автоматизированного учёта поступ-ления и отгрузки ТМЦ, уровень сохранности сведений в базе данных и предотвращение несанкционированного доступа к системе электронной маркировки и автоматизированного учёта поступления и отгрузки ТМЦ требует доработки – 0,75* *3. Обеспечена возможность электронной маркировки ТМЦ; учёт поступления и отгрузки ТМЦ осуществляется «вручную» – 0,4* *3. Обеспечена возможность электронной маркировки только наиболее важных ТМЦ; учёт поступления и отгрузки ТМЦ осуществляется «вручную» – 0,1*
13.5.	Нормативное правовое обеспечение сохранности ТМЦ k_{36}=	13.5.1. Внутренние документы, регламентирующие порядок обеспечения сохранности и движения ТМЦ *(полнота и*	Изучение документации.	*1. Внутренние документы разработаны качественно в полном объёме; существуют в*

		ясность инструкций). 13.5.2. Наличие договоров о материальной ответственности, в т.ч. солидарной:	Изучение документации.	*полном объёме договора о материальной ответственности – 1* *2. Внутренние документы не регламентируют некоторые аспекты сохранности ТМЦ, что создаёт предпосылки снижения уровня защиты ТМЦ; существуют в полном объёме договора о материальной ответственности – 0,75* *3. Внутренние документы разработаны качественно в полном объёме; договора о материальной ответственности требуют доработки – 0,75* *4. Внутренние документы не регламентируют некоторые аспекты сохранности ТМЦ, что создаёт предпосылки снижения уровня защиты ТМЦ; договора о материальной ответственности требуют доработки – 0,5* *5. Внутренние документы разработаны качественно в полном объёме; договора о материальной*

				ответственности отсутствуют – 0,5 *6. Внутренние документы разработаны формально, существуют в полном объёме договора о материальной ответственности - 0,3* *7. Внутренние документы разработаны формально, договора о материальной ответственности отсутствуют – 0,1*
14.	Защита товарно-материальных ценностей при осуществлении производственных процессов и перемещении внутри предприятия			
14.1.	Система технического контроля расходования ТМЦ k_{37}=	14.1.1. Система охранного телевидения в производственных помещениях *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*. 14.1.2. Средства автоматического учета расходования ТМЦ и выхода конечной продукции *(спецификация контрольных устройств, датчиков и т. п., предотвращение несанкционированного доступа (использование электронных ключей, ПИН-кодов и т. п.), автоматическое*	Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ. Изучение документации. Наблюдение функциониро-вания.	*1. Обеспечена возможность автоматического учёта расходования ТМЦ и выхода конечной продукции, в т.ч. в режиме on-line; обстановка в производственных помещениях наблюдаема – 1* *2. Обеспечена возможность автоматического учёта основных операций расходования ТМЦ и выхода конечной продукции; обстановка в производственных помещениях наблюдаема – 0,6* *3. Обеспечена возможность*

		протоколирование операций актуализации сведений о движении ТМЦ и выходе конечной продукции, резервное копирование базы данных о движении и наличии ТМЦ, а также выходе конечной продукции, удалённый контроль движения и наличия ТМЦ в режиме on-line).		*автоматического учёта основных операций расходования ТМЦ и выхода конечной продукции; обстановка в производственных помещениях дистанционно ненаблюдаема (наблюдаема не чётко) – 0,4 (0,5)* *4. Автоматический учёт расходования ТМЦ и выхода конечной продукции не предусмотрен; обстановка в производственных помещениях наблюдаема – 0,2*
15.	Обеспечение информационной безопасности, в т.ч. сохранение коммерческой тайны			
15.1.	Программно-технические средства предотвращения несанкционированного доступа, повреждения и утраты информационных ресурсов (ИнР) k_{38}=	15.1.1. Программно-технические средства разграничения и предотвращения доступа к информационным ресурсам, размещенным в корпоративных и локальных сетях и в базах данных *(коммерческие программные продукты, электронные и технические ключи, шифрование, технические и программные решения, др.)*. 15.1.2. Средства резервирования и восстановления информации, хранящейся в базах данных и в файловых системах в сетях и на рабочих станциях:	Изучение документации. Проверка функционирования Изучение документации, в т.ч. протоколов резервного копирования.	*1. Обеспечена сохранность информационных ресурсов при любых авариях, вирусах и целенаправленном негативном воздействии человеческого фактора – 1* *2. Обеспечено периодическое резервирование информационных ресурсов, высокая надёжность их сохранности при авариях в сетях и(или) на серверах и проникновении вирусов, а также защита от целенаправленного негативного воздействия*

		15.1.3. Средства антивирусной защиты:	Проверка наличия программно-технических средств.	*человеческого фактора – 0,9* *3. Обеспечено периодическое резервирование информационных ресурсов, их сохранность при воздействии вирусов и попытках воздействия человеческого фактора извне – 0,7* *4. Обеспечено периодическое резервирование информационных ресурсов, их сохранность при попытках неквалифицированного воздействия внутреннего человеческого фактора – 0,3* *5. Периодическое резервирование информационных ресурсов не предусмотрено, их сохранность обеспечивается только средствами операционной системы – 0,1*
15.2.	Технические средства противодействия промышленному шпионажу k_{39}=	15.2.1. Программно-технические средства защиты внешнего контура корпоративной и локальных сетей: 15.2.2. Средства шифрования сообщений, выходящих за контур корпоративной сети: 15.2.3. Средства мониторинга действий пользователей в корпоративных и	Изучение документации. Проверка наличия. Изучение документации. Проверка наличия. Изучение документации. Проверка протоколов	*1. Обеспечена защита информации от утечки по электронным каналам; действия пользователей сети контролируются – 1* *2. Обеспечена защита информации от доступа и утечки по электронным каналам; действия пользователей сети не контролируются*

		локальных сетях, а также обмена сообщениями во внешних сетях: 15.2.4. Средства предотвращения прослушивания категорированных помещений (кабинетов руководителей, переговорных и т. п.): 15.2.5. Средства предотвращения прослушивания телефонных переговоров, а также съема информации с приборов и устройств, имеющих излучающие, электродинамические, электромагнитные и т. п. элементы:	работы. Изучение документации. Проверка наличия. Изучение документации. Проверка наличия.	*– 0,75* *3. Обеспечена защита информации от доступа и утечки по телекоммуникационным каналам; действия пользователей сети не контролируются – 0,5* *4. Обеспечена защита информации от доступа и утечки по телекоммуникационным каналам только при воздействии сетевых роботов, автоматически активизирующих программных средств несанкционированного доступа; действия пользователей сети не контролируются – 0,25* *5. Обеспечена конструктивная защита от копирования на внешние носители наиболее важной информации, а также установлены ограничения на объём передачи информации во внешние сети - 0,1*
15.3.	Нормативное правовое обеспечение информационной безопасности k_{40}=	15.3.1. Внутренние документы, регламентирующие порядок доступа к информационным ресурсам и обеспечения их сохранности *(полнота и ясность инструкций, др.)*.	Изучение документации.	*1. Все действия пользователей с информацией регламентированы; имеются лицензии на используемое программное обеспечение - 1* *2. Регламентируетс*

		15.3.2. Внутренние документы, регламентирующие порядок обеспечения защиты сведений, содержащих коммерческую тайну *(полнота и ясность инструкций, наличие утвержденного перечня сведений, содержащих коммерческую тайну, др.)*. 15.3.3. Наличие лицензий на используемое программное обеспечение:	Изучение документации. Проверка наличия лицензий.	*я порядок обеспечения защиты сведений, содержащих коммерческую тайну; имеются лицензии на используемое программное обеспечение - 0,75* *3. Регламентируетс я порядок обеспечения защиты сведений, содержащих коммерческую тайну; отсутствуют лицензии на некоторые образцы используемого программного обеспечения - 0,5* *4. Регламентируетс я порядок обеспечения защиты сведений, содержащих коммерческую тайну; отсутствуют лицензии на используемое программное обеспечение - 0,25*
15.4.	Защита помещений размещения хранилищ информаци-онных ресурсов, в т.ч. на бумажных носителях, и серверов k_{41}=	15.4.1. Дверь в помещение *(толщина, материал дверного полотна, полнотелость, дополнительные средства усиления прочности, петли, торцевые крюки, глазок, цепочка, другие конструктивные особенности, количество и типы замков, кроксимити-карты, обрамление дверного проема*	ВнОсм. Изучение документации.	*1. Проникновение в хранилище информационных ресурсов (серверную) или эвакуация из него скрытно, а также без приспособлений, технических средств или инструментов (снаряжения) невозможны - 1* *2. Проникновение в хранилище*

		(усиление дверных коробок стальным уголком, др.). 15.4.2. Средства дистанционного и автоматического управления дверными замками (запорами) в помещении: 15.4.3. Оконные проемы в помещении (в т.ч. окна выдачи документов и съемных носителей информации) *(размер (в т.ч. окон выдачи), прочностные характеристики решеток, защитных щитов или ставень, конструктивные особенности, засовы, запоры, др.)*. 15.4.4. Стены, межэтажные перекрытия *(материал, толщина, конструктивные особенности, укрепление металлическими решетками не капитальных стен, перекрытий и перегородок, др.)*. 15.4.5. Система охранного телевидения входа в помещение и обстановки внутри помещения *(спецификация и количество камер, разрешение, чувствительность, отношение сигнал/шум, тип видеонакопителя, поле наблюдения, др.)*. 15.4.6. Система охранной сигнализации *(на открывание, пролом, удар, датчики и извещатели контроля объема, вывод сигналов*	Изучение документации. Проверка функционирования. ВнОсм. Изучение документации. ВнОсм. Изучение документации. Изучение ТехДок. Проведение натурных испытаний. Проверка СГЭ. Изучение ТехДок. Проведение эксперимента. Проверка СГЭ.	*информационных ресурсов или эвакуация из него скрытно невозможны.* *Проникновение в хранилище информационных ресурсов и эвакуация из него несанкционированным (необычным) образом затруднены - 0,85* *3. Проникновение в хранилище информационных ресурсов не представляет серьёзных трудностей, но сделать это скрытно невозможно – 0,6* *4. Возможно скрытное проникновение в хранилище информационных ресурсов или эвакуация из него, но для этого требуется специальное снаряжение – 0,35* *5. Проникновение в хранилище информационных ресурсов затруднительно, но возможно совершить это скрытно – 0,1*

		тревоги, кнопки тревожной сигнализации, прокладка шлейфов сигнальных устройств, др.). 15.4.7. Система тревожной сигнализации *(вывод сигнала на пульт централизованной охраны, в милицию, др.)*.	Изучение ТехДок. Проведение эксперимента. Проверка СГЭ.	
16.	Обеспечение пожарной безопасности			
16.1.	Технические средства обеспечения пожаробезо-пасности k_{42}=	16.1.1. Гидранты, пожарные колодцы и водоемы *(количество, мощность, объем запаса воды, др.)*. 16.1.2. Огнетушители *(количество, в т.ч. в кассовом помещении и других категорированных помещениях, тип (марка), объем)*. 16.1.3. Автоматические стационарные установки пожаротушения *(категории и назначения помещений, спецификация систем, их ТТХ)*. 16.1.4. Пожарные щиты и их комплектация: 16.1.5. Извещатели о пожаре *(тип, марка, ТТХ, количество)*. 16.1.6. Вывод сигналов о возгорании *(на пульт охраны, на пульт подразделений пожарной охраны, сирена, др.)*.	ВнОсм. Изучение документации. ВнОсм. Изучение документации. Изучение документации. ВнОсм. Изучение документации. ВнОсм. Изучение документации. ВнОсм. Тестовая проверка. Изучение документации. Тестовая проверка.	*1. Возможность незамеченного возгорания практически исключена; в наличии (исправны) средства сигнализации и пожаротушения, позволяющие локализовать очаг до прибытия пожарных – 1* *2. Возможность незамеченного возгорания практически исключена; в наличии (исправны) средства сигнализации и пожаротушения, позволяющие локализовать небольшой очаг до прибытия пожарных – 0,75* *3. Средства автоматической сигнализации о возгорании отсутствуют; в наличии (исправны) средства сигнализации и пожаротушения, позволяющие локализовать очаг до прибытия*

				пожарных – 0,5 *4. Средства сигнализации о возгорании отсутствуют; в наличии (исправны) средства пожаротушения, позволяющие локализовать небольшой очаг до прибытия пожарных – 0,25* *5. Средства автоматической сигнализации о возгорании отсутствуют; в наличии (исправны) примитивные средства пожаротушения, позволяющие локализовать маленький очаг непосредственно после возгорания – 0,1*
16.2	Технические средства предупрежде-ния возгорания k_{43}=	16.2.1. Средства предупреждения возгорания в помещениях, в которых находятся легковоспламеняющиеся, взрывчатые, особо опасные вещества или значительные ценности *(покрытия стен, полов и потолков, искрогасители, искроуловители, огнезадерживающие, огнепреграждающие, пыле- и металлоулавливающие и противовзрывные устройства, системы защиты от статического электричества, шиберы,*	Изучение документации.	*1. Обеспечена устойчивость к намеренному поджигу; исключается возгорание от случайных факторов, аварий оборудования и электропроводки – 1* *2. Исключается возгорание от случайных факторов, аварий оборудования и электропроводки – 0,75* *3. Обеспечена защита от распространения пожара – 0,5* *4. Обеспечена*

		др.).		*частичная защита от распространения пожара – 0,25*
16.3.	Нормативное правовое обеспечение пожарной безопасности k_{44}=	16.2.1. Внутренние документы, регламентирующие порядок поддержания состояния пожарной безопасности, действия персонала, в т.ч. инструкции по мерам пожарной безопасности, противопожарный режим, порядок эвакуации, приказ о назначении ответственного за пожарную безопасность *(наглядность и доступность инструкций к ознакомлению, их полнота и ясность, др.)*.	Изучение документации. Проверка работоспособности. Изучение документации. Проведение эксперимента.	*1. Обеспечение пожарной безопасности регламентировано; издан приказ о назначении ответственных - 1* *2. Обеспечение пожарной безопасности регламентировано в основном; издан приказ о назначении ответственных – 0,75* *3. Обеспечение пожарной безопасности регламентировано; приказ о назначении ответственных не издан – 0,5* *4. Обеспечение пожарной безопасности не регламентировано; издан приказ о назначении ответственных – 0,25*
17.	Обеспечение качества человеческого ресурса с точки зрения добросовестности			
17.1.	Силы и средства установления истины о кандидате на работу k_{45}=	17.1.1. Средства проверки подлинности документов: 17.1.2. Программно-технические средства выяснения правдивости ответов испытуемого («детектор лжи»): 17.1.3. Психолог *(штатный, аутсорсинг, квалификация, др.)*. 17.1.4. Тесты для	Изучение кадровой документации. Изучение документации. Изучение кадровой документации. Опрос работ-	*1. Обеспечено объективное и субъективное изучение правдивости кандидата и выявления его склонности к криминальным и др. социально вредным действиям – 1* *2. Обеспечено субъективное изучение*

		выяснения квалификации кандидатов по категориям, составления психологических портретов, выявления склонности к криминальным действиям, др.:	ников кадровой службы и службы безопасности о практике использования тестов.	*правдивости кандидата и выявления его склонности к криминальным и др. социально вредным действиям – 0,7* *3. Обеспечено объективное изучение правдивости кандидата и выявления его склонности к криминальным и др. социально вредным действиям – 0,5* *4. Обеспечена проверка подлинности документов – 0,1*
17.2.	Нормативное правовое обеспечение «чистоты ря8дов» k_{46}=	17.3.1. Внутренние документы, регламентирующие порядок изучения кандидатов в соответствии с нормативной правовой базой Российской Федерации *(полнота, ясность, правовая безупречность)*.	Изучение документации.	*1. Порядок изучения кандидата подробно регламентирован и предполагает объективное и субъективное изучение, а также взаимодействие кадрового аппарата и службы безопасности – 1* *2. Порядок изучения кандидата регламентирован, однако процедуры объективного и субъективного изучения «по шагам» не описаны – 0,75* *3. Порядок изучения кандидата регламентирован, но процедуры объективного и субъективного изучения документами не предусмотрены – 0,5*

				4. Порядок изучения кандидата регламентирован в общих чертах, процедуры действий не описаны – 0,25
18.	Управление функционированием системы обеспечения защиты ресурсов и безопасности			
18.1.	Организационно-штатное и техническое обеспечение k_{47}=	18.1.1. Организационно-штатная структура СБ: 18.1.2. Качество персонала по направлениям деятельности *(профессиональная подготовка, средний возраст, опыт работы)*. 18.1.3. Средства офисной техники, аудио- видео записи и фотографирования, автотранспорт: 18.1.4 Вооружение и средства самообороны:	Изучение документации. Изучение кадровой документации. Проверка наличия в соответствии с описями и работоспособности. Проверка наличия в соответствии с описями. ВнОсм.	*1. Штат укомплектован по всем направлениям деятельности; оснащён и вооружён – 1* *2. Штат укомплектован в основном, оснащён и вооружён – 0,8* *3. Штат укомплектован и оснащён в основном – 0,65* *4. Штат укомплектован в основном, но плохо оснащён – 0,5* *5. Штат неудокомплектован более чем на половину, но оснащён – 0,3* *6. Штат неудокомплектован более чем на половину и плохо оснащён – 0,15*
18.2.	Нормативное правовое обеспечение функционирования системы обеспечения безопасности k_{48}=	18.2.1. Положение о СБ *(полнота в части регламентаций основных функций и задач, ясность)*. 18.2.2. Должностные инструкции сотрудников СБ *(полнота и ясность, др.)*. 18.2.3. Инструкции по действиям должностных лиц и персонала в различных условиях	Изучение документации. Изучение документации. Изучение документации и мест её наглядного	*1. Деятельность по обеспечению безопасности бизнеса полностью регламентирован, включая порядок проведения закупочных процедур – 1* *2. Деятельность службы безопасности полностью*

		обстановки, сопряженной с угрозами (при прибытии сотрудников контролирующих органов, нападениях, чрезвычайных ситуациях и т. п. *(полнота и ясность, соответствие нормативной правовой базе Российской Федерации)*. 18.2.4. Внутренние документы, регламентирующие порядок осуществления закупок, проведения тендеров и конкурсов *(полнота, ясность, др.)*.	размещения. Изучение документации.	*регламентирована, однако деятельностью других подразделений и должностных лиц бизнеса, связанная с обеспечением безопасности и взаимодействием с СБ не регламентирована – 0,5* *3. Деятельность СБ регламентирована частично (отсутствуют некоторые инструкции, в принятых документах не учтены некоторых задачи и аспекты) – 0,25*

Научное издание

Д.В. Трошин – кандидат технических наук, ведущий научный сотрудник Центра проблем экономической безопасности и стратегического планирования Института экономической политики и проблем экономической безопасности Финансового университета при Правительстве Российской Федерации

ТРОШИН Дмитрий Владимирович

Безопасность предприятия
смысл, онтология, оценка

Монография

Технический редактор А.В. Жильцов
Подписано в печать 28.09.2015. Формат 60х84 $^{1}/_{16}$.
Усл. печ. л. 13,25. Тираж 500. Заказ № 441.
Редакционно-издательское управление
Тверского государственного университета
Адрес: 170100, г. Тверь, Студенческий пер. 12, корпус Б.
Тел. РИУ (4822) 35-60-63.