

3. Классификация угроз экономической безопасности организации

В определенный период своего развития каждая организация сталкивается с проблемой защиты своих интересов от противоправных действий конкурентов и посягательств недоброжелателей. В современных условиях не всегда правовых конкурентных отношений, несовершенства действующего законодательства, произвола фискальных органов и т.п., еще на стадии создания организации (составление бизнес-плана и проекта учредительных документов) необходимо предусмотреть меры обеспечения экономической безопасности организации, которые позволят предотвратить либо уменьшить негативное влияние внешних и внутренних угроз. Необходимость обеспечения безопасности определена наличием целого ряда факторов и источников угроз, которые в той или иной степени оказывают влияние на безопасность организации.

Угроза экономической безопасности организации - это:

1) совокупность факторов, воздействий внешней и внутренней среды предприятия, которые нацелены на незаконное или злостное воспрепятствование или затруднение его функционирования в соответствии с уставными, долгосрочными и краткосрочными целями и задачами, а также на отчуждение результатов его деятельности,

2) потенциальные или реальные действия физических или юридических лиц, нарушающее состояние защищенности субъекта предпринимательской деятельности и способные привести к ее прекращению, либо к экономическим и другим потерям. В частности, ущерб интересам предпринимателя может быть нанесен в результате недобросовестных действий конкурентов, невыполнения партнерами, заказчиками, поставщиками, клиентами своих обязательств по оплате контрактов, поставке товаров и т. п., а также кризисных явлений в экономике, непредсказуемых изменений конъюнктуры рынка, стихийных бедствий, чрезвычайных происшествий, управленческой некомпетентности, социальной напряженности и, наконец, неблагоприятной экономической политики государства.

Источниками отрицательных влияний на экономическую безопасность организации могут быть:

- сознательные или бессознательные действия отдельных должностных лиц и субъектов хозяйствования (органов государственной власти, международных организаций, конкурентов);

- стечение объективных обстоятельств (состояние экономической конъюнктуры на рынках данного предприятия, научные открытия и технологические разработки, форс-мажорные обстоятельства и т. п.).

В зависимости от субъектной обусловленности отрицательные влияния на экономическую безопасность могут быть объективными и субъективными. Объективными считаются такие отрицательные влияния, которые возникают не по вине самого предприятия или его отдельных работников. Субъективные влияния имеют место вследствие неэффективной работы предприятия в целом или его отдельных работников (прежде всего руководителей и функциональных менеджеров).

Угрозой экономической безопасности может быть не всякое действие, имеющее негативные последствия. Так, не следует считать угрозой экономической безопасности организации деятельность руководства организации по вложению средств в ценные бумаги, внедрение новых организационных форм, организацию реализации новой услуги, товара, работы. Все эти управленческие решения являются рискованными и могут иметь негативные экономические последствия вследствие того, что может резко измениться конъюнктура на рынке ценных бумаг, потребности населения, либо новые организационные формы не оправдают себя. Но нужно иметь в виду, что в конечном счете все это направлено на достижение основной цели организации, на его дальнейшее развитие. Такого рода решения составляют неотъемлемую часть самой предпринимательской деятельности, которая

осуществляется с риском и предполагает определенные потери.

Не может считаться угрозой безопасности промышленным предприятиям установление руководством организации низких цен на продукцию в начальный период ее реализации. Хотя в этом случае может отсутствовать прибыль и, наоборот, иметь место убыток, но это стандартный маркетинговый прием, имеющий целью привлечь покупателей к незнакомому для них продавцу. Позже разница в ценах будет устранена.

Действия, определяемые как угрозы, сознательно направлены на получение какой-либо выгоды от экономической дестабилизации организации, от посягательств на ее экономическую безопасность. Угрозы, как правило, несут за собой нарушение законодательных норм (той или иной отрасли права -гражданского, административного, уголовного) и предполагают определенную ответственность лиц, их осуществляющих. Можно отметить три признака, характерных для угроз экономической безопасности промышленным предприятиям: сознательный и корыстный характер, направленность действий на нанесение ущерба субъекту предпринимательства, противоречивый характер.

Существуют самые различные угрозы, которые могут одновременно относиться к различным группам классификации. Классификация источников угроз (факторов) приведена в таблице 1.3.1.

Таблица 1.3.1. Классификация источников угроз (факторов) экономической безопасности

№.	Признаки	Угрозы
1	По месту возникновения	Внутренние, внешние
2	По степени опасности	Особенно опасные, опасные
3	По возможности осуществления	Реальные, потенциальные
4	По масштабу осуществления	Локальные, общесистемные
5	По длительности действия	Временные постоянные
6	По направлению	Производственные, финансовые, технологические, социально-экономические
7	По отношению к ним	Объективные, субъективные
8	По характеру направления	Прямые, косвенные
9	По вероятности наступления	Явные, латентные
10	По природе возникновения	Политические, криминальные, конкурентные, и т.п.

Факторы, влияющие на уровень экономической безопасности предприятия, могут быть следующими (рис. 1.3.1).

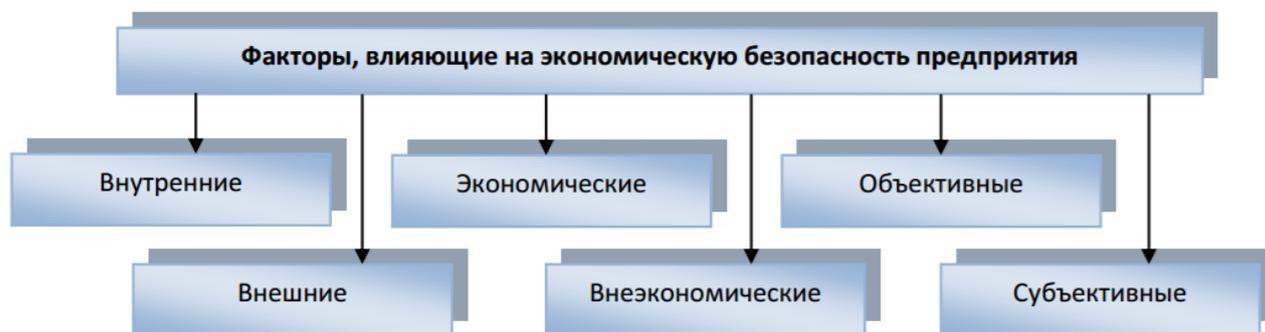


Рис. 1.3.1. Факторы, влияющие на уровень экономической безопасности предприятия

Классификация угроз безопасности может быть реализована разделением на угрозы связанные с внутренними и внешними факторами (рис. 1.3.2).



Рис. 1.3.2. Классификация угроз по факторам и мотивации

Для каждой организации «внешние» и «внутренние» угрозы сугубо индивидуальны.

Примерная классификация основных видов угроз безопасности организации приведена на рисунке 1.3.3.

Составляющие внутренних угроз: персонал; техника и технологии; финансы; информация.

К внутренним угрозам относятся действия или бездействия (в том числе умышленные и неумышленные) сотрудников организации, противоречащие интересам его коммерческой деятельности, следствием которых могут быть нанесение экономического ущерба компании, утечка или утрата информационных ресурсов (в том числе сведений, составляющих коммерческую тайну и / или конфиденциальную информацию), подрыв ее делового имиджа в бизнес-кругах, возникновение проблем во взаимоотношениях с реальными и потенциальными партнерами (вплоть до утраты важных контрактов), конфликтных ситуаций с представителями криминальной среды, конкурентами, контролирующими и правоохранительными органами, производственный травматизм или гибель персонала и т.д.

Хайитматов У.Т., Азаматов О.Х., Мажидов Р.Р., Хакимов А.Ф. Обеспечение экономической безопасности предприятий в современном бизнесе // Иктисодиёт ва инновацион технологиялар. 2012. № 4.

Финансовая составляющая экономической безопасности предприятия характеризуется производительностью труда работников, фондоотдачей, рентабельностью производства, издержками, дебиторской и кредиторской задолженностью, уровнем инновационной активности, долей обеспеченности собственными источниками финансирования оборотных средств, материальных и энергетических ресурсов для производства продукции. Финансовые угрозы предприятия проявляются как осознанные вредоносные действия людей или организаций, либо как некачественная работа сотрудников предприятия или его партнёров; недостаточный контроль за структурой вложений предприятия, соотношением частей финансового портфеля по рискованности и доходности его составляющих. К финансовым угрозам также относят воздействия, причиной которых стали обстоятельства непреодолимой силы, не связанные напрямую с деятельностью предприятия.

Кадровые угрозы находят выражение, с одной стороны, в недостаточной квалификации сотрудников предприятия, слабой организации системы управления персоналом и т.п. Слабая квалификация персонала, нежелание или неспособность приносить максимальную пользу своему предприятию негативно воздействуют на экономическую безопасность предприятия. Среди объектов интеллектуальной собственности следует выделить изобретения, технические новации, ноу-хау, дизайн, компьютерные программы и т.п. Социальные факторы определяются стандартами жизненного уровня населения страны, куда входят уровень и системы оплаты труда, режим труда и отдыха, мотивация труда, структура персонала.

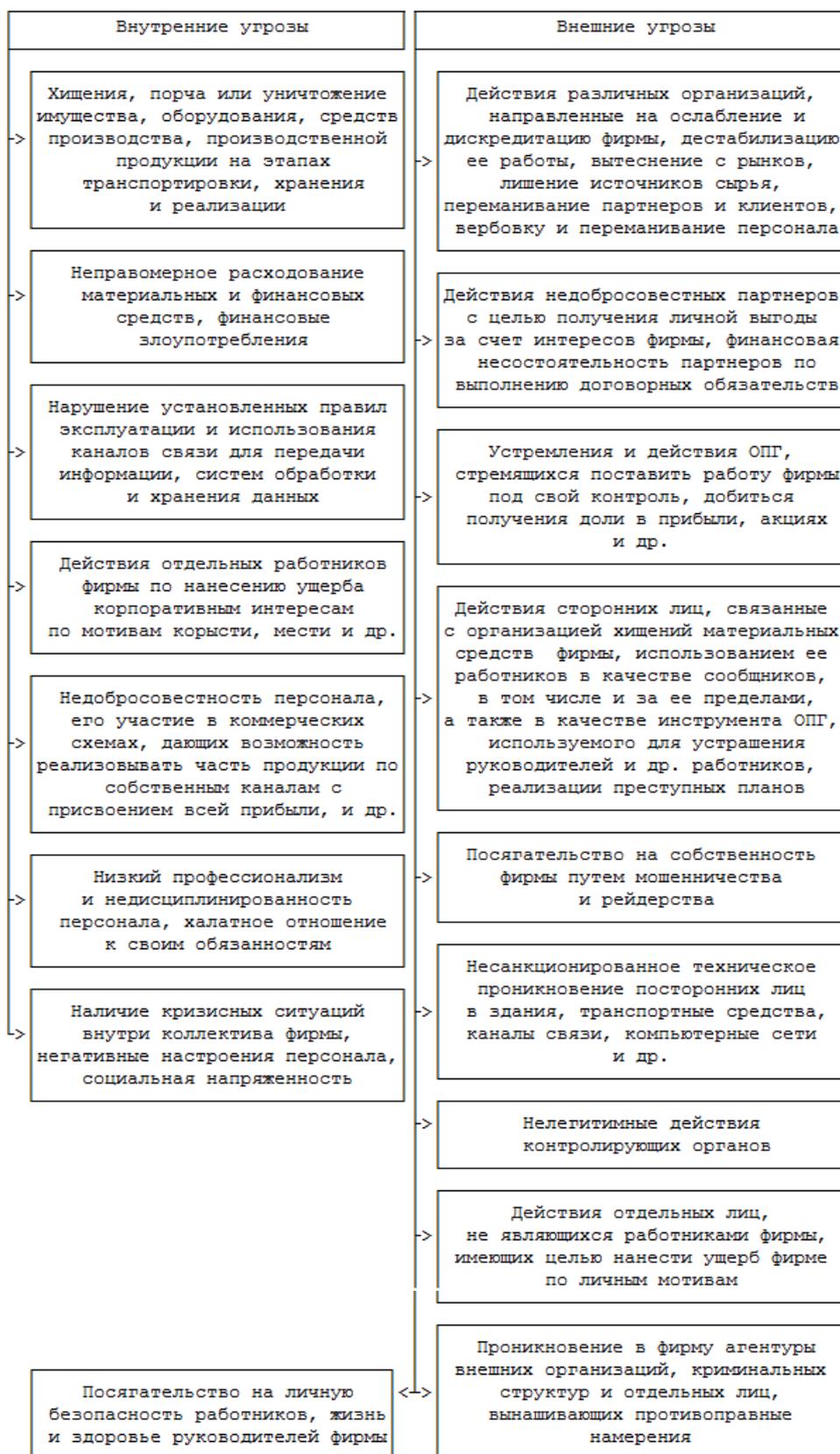


Рис. 1.3.3. Примерная классификация основных видов угроз безопасности организации
Ищейнов В.Я. *Безопасность фирмы от противоправных действий и недобросовестной конкуренции* // *Делопроизводство*. 2009. N 2.

Информационные угрозы включают различные группы злоумышленных и незлоумышленных воздействий. К первой группе относятся действия какихлибо лиц или организаций, имеющие своей целью нанесение ущерба благосостоянию по вопросам информационного обеспечения деятельности предприятия. Ко второй группе относятся, прежде всего, негативные внутренние воздействия, т.е. упущения и ошибки в деятельности информационно-аналитической службы предприятия.

Технико-технологическая составляющая угрозы - это несоответствие уровня используемых технологий лучшим мировым аналогам. Факторы производства определяют динамику производства в заданный период времени, уровень освоения производственной мощности, темпы обновления основных производственных фондов, прогрессивность технологии, ритмичность производства, технический ресурс, необходимый объем инвестиций в инновации.

Степень влияния факторов внешней и внутренней среды на экономическую безопасность предприятия определяется системой критериев и показателей оценки этого влияния. Для выработки мер, предупреждающих зарождающиеся угрозы социально-экономической безопасности предприятия необходимо четко определить индикаторы (показатели) социально-экономической безопасности предприятия и их пороговые значения. Целесообразно разделить все индикаторы, необходимые для мониторинга состояния уровня безопасности, разделить на две группы (рис. 1.3.4): регламентируемые государством; аналитические (расчетные).

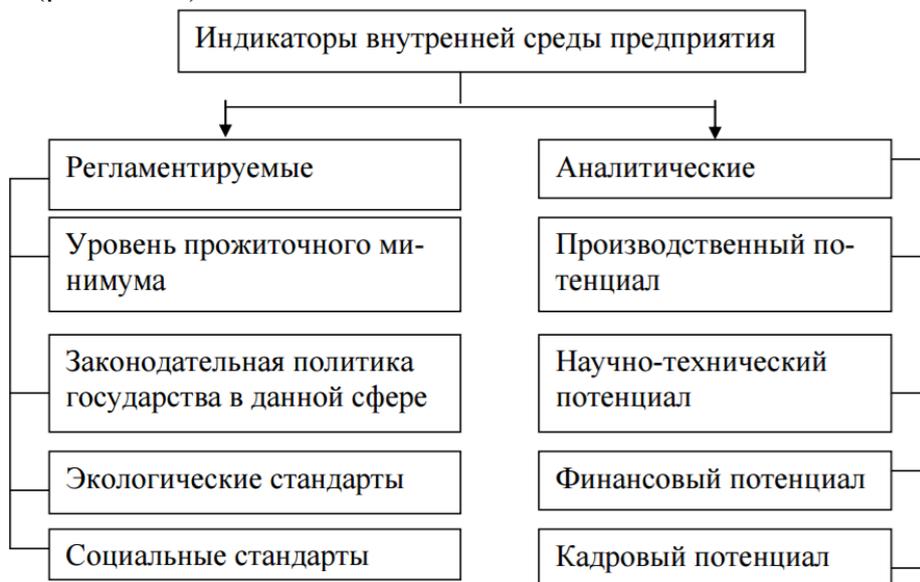


Рис. 1.3.4. Индикаторы экономической безопасности предприятия

Регламентируемые индикаторы определяются механизмом системы экономической безопасности и ее обеспечением законодательной политикой государства, которая включает совокупность законодательных актов, правовых норм, методов воздействия на объем с целью соблюдения стандартов безопасности в различных сферах деятельности, в первую очередь, в области социальной ориентации.

В каждой из сфер могут быть разработаны и утверждены на различных уровнях стандарты, уровень которых контролируется специальными органами. Требования стандартов, имеющих макроэкономическое значение, могут распространяться на все предприятия вне зависимости от их отраслевой принадлежности и форм собственности. К таким стандартам могут быть отнесены: уровень оплаты труда работающих, пороговым значением которого должен быть размер не ниже прожиточного минимума, установленного

государством; себестоимость продукции, пороговые значения которой являются общественно-необходимые затраты, определяемые методикой, используемой в системе бенчмаркетинга; норма прибыли, нижнее значение которой должно обеспечить уплаты регламентированных налоговой службой платежных обязательств; наличие доли рынка (спроса) на поставку продукции в объеме не ниже критического (точки безубыточности); нормы экономических стандартов и другие.

Евдокимов Ф.И., Бородин О.А. Экономическая безопасность предприятия: критерии и методы оценки // Экономика: проблемы теории та практики: збірник наукових праць. - Дніпропетровськ: ДНУ, 2004. - Випуск 192, Т. IV. - С.1134-1142.

Другой источник угроз - **внешняя среда** предприятия.

Внешнюю среду следует рассматривать как совокупность факторов, находящихся за пределами сферы влияния предприятия, характеризующихся высоким уровнем неопределенности, отсутствием общепринятой системы диагностики ее состояния и прогноза развития. Классификация факторов внешней среды позволяет разделить их на главные и второстепенные, объективные субъективные, контролируемые и неконтролируемые, реально существующие и потенциальные, управляемые и неуправляемые, случайные и детерминированные (рис. 1.3.5).



Рис. 1.3.5. Основные факторы внешней среды, влияющие на экономическую безопасность предприятия

Классификация факторов внешней среды позволяет выделить наиболее значимые факторы и абстрагироваться от малозначимых, сфокусировать анализ на ключевых факторах успеха. Если использовать такой прием для построения количественных и качественных факторов экономической безопасности предприятия, то в нее следует внести факторы внешней и внутренней среды. Задачей предприятия является контроль воздействия внешней среды и разработка мер оказания влияния на это воздействие, обеспечивающих защищенность от отрицательного влияния внешней среды. В практической деятельности предприятия весьма затруднительно определить все факторы внешней среды, влияющие на экономическую безопасность предприятия и вероятность наносимого ими ущерба. Поэтому среди них следует выделить те, которые могут контролироваться маркетинговой политикой предприятия, работающего на рынок.

Важно понимать, что ресурсы внешней среды ограничены. Высокая конкуренция в борьбе за ресурсы является причиной банкротства предприятий. Именно экономическая ответственность, формой реализации которой выступает банкротство, заставляет предприятия работать эффективно. В противном случае происходит перераспределение ресурсов от неэффективно к успешно работающим предприятиям. В этом проявляется жесткость рыночных механизмов регулирования экономических процессов.

Евдокимов Ф.И., Бородин О.А. Экономическая безопасность предприятия: критерии и методы оценки // Экономика: проблемы теории та практики: збірник наукових праць. - Дніпропетровськ: ДНУ, 2004. - Випуск 192, Т. IV. - С.1134-1142.

Из внешней среды в рыночной экономике могут исходить следующие угрозы:

- недружественные поглощения;
- взлом и разрушение информационного обеспечения работы предприятия (вирусы, сетевые атаки и т.п.);
- рейдерские атаки;
- недобросовестная конкуренция;
- атаки гринмейла;
- отрицательное влияние политических волнений;
- захват и передел собственности;
- неразвитая инфраструктура рынка;
- взяточничество;
- доступ конкурентов к коммерческой тайне;
- промышленный шпионаж;
- действия криминальных структур;
- кража материальных средств;
- мошенничество;
- повреждение активов и объектов основных средств предприятия.

Ключкова М.В. Экономическая безопасность предприятия как необходимый элемент управления предприятием в современной рыночной экономике // Системное управление, 2014. №4 (25). С. 53-58.

Существуют три внешних источника угрозы такому функционированию. Первый - это неблагоприятная для предприятия экономическая политика государства. Манипуляции последнего в целях регулирования экономики учетной ставкой, валютным курсом, ставками таможенного тарифа, налогов и т. д. могут в ряде случаев противоречить производственной, коммерческой и экономической политике предприятия.

Реальную опасность для предприятия также представляют административные гонения на рынок, насильственное сужение сферы товарно-денежных отношений, нарушения со стороны государственных органов законов, регламентирующих предпринимательскую деятельность, превышения ими установленной компетенции во взаимоотношениях с предприятием, необоснованное вмешательство в его производственную экономическую и коммерческую деятельность, различные формы посягательства на собственность предприятия и т. п.

При выходе на внешние рынки предприятие может подвергнуться негативному воздействию в результате неблагоприятной экономической политики иностранных государств. Серьезную угрозу для развития предприятия могут представлять политически мотивируемые действия по свертыванию или ограничению экономических связей. Экономические санкции ведут к взаимному недоверию и, подрывая материальную основу взаимоотношений, дестабилизируют безопасность в области экономики не только на межгосударственном уровне.

Вторым источником внешней угрозы для коммерческой деятельности предприятия

являются действия иных хозяйствующих субъектов. Прежде всего, речь идет о недобросовестной конкуренции, к действиям которой относятся:

- нарушения прав конкурентов на промышленную собственность (систематическое скрытое использование наименований конкурента, несанкционированное воспроизводство продукции конкурента, раскрытие секретов торговли и производства конкурента, промышленный шпионаж);

- подрыв репутации конкурента (распространение ложных сведений, дискредитирующих предприятие, продукцию, торговую деятельность конкурента; сравнительная, мошенническая и обманная реклама);

- дезорганизация производства конкурентов путем сманивания и подкупа их рабочих и служащих для завладения секретами торговли и производства;

- прочие недобросовестные действия (дискриминация конкурентов, бойкот, демпинг).

Недобросовестную конкуренцию дополняют протекционистские барьеры на государственном уровне. В данном случае речь идет об ограничительной деловой практике. **Ограничительная деловая практика** - это совокупность приемов монополистического давления на партнеров в торговле и потребителей, применяемых для захвата, удержания и реализации господствующего положения на рынках на основе ограничения конкуренции. Негласный характер барьеров, устанавливаемых с помощью ограничительной деловой практики непосредственными участниками торгового оборота, делает их особенно опасными, так как они подрывают действующие деловые отношения.

Российские предприятия при выходе на внешние рынки с уже сложившимися там монополистическими структурами попадают в категорию аутсайдеров ограничительной деловой практики в наибольшей степени. Причем в условиях жесткого давления на рынках с повышенным уровнем монополизации в самом неблагоприятном положении оказываются новые экспортеры промышленной продукции. В зависимости от субъекта выделяют две основные разновидности ограничительной деловой практики - индивидуальную и групповую. В первом случае субъектом ограничительной деловой практики выступает отдельная фирма, во втором - международные и национальные союзы предпринимателей.

Определенные возможности для борьбы с ограничительной деловой практикой на зарубежных рынках представляет антимонопольное законодательство, специально направленное на пресечение рыночных злоупотреблений монополистических предприятий. Кроме этого, существуют международные нормативы, разработанные по линии ООН и других учреждений, касающиеся ограничительной деловой практики.

Избежать ограничительной деловой практики российское предприятие может, например, путем перемещения сделок с одних фирм или рынков на другие. Однако сделать это значительно сложнее, если ограничительная практика осуществляется на коллективной основе. К наиболее распространенным приемам групповой ограничительной деловой практики относится разделение рынков и согласование цен.

Третий внешний источник угроз - кризисные явления в мировой экономике. Они «переливаются» из страны в страну через каналы внешних экономических связей. Последовательная интеграция России в мировую экономику порождает зависимость российских коммерческих предприятий от происходящих в мире экономических процессов (структурная перестройка, падение цен спроса и цен на энергоносители и др.). По мере втягивания национальной экономики в мировой воспроизводственный процесс усиливается ее подверженность влиянию внешних факторов. Таким образом, в стремлении к прибыльной деятельности современное предприятие, обеспечивая собственную безопасность, должно уделять внимание динамике спроса, политике правительства и центральных банков, отношениям с соперниками, тенденциям научно-технического прогресса, мировой политике и международной хозяйственной конъюнктуре и т. д.

Если с учетом данной позиции характеризовать современную обстановку в России, то

она, прежде всего, определяется устойчивой по своим темпам криминализацией страны и небывалым ростом уголовного терроризма, который все чаще приобретает политическую окраску. При этом национальная экономика и в том числе российский частный бизнес несут огромные потери.

Чтобы дать полную картину обстановки в российской национальной экономике, следует учитывать такие особенности нашего рынка, как: структурное деформирование национального хозяйства; размах промышленного и коммерческого шпионажа (со стороны различных структур, использующих методы агентурного и технического проникновения к коммерческой тайне); отсутствие единой стратегии обеспечения безопасности предпринимательских структур; отсутствие цивилизованных юридических гарантий для реализации коммерческих интересов предпринимателя.

Говоря о внутренних угрозах, следует подчеркнуть, что наиболее широкое распространение в российской действительности получили кражи, грабежи, разбои, мошенничество, вымогательство, взяточничество, злоупотребление служебным положением, должностной подлог, а также различные формы недобросовестной конкуренции и такие особо опасные формы, как заказные убийства и захват заложников.

Здесь же следует упомянуть и о таких особенностях российской экономики, как: низкая капитализация экономической системы; высокая степень монополизации экономики; высокая импортная зависимость и замкнутость экспорта на сырье; избыточность таможенных ограничений; низкая производительность труда.

Каранина Е.В. Финансовая безопасность (на уровне государства, региона, организации, личности) - Монография. Киров: ФГБОУ ВО «ВятГУ», 2015. 239 с.

Контроль воздействия предприятия на факторы экономической безопасности определяется способностью предприятия оказывать влияние на это воздействие. Предприятие может самостоятельно осуществлять выбор поставщиков ресурсов, средств производства, формы стимулирования покупателей, формировать сегменты и целевой рынка в зависимости от конъюнктуры. Однако оно не в состоянии контролировать решения, принимаемые государством в области налоговой политики, финансовой поддержки предприятий отдельных отраслей промышленности, определения курса национальной валюты. Трудность в оценке влияния контролируемых факторов внешней среды состоит в том, что они, как правило, не поддаются формализации.

Если учитывать, что внешние и внутренние угрозы различаются как реальные и потенциальные, то деятельность по обеспечению безопасности будет сводиться к прогнозированию угроз, определению и реализации наиболее эффективных мер по их локализации. Отсюда следует, что основой организации, планирования и реализации мер по обеспечению безопасности в различных сферах является анализ и оценка характера реальных и потенциальных внутренних и внешних угроз, кризисных ситуаций, а также прочих неблагоприятных факторов, препятствующих достижению поставленных целей и представляющих опасность для жизненно важных интересов организации.

Множество непреднамеренных угроз, которые связаны с внешними факторами, обусловлено влиянием воздействий, неподдающиеся предсказанию.

К внутренним непреднамеренным угрозам относят те, которые связаны с отказами коммуникационной и вычислительной техники, ошибками программного обеспечения, сотрудников, другими внутренними непреднамеренными воздействиями. Отдельно следует выделить угрозы связанные с преднамеренными ошибками, которые возникают за пределами бизнеса (табл. 1.3.2).

Таблица 1.3.2. Угрозы, связанные с преднамеренными ошибками

Угрозы	Характеристика
1. Несанкционированный доступ к информации, которая хранится в системе	Доступ к информации, который нарушает правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами
2. Отрицание действий, которые связаны с манипулированием информацией	В частности, несанкционированная модификация, которая приводит к нарушению целостности данных
3. Ввод в программные проекты и продукты «логических бомб»	Срабатывают при выполнении определенных условий или по истечении обусловленного периода времени и частично или полностью выводят из строя компьютерную систему
4. Разработка и распространение компьютерных вирусов	Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой»
5. Небрежность в разработке, поддержке и эксплуатации программного обеспечения, которые приводят к краху компьютерной системы	Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.
6. Изменение компьютерной информации и подделка электронных подписей	Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.
7. Хищение информации с последующей маскировкой	В частности, использование идентификатора, который не принадлежит пользователю, для получения доступа к ресурсам системы
8. Перехват	Например, нарушение конфиденциальности данных и сообщений
9. Отрицание действий или услуги	Отрицание существования утерянной информации
10. Отказ в предоставлении услуги	Комплекс нарушений, которые вызваны системными ошибками, несовместимостью компонент и ошибками в управлении

Угрозы предприятию, исходящие от внутренних и внешних источников опасности, определяют содержание деятельности по обеспечению внутренней и внешней безопасности.

Система безопасности организации сможет решать стоящие перед ней задачи только тогда, когда будет действовать, то есть ее неотъемлемым составным элементом являются практические действия по обеспечению безопасности бизнеса.

Таким образом, служба безопасности предприятия призвана на основе эффективного использования корпоративных ресурсов создать условия для достижения целей бизнеса,

своевременно обнаружить и максимально ослабить воздействие различного рода опасностей и угроз в условиях конкуренции и хозяйственного риска.

Попова Е.Н., Попова Т.Н. Экономическая безопасность предприятия, угрозы экономической безопасности предпринимательства // NovaInfo.Ru. 2016. Т. 3. № 54. С. 86-89.

Обеспечение экономической безопасности организаций необходимо рассматривать как процесс прогнозирования и предотвращения всесторонних ущербов от негативных воздействий на их экономическую безопасность по различным аспектам финансово-хозяйственной деятельности. Эффективный результат работы организаций по обеспечению доходности и устойчивости бизнеса может быть достигнут именно за счет прогнозирования и своевременного предотвращения ущербов, как очевидно представляющих угрозу экономической безопасности, так и потенциально вероятных.

Основополагающим элементом при исследовании экономической безопасности рассматриваемых организаций является выбор ее критерия. Он предполагает признак или суммы признаков, на основании которых делается заключение о состоянии экономической безопасности организации. Экономическую их безопасность можно оценивать с помощью различных критериев:

1. Организационная сторона - в этом случае предполагается сохранение как самих организаций, так и их организационной целостности, нормальное функционирование основных подразделений (отделов, служб и т.п.). Основные подразделения (производственные основные и вспомогательные цеха, службы снабжения и сбыта, конструкторско-технологические подразделения, финансово-экономические и маркетинговые управления, бухгалтерия, отдел кадров) выполняют все свои функции для достижения основной цели организаций;

2. Правовая сторона - имеется в виду постоянное обеспечение соответствия деятельности организаций действующему законодательству, что выражается в отсутствии претензий к нему со стороны правоохранительных органов (или контрагентов). Кроме того, отсутствуют потери от сделок с внешними партнерами вследствие нарушения последними законодательства (умышленно либо неумышленно). Это обеспечивается юридической экспертизой всех осуществляемых операций и сделок, заключаемых договоров;

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

4. Экономическая сторона - проявляется в стабильности или имеющих тенденцию к росту основных финансово-экономических показателей деятельности организаций таких, как собственный капитал, годовой объем реализации продукции, прибыль, рентабельность продаж, оборачиваемость активов, рентабельность активов, финансовый рычаг, рентабельность собственных активов. В них отражаются общие результаты обеспечения безопасности с организационной, правовой, информационной и собственно экономической сторон. Сюда могут входить такие показатели, как отсутствие штрафов, санкций со стороны государственных органов за нарушение законодательства (например, налогового, антимонопольного), отсутствие потерь от сделок с контрагентами.

Таким образом, организации могут испытывать воздействия различных физических и юридических лиц, которые несут негативные последствия, прежде всего, для их экономического состояния. В этом случае возникает понятие угрозы безопасности предпринимательства. Причем наиболее важное значение для организаций приобретают угрозы экономической безопасности, поскольку все потери (организационные, информационные, материальные, имиджа организации) в конечном счете, выражаются именно в экономических потерях (и все прочие угрозы в основе имеют, как правило, экономические мотивы). При этом количественная оценка уровня экономической безопасности должна исходить из показателей планирования, учета и анализа хозяйственной

деятельности рассматриваемых организаций. Для этого целесообразно исследовать показатели устойчивости организаций для обновления.

Самочкин В.Н., Барахов В.И. Экономическая безопасность промышленных предприятий // Известия Тульского государственного университета. Экономические и юридические науки. 2014. Выпуск № 3-1.

В целом экономическая безопасность организации предполагает:

- высокую финансовую эффективность, независимость и устойчивость работы организации;
- развитость и конкурентоспособность технологической базы организации;
- высокий уровень организации управления организацией;
- жесткий кадровый отбор;
- обеспечение соответствия экологическим стандартам;
- эффективный механизм правового регулирования всех направлений деятельности организации; обеспечение информационной безопасности работы организации;
- гарантии безопасности работников организации, а также сохранности их имущества и профессиональных интересов.