**Панкратьев Вячеслав Вячеславович**

# **М Е Т О Д И Ч Е С К О Е П О С О Б И Е**

#

**Корпоративная**

**безопасность**

**РИСК МЕНЕДЖМЕНТ**

**Москва**

**2023**

**РИСК МЕНЕДЖМЕНТ**

**Риск-менеджмент в корпоративной безопасности**

*Риск* — комбинация вероятности события и его последствий. Результат риска может быть как прибыль, так и убыток.

*Событие* — наступление определенного стечения обстоятельств.

*Угроза* – субъект или обстоятельства, которые намереваются причинить вред бизнесу.

*Уязвимость* – это недостаток средств защиты от угрозы.

*Отличие риска от угрозы*

* риск может привести как к положительному, так и к отрицательному результату, а реализация угрозы только к отрицательному;
* последствия риска можно разделить с кем то, а угрозу нет;
* риск (в негативном смысле) это сочетание угрозы и уязвимости

*Управление рисками организации* – это процесс, осуществляемый советом директоров, менеджерами и другими работниками, который начинается при разработке стратегии и затрагивает всю деятельность организации. Он направлен на определение событий, которые могут влиять на организацию, и управление связанным с этими событиями риском, а также контроль того, чтобы не был превышен риск-аппетит организации (допустимые пределы риска) и предоставлялась разумная гарантия достижения целей организации.

*Управление рисками организации:*

* представляет собой непрерывный процесс, охватывающий всю организацию;
* осуществляется работниками на всех уровнях организации;
* используется при разработке и формировании стратегии;
* применяется во всей организации, на каждом ее уровне и в каждом подразделении и включает анализ портфеля рисков на уровне организации;
* нацелено на определение событий, которые могут влиять на организацию и управление рисками таким образом, чтобы они не превышали готовности организации идти на риск (риск-аппетит);
* дает руководству и совету директоров организации разумную гарантию достижения целей;
* связано с достижением целей по одной или нескольким пересекающимся категориям.

*Стандарты риск-менеджмента*

* FERMA (Federation of European Risk Management Association) - разработан риск-менеджерами для постановки системы управления рисками любого предприятия. Предназначен для риск-менеджеров. Носит рекомендательный характер. Стандарт FERMA задает четыре типа рисков: стратегические, финансовые, операционные и риски опасностей. Кроме того, существуют внешние и внутренние факторы рисков;
* COSO ERM – стандарт, ориентированный на повышение достоверности отчетной документации на предприятии. Ориентирован на внутренних аудиторов. Является обязательным для публичных организаций, работающих на американском рынке;
* ГОСТ Р ИСО 31000-2019 Национальный стандарт РФ. Менеджмент риска. Принципы и руководство;
* ГОСТ Р 58771-2019 Национальный стандарт РФ. Менеджмент риска. Технологии оценки риска;
* Письмо Центрального Банка от 10 апреля 2014 г. N 06-52/2463 «О кодексе корпоративного управления».

*Автоматизация риск-менеджмента*

* [https://riskgap.ru](https://riskgap.ru/)

*Зоны ответственности по управлению рисками:*

* *совет директоров* - определение целей в области управления рисками, а также принципов организации и функционирования СУР, утверждение риск-аппетита;
* *комитет по аудиту* - мониторинг рисков и обеспечение контроля за надежностью и эффективностью СУР;
* *генеральный директор (правление)* - выделение необходимых ресурсов для обеспечения функционирования СУР и принятие решений, ведущих к достижению целей и задач в области управления рисками и соблюдению риск-аппетита;
* *руководитель подразделения по управлению рисками* – несет ответственность за развитие и функционирование СУР, содействие регулярному обмену информацией по рискам, контроль соблюдения риск-аппетита;
* *служба по управлению рисками* - координация процесса риск-менеджмента, агрегирование информации по рискам и содействие регулярному обмену информацией, мониторинг ключевых рисков;
* *владельцы рисков* - постоянное оперативное управление рисками, входящими в зону их компетенции;
* *управление внутреннего аудита* - оценка эффективности СУР

*Типовой функционал службы управления рисками:*

* осуществляет актуализацию рисков уровня предприятия и готовит отчетность по ключевым рискам;
* отвечает за организацию, координацию, контроль, методологическую поддержку и развитие процесса управления рисками;
* информирует руководство предприятия и совет директоров (включая комитет, в функции которого входит рассмотрение вопросов управления рисками) о состоянии СУР в компании и обеспечивает контроль за исполнением поручений совета директоров и первого лица компании в части развития СУР;
* инициирует процесс актуализации рисков, обеспечивает сбор и консолидацию информации, получаемой от подразделений;
* взаимодействует с руководителями и представителями бизнес - функций в рамках выявления и оценки рисков и обсуждения подходов к управлению рисками;
* инициирует процесс идентификации и актуализации рисков в проектах, стратегическом и бюджетном планировании;
* отвечает за подготовку материалов и результатов актуализации рисков для совета директоров (включая комитет, в функции которого входит рассмотрение вопросов управления рисками) и органов управления компании по мере необходимости;
* формирует и поддерживает в актуальном состоянии перечень владельцев рисков компании по результатам предложений руководителей соответствующих функций;
* ведет консолидированный реестр рисков головной компании и ДЗО

*Комитет по управлению рисками*

* комитет по управлению рисками может быть создан при руководстве компании (правлении), либо при совете директоров;
* данный орган создается для более тщательного рассмотрения вопросов управления рисками, определения риск-аппетита и отслеживания его соблюдения по ключевым рискам компании;
* на уровне совета директоров комитетом, в компетенции которого входит рассмотрение вопросов управления корпоративными рисками, является либо отдельный орган, либо один из существующих комитетов (создание которых регулируется, например, листинговыми требованиями), в частности, комитет по аудиту. Комитет по рискам создается для целей надзора за СУР, что соответствует передовым практикам управления рисками;
* кроме того, комитет по рискам может создаваться при правлении для более тщательной проработки вопросов по рискам до их последующего вынесения на рассмотрение совета директоров;
* вопросы управления рисками могут также рассматриваться на других функциональных комитетах при правлении, например, на комитете по инвестициям или бюджетном комитете;
* на уровне филиалов, дочерних и зависимых обществ могут создаваться локальные комитеты по рискам.

*Владельцы рисков*

* владельцами рисков являются представители высшего руководства или представители структурных подразделений, обладающие полномочиями для принятия управленческих решений, которые могут повлиять на уровень существенности рисков, курируемых структурными подразделениями. Владельцы рисков участвуют в определении границ допустимого уровня рисков и отвечают за их соблюдение;
* владельцы рисков на регулярной основе осуществляют идентификацию новых рисков, анализ и оценку рисков, а также разрабатывают и реализуют мероприятия по управлению профильными рисками;
* помимо закрепленной функциональной и административной подотчетности владельцы рисков отвечают за предоставление информации по курируемым рискам в службу риск-менеджмента. Для выполнения ряда организационных задач в процессе управления рисками владельцы рисков могут назначать риск-координаторов из числа подчиненных сотрудников. Назначение такого сотрудника чаще всего возможно только при условии создания института риск - координаторов по всей организации.

# *Внутренние документы системы управления рисками:*

* положение по управлению рисками;
* положение о комитете по управлению рисками;
* положение об отделе по управлению рисками;
* положения по управлению конкретными рисками;
* карта рисков;
* реестр рисков;
* внутренняя отчетность;
* иные документы.

*Система анализа и управления экономическими рисками включает в себя:*

1 этап – определение (идентификация) риска

2 этап – анализ риска

* сила воздействия;
* вероятность;
* классификация;
* владелец риска;
* вариант реализации;
* ключевые индикаторы риска;
* возможность управляемости и цена управления риском;
* определение границ допустимого риска (риск-аппетит).

3 этап – работа с риском

* принятие риска;
* отказ от риска;
* передача риска;
* управление риском.

4 этап – мониторинг ситуации

*Источники информации, которые позволяют выявить причины риска и возможные его виды:*

* личный опыт руководителей и специалистов;
* результаты ревизий;
* результаты аудита;
* результаты проверок контролирующими и правоохранительными органами;
* информационно-аналитические материалы;
* информация из СБ;
* информация из службы внутреннего контроля;
* материалы бухгалтерской отчетности;
* статистические данные;
* материалы маркетинговых исследований, информация из СМИ, Интернет

**Методы, используемые для прогнозирования рисков**

*Метод SWOT анализа*

Данный метод предполагает внесение в особую таблицу данных, характеризующих деятельность предприятия. Таблица состоит из четырех блоков:

* блок сила (strength) – в этом блоке анализируются наиболее сильные стороны предприятия, в том числе:
* продукция (высокое качество, низкая себестоимость, грамотное ценообразование, сильная реклама, монопольное положение на рынке и т.д.);
* сервис/персонал (высокий профессионализм персонала, развитие работников, социальные программы, сервисная поддержка, торговые марки, позиционирование и т.д.);
* инжиниринг и разработка новых продуктов (модернизация оборудования, совершенствование технологий, повышение качества и т.д.);
* менеджмент (низкие расходы на управление, мобильная структура, единая координация, быстрое прохождение управленческих сигналов и т.д.);
* возможность работать дистанционно, а также в условиях кризиса, пандемии и локдаунов
* блок слабость (weakness) – в этом блоке анализируются слабые стороны предприятия, в том числе долговые обязательства, низкая квалификация рабочих, трудовые конфликты, плохое качество продукции, неудачный имидж, устаревшее оборудование, неэффективные технологии и т.д.;
* блок возможности (oportunities) – в этом блоке анализируются возможности предприятия, в том числе:
* административные возможности (лоббирование, связь с административным ресурсом, зависимость органов государственной власти от предприятия, возможность влиять на принятие управленческих решений в государственных органах и т.д.);
* экономические возможности (возможности по наращиванию объемов производства, по получению заказов, по переориентации производства, по повышению качества, по снижению цены, по привлечению инвестиций, по получению кредитов и т.д.);
* научно-технические возможности (взаимодействие с НИИ, модернизация технологий, вложения в науку, иное участие в научной деятельности);
* рыночные возможности (сильная конкурентная позиция, рост спроса, монополизация, отсутствие товаров-заменителей и т.д.)
* блок угрозы (threats) – в этом блоке анализируются внешние условия, которые могут нанести вред предприятию, в том числе нехватка сырья, усиление государственного регулирования, появление новых конкурентов, санкции, изменение курса валют, возрастание процентных ставок на кредиты и т.д.

После заполнения таблицы рассматриваются комбинации полученных характеристик. Комбинации "возможности - сильные стороны" можно использовать как ориентиры стратегического развития, комбинации "возможности - слабые стороны" применять для внутренних преобразований, комбинации "угрозы - слабые стороны" рассматриваются как ограничения стратегического развития, комбинации "угрозы - сильные стороны" - как потенциальные стратегические преимущества.

*PEST анализ*

PEST анализ это инструмент, предназначенный для выявления политических (Р), экономических (Е), социальных (S) и технологических (T) факторов внешней среды, которые влияют на деятельность предприятия. Учитывая то, что PEST анализ касается внешних факторов, которые оказывают воздействие на деятельность предприятия, внешнюю среду принято разделять:

* макросреда (политика, экономика, социально-демографическая среда, научно-технический прогресс, природные факторы, пандемия и т.д.)
* микросреду (поставщики, покупатели, акционеры, конкуренты, кредиторы и т.д.)

*PESTLE – анализ*

PESTLE – анализ - политический, экономический, социальный, технологический, юридический, экологический. При применении анализируются риски, связанные с каждым из аспектов, приведенных в названии. По итогам анализа возникает перечень угроз, которые могут помешать в достижении целей. PESTLE можно расширить до STEEPLED (PESTLE + образовательный и демографический виды анализа).

*Метод диверсионного анализа*

Данный метод предполагает специальное моделирование возникновения нежелательных явлений, чтобы затем, найдя способы их нейтрализации, упредить их реальное появление. По сути, речь идет о придумывании диверсии, отсюда и название подхода. Естественно, после того, как диверсия придумана, следует проверить, не реализована ли она на практике, есть ли вероятность ее реализации и если такая возможность не исключается, необходимо решить, как этого не допустить.

Этапы метода диверсионного анализа

* определение диверсионной задачи в виде: «Дано предприятие, осуществляющее определенные виды деятельности. Необходимо создать для него максимально возможное количество вредных факторов»;
* определяются основные параметры работы предприятия и их значения для нормальной работы организации;
* выявляются вредные явления, которые могут нарушить нормальный режим работы предприятия и проводится их экспериментальный анализ, резко увеличивая или, наоборот уменьшая параметры этих явлений;
* определяются опасные зоны (болевые точки) т.е. наиболее уязвимые места в бизнес-процессах предприятия. Как правило, к типовым опасным зонам относятся зоны концентрации проходящих через систему потоков (потоки людей, денежные потоки, информационные потоки и т.п.), зоны, где работники выполняют большое количество разных функций, зоны контакта с внешней средой (зоны контакта с клиентами, с конкурентами, с проверяющими органами и т.п.), зоны стыковки разных систем, отделов (например, отдел закупок – отдел продаж – рекламный отдел – бухгалтерия, из-за несогласованности на стыках этих отделов часто возникают аварийные ситуации), зоны, в которых ответственные решения должны приниматься в условиях высокой неопределенности, недостатка времени и информации (в стрессовых обстоятельствах) и т.п.;
* анализируются причины вредных явлений и определяется, какие из них можно реализовать в данной задаче;
* анализируется обострение смоделированной ситуации, т.е. как усилить вредные эффекты.

*Метод сценариев*

 *Анализ сценариев.* При разработке стратегии развития компании возможны различные сценарии развития. Это  связано  с  каждым  из  аспектов,  причем каждый раздел стратегии должен быть взаимосвязан с другими. Выбрать приемлемый с точки зрения риска вариант позволяет метод анализа сценариев.

*Метод планирования непрерывности бизнеса*

 *Планирование непрерывности бизнеса.* Метод основан на выявлении возможных проблем, которые могут привести к кризису, связанному с невозможностью осуществлять деятельность на тех же условиях, что и раньше. Существуют стандарты по планированию непрерывности бизнеса, к примеру, британский BS 25999. В нем представлены типовые угрозы – эпидемии, пожары, наводнения, землятрясения, перебои в энергоснабжении, хакерские атаки, терроризм и т.д. Но стандарт надо настроить на российскую специфику (административное давление, черный PR, санкции, нарушение логистических цепочек, уход ключевых работников и т.д.).

*Метод рассмотрения каждого бизнес процесса*

 *Рассмотрение каждого бизнес процесса*. Самый эффективный способ для выявления операционных рисков. Основан на том, что все процессы подвергаются подробнейшему изучению на предмет - как возможностей для улучшения, так и негативных рисков.

*Метод HAZOP*

 *HAZOP (исследование опасностей и функционирования).* Это процесс детализации и идентификации проблем опасности и работоспособности системы, при этом под системой подразумевается промышленный объект. Основная задача – найти потенциально опасные процедуры, которые могут привести к нарушению функционирования системы.

*Метод FMEA*

 *Анализ видов и последствий отказов (FMEA).* Метод подразумевает рассмотрение всех возможных отказов (сбоев) в технологическом процессе и оценку последствий их реализации. Для его использования все возможные сбои (отказы, отключение оборудования, остановка конвеера и т.д.) классифицируются по величине последствий, и дальше подробно рассматривается все, начиная от самых критичных.

*Метод FTA*

 *Анализ дерева неисправности (FTA).* Метод основан на анализе комбинаций событий нижнего уровня, которые могут привести к нежелательному состоянию. Рассмотрение идет сверху вниз для каждого из событий, то есть для определенного события, например, взрыва, рассматриваются все возможные варианты, приводящие к нему. К примеру, взрыв происходит из-за повышения давления, скажем в котле. Соответственно возможными вариантами могут быть выход из строя предохранительного клапана, нарушение подачи какого-нибудь компонента, приводящее к взрывному росту давления, несвоевременное реагирование обслуживающего персонала, старение оборудования и т.д.

*Метод рабочих групп и мозгового штурма*

*Метод экспертных мнений*

*Метод аналогии*

*Метод анкетирования работников*

*Метод расследования причин и событий*

*Оценка риска*

*Оценка риска* – это совокупность аналитических мероприятий, позволяющих спрогнозировать возможность получения дополнительного дохода или определенной величины ущерба от возникшей рисковой ситуации. В решении данной задачи особое значение имеет своевременный расчет величины возможного ущерба, который, как правило, подсчитывается с помощью:

* статистического метода;
* экспертного метода;
* расчетно-аналитического метода.

*Статистический метод* позволяет проанализировать частоту возникновения того или иного вида непредсказуемых потерь в собственной компании, статистику потерь на аналогичных предприятиях, величину потерь и другие факты. При достаточном массиве данных можно спрогнозировать степень риска, частоту возникновения потерь и т.д. Принимая решение, необходимо сопоставить число случаев потерь с числом случаев, когда риск приводил к благоприятным последствиям и получению дохода, а также масштабы ущерба с дополнительно получаемой прибылью.

*Метод экспертных оценок* позволяет сопоставить представление о степени риска на основе изучения, сопоставления и использования опыта, знаний, расчетов специалистов (экспертов) по различным аспектам хозяйственной деятельности: менеджеров, маркетологов, финансистов, снабженцев и т.д.

*Расчетно-аналитический метод* основан на использовании теории вероятности, теории игр, на прикладных математических методах оценочных расчетов для построения графика вероятности возникновения потерь. Однако данный метод наиболее эффективен в производственном предпринимательстве, так как в нем конкретные величины имеют такие параметры, как простой оборудования, потери рабочего времени, увеличение процента брака, снижение производительности труда и др.

*По степени вероятности риски оцениваются как:*

* реальные, где вероятность может быть подсчитана, например, исходя из статистики, экспертным методом, методикой группового SWOT анализа и т.д.;
* потенциальные

*Определение допустимых пределов риска*

Определение допустимых пределов риска (ущерба) осуществляется на основе сопоставления величины прогнозируемого ущерба с точкой критического объема производства и в целом с зонами риска.

*Методы управления рисками подразделяются*

* методы минимизации потерь;
* методы возмещения потерь

*Методы минимизации потерь* позволяют уменьшить величину ущерба, когда риска избежать невозможно или он возникает внезапно. Они подразделяются на следующие виды:

* *методы упреждения риска*, которые позволяют уберечься от случайностей при помощи превентивных действий. К этим методам относится:
* стратегическое планирование, которое может снять большую часть неопределенности, предугадать появление узких мест в производственном цикле, упредить ослабление позиций предприятия в своем секторе рынка и т.д.;
* бюджетирование;
* использование защищенных счетов (например, спецсчета по оборонзаказу, счета-эскроу и т.д.);
* прогнозирование внешней экономической обстановки, которое включает в себя разработку сценариев развития и оценку рынка, прогнозирование поведения возможных партнеров, региональное или общеэкономическое прогнозирование;
* мониторинг рисков, а также мониторинг социально-экономической и нормативно-правовой среды. Полученные в ходе мониторинга результаты позволяют уловить новые тенденции во взаимоотношениях хозяйствующих субъектов, заблаговременно подготовиться к нормативным новшествам, предусмотреть необходимые меры для компенсации потерь;
* методы предотвращения убытков, например, установкой пожарной или охранной сигнализации и средств пожаротушения;
* работа «под заказ» (например гособоронзаказ);
* установление лимитов (показателей риска);
* метод активного целенаправленного маркетинга, который должен агрессивно формировать спрос на продукцию.
* *методы уклонения от риска*. Среди наиболее популярных можно отметить:
* отказ от нежелательных или опасных партнеров;
* отказ от рискованных проектов;
* продажа рискового актива.
* *методы локализации риска* используются, когда удается четко и конкретно вычислить и идентифицировать источники риска. Вычислив экономически опасный участок или этап, необходимо сделать его контролируемым и тем самым снизить уровень риска (ущерба). Для реализации этого метода создаются и используются дочерние предприятия или специальные структурные подразделения для выполнения рискованных проектов;
* *Распределение или передача риска* достигается путем:
* различного рода интеграции с другими участниками, заинтересованными в успехе общих дел. С этой целью могут создаваться акционерные общества, холдинги, приобретение акций другого предприятия, вступление в ассоциации, концерны и т.д.;
* передачи на аутсорсинг отдельных направлений деятельности;
* заключение договоров, где риски «перекинуты» на другую сторону договора;
* приобретение контроля над деятельностью в связанных областях;
* хеджирование, например заключение долгосрочного договора по фиксированной цене;
* диверсификация сбыта;
* диверсификация логистики;
* диверсификация закупок;
* диверсификация инвестиций;
* диверсификация деятельности;
* распределение риска по времени.

*Методы возмещения потерь* направлены на то, чтобы в случае возникновения потерь иметь возможность их возмещения. Они подразделяются на следующие виды:

* *создание системы резервов* предполагает создание запасов сырья, материалов, комплектующих изделий, денежных средств, формирование планов их использования в кризисных ситуациях, установление запасных контактов и связей;
* *страхования хозяйственных рисков;*
* *использование гарантов -* банковские гарантии, гарантии государства и т.д.;
* *использование ст.* 406.1 ГК РФ - возмещение потерь, возникших в случае наступления определенных в договоре обстоятельств

*Система управления рисками характеризуется следующим:*

* определена стратегия и цели управления рисками, которые согласуются со стратегией развития организации;
* разработана детальная нормативно - методическая документация по СУР, при этом верхнеуровневый документ (политика) утвержден Советом директоров;
* закреплена и используется единая терминология в области управления рисками;
* определены и закреплены в нормативных документах организации роли, полномочия и ответственность участников процесса управления рисками в рамках СУР;
* система мотивации руководства включает цели по управлению рисками;
* определены задачи, шаги и ожидаемые результаты в рамках процесса управления рисками;
* определена система отчетности по рискам и выстроен непрерывный мониторинг уровня риска и ключевых рисков;
* разрабатываются, реализуются и по мере необходимости пересматриваются мероприятия по управлению рисками, на реализацию мероприятий выделяются необходимые ресурсы в соответствии с приоритетностью рисков и мероприятий;
* риск-аппетит утвержден, пересматривается при необходимости, доведен до сведения всех бизнес-функций и используется при принятии управленческих решений;
* осуществляется оценка эффективности СУР и принимаются меры по развитию риск-ориентированной культуры.

**Риск-менеджмент в экономической безопасности**

*Виды рисков:*

* *экономические* (макроэкономические риски, связанные с экономикой страны и мира, зависимость от импорта, пандемия, ориентировка на экспорт продукции и т.д.);
* *политические* (административный ресурс, взаимоотношения с государственными контролирующими и правоохранительными органами, принятие политических решений, государственная монополизация отдельных отраслей, санкции, импортозамещение и т.д.);
* *юридические* (изменение законодательства, оформление разрешительных и правоустанавливающих документов, первичная приватизация, условия договора и т.д.);
* *предпринимательские* (взаимоотношения с контрагентами, конкурентами, изменение спроса-предложения, локдауны и т.д.);
* *социальные* (национальные особенности, менталитет, низкий уровень жизни и платежеспособность населения, социальные волнения и т.д.);
* *управленческие* (незащищенная структура бизнеса, принятие неправильных управленческих решений, непрофессионализм управленцев, незащищенность лиц, принимающих решение, личные интересы лиц, принимающих решение и т.д.);
* *финансовые и инвестиционные* (отсутствие финансирования, валютные риски, кредиты, налоги, штрафы, дебиторская задолженность и т.д.);
* *информационные* *и репутационные* (разглашение информации, недостоверная информация, отсутствие информации, манипулирование, черный PR, информационное противоборство, риски, связанные с ИТ безопасностью и т.д.);
* *технические и технологические* (технологические аварии, технические сбои, устаревшие технологии, устаревшее оборудование, нарушение технологий и т.д.);
* *имущественные* (кражи, неправомерное использование, порча и т.д.);
* *кадровые* (противоправные действия, некомпетентность, халатность, злоупотребление правом, психологические конфликты и т.д.);
* *природные* (наводнения, землетрясения, природные пожары, низкая температура воздуха и т.д.);
* *техногенные* (чрезвычайные ситуации, пандемия, пожары, террористические акты, диверсии, военные действия и т.д.);
* *невыполнение социальных функций.*

*Факторы, учитываемые при оценке экономических рисков:*

*Политические факторы:*

* выборы всех уровней (человеческий фактор в административном ресурсе);
* изменение законодательства;
* государственное регулирование в отрасли;
* государственное регулирование конкуренции;
* административные решения;
* санкции;
* импортозамещение;
* вступление государства в международные договоры, присоединение к конвенциям и т.д.;

*Экономические факторы:*

* инфляция;
* валютные риски;
* экономическое развитие (ВВП и т.д.);
* ставка рефинансирование ЦБ;
* рынок и торговые циклы;
* покупательский спрос;
* затраты предприятия (энергетика, коммуникации, сырье и т.д.);
* ценовая политика и надежность поставщиков.

*Социально-культурные факторы:*

* занятость населения;
* базовые ценности населения, культура;
* платежеспособность населения;
* отношение к труду и отдыху;
* влияние СМИ и социальных медиаресурсов;
* демографические изменения;
* религиозные факторы;
* социальная напряженность;
* уровень образованности;
* производительность труда;
* преступность.

*Технологические факторы:*

* патенты;
* НИОКРы;
* технологии, особенно информационные;
* цифровизация;
* новые продукты;
* стартапы и экосистемы

*Правовые факторы:*

* дискриминационные законы;
* антимонопольные законы;
* социальные законы (занятость населения, безопасность населения, защита прав потребителей и т.д.);
* законы об авторском и патентном праве;
* законы об информационном праве (персональные данные, коммерческая тайна и т.д.)

*Экологические факторы:*

* климатические изменения;
* защита окружающей среды;
* экологические продукты;
* экологические стандарты;
* стандарты переработки;
* возобновляемые источники энергии

*Виды рисков*

*По возможности предвидения:*

* прогнозируемые риски — это риски, которые возможно спрогнозировать;
* непрогнозируемые риски — это риски, которые нельзя спрогнозировать.

*По характеру проявления во времени:*

* постоянный риск, он характерен для всего периода ведения деятельности предприятия и связан с действием постоянных факторов (например, выдача кредитов банком это постоянный риск);
* временный риск, он носит временный характер, возникающий лишь на отдельных временных этапах (например, на период действия договора).

*По возможности передачи (страхования):*

* передаваемые (страхуемые) риски — это риски, которые могут быть переданы, например, в порядке внешнего страхования соответствующим страховым организациям;
* не передаваемые (не страхуемые) риски — это риски, которые нельзя передать иным организациям, например, по которым отсутствует предложение соответствующих страховых продуктов на страховом рынке.

*По источникам возникновения:*

* внешний риск — это риск, не зависящий от деятельности предприятия;
* внутренний риск — это риск, зависящий от деятельности предприятия.

*По размеру возможного ущерба (воздействию):*

* критический риск  — это риск, потери по которому могут обанкротить предприятие;
* не критический риск – это риск, потери по которому организация может принять (допустить).

*Типы критических рисков*

* взаимоотношения с административным ресурсом (отзыв лицензии, приостановка деятельности предприятия, закрытие бизнеса, неуплата налогов, изменение законодательства, принятие политических решений, принятие управленческих решений, введение санкции и т.д.);
* взаимоотношения со стратегическими партнерами (разрыв франшизы, дилерского соглашения, расторжение договора с ключевым партнером и т.д.);
* неправильное принятие стратегических решений исполнительными органами (кредиты, бизнес-планы, слияния и поглощения и т.д.);
* конфликты между учредителями или акционерами;
* юридические ошибки (незаконная приватизация и т.д.);
* технологические риски;
* имиджевые риски;
* субъективные риски (человеческий фактор).

*Риски со стороны административного ресурса реализуются:*

* несовершенство и изменчивость законодательства;
* принятие государственных решений;
* государственная монополизация;
* курс на импортозамещение (например, запрет использования иностранного программного обеспечения)
* коррупция;
* использование административного ресурса конкурентами;
* интересы государства в бизнесе.

*Способы защиты от рисков со стороны административного ресурса:*

* не нарушать требования законодательства;
* не привлекать внимание;
* юридическая защита (суды, адвокаты и т.д.);
* прокурорская защита;
* жалобы в вышестоящие государственные органы;
* сотрудничество с административным ресурсом;
* включение интересов государства в бизнес (акции принадлежат государству, участие в гособоронзаказе, вхождение в госкорпорацию и т.д.);
* сотрудничество с общественно-политическими организациями (например, с торгово-промышленной палатой);
* сотрудничество с политическими партиями;
* ведение социально ориентированного бизнеса;
* информационная защита (информирование в интернете, СМИ и т.д.);
* изменение юрисдикции бизнеса (оффшор, иностранные акционеры, иностранный капитал и т.д.);
* вывод активов и отъезд в другую страну.

*Риски со стороны конкурентов реализуются:*

* законные способы ведения конкурентной борьбы (наличие конкурентных преимуществ и т.д.);
* незаконные способы ведения конкурентной борьбы (промышленный шпионаж, нарушение антимонопольного законодательства, картельный сговор, демпинг, неправомерное использование товарных знаков, незаконный доступ к коммерческой информации и т.д.);
* неэтические способы ведения конкурентной борьбы (переманивание персонала, черный пиар, маскировка под известный бренд, использование административного ресурса, использование своего доминирования на рынке и т.д.).

*Способы защиты от неэтических действий конкурентов (например, черного PR)*

* активный белый PR своей компании;
* не оправдываться, но признать свою ошибку (если она была) и обещать ее исправить;
* быстрота реагирования;
* официальные заявления первых лиц и официальных источников. Акцент на дискредитацию и антирекламу;
* обеспечить доступность сайта и ресурсов предприятия. Разместить соответствующую информацию на сайте;
* обеспечить доступность колл-центров (провести инструктаж что говорить, а что нет);
* обеспечить скоординированные действия между подразделениями (создание оперативного штаба, СБ, реклама, информационная безопасность, руководители подразделений и т.д.);
* ограничить доступ к информации;
* использовать юридическую защиту (суд, ФАС и т.д.);
* дискредитация конкурента;
* дискредитация информации;
* использовать «окна авертона»;
* доведение ситуации до абсурда;
* информационное контрнападение;
* увод ситуации в сторону.

**Информация об авторе:**

**Панкратьев Вячеслав Вячеславович –** полковник юстиции в запасе, заведующий кафедрой безопасности в Университете государственного и муниципального управления, эксперт в области корпоративной безопасности, защите активов и управлению рисками. Преподаватель - консультант, автор и ведущий обучающих семинаров и курсов повышения квалификации по тематикам, связанных с корпоративной безопасностью. Опыт преподавания и консалтинга с 1997 года. Автор книг и методических пособий по безопасности предпринимательской деятельности. Независимый консультант. Разработчик методик аудита безопасности предприятия и создания КСБ – корпоративных стандартов безопасности.

**www.vvpankrat.ru**

**vv\_pankrat@mail.ru**

**+7-963-632-41-20**