УДК 336

Совершенствование систем контроллинга промышленных предприятий под влиянием современных угроз

Рахлис Т.П., к.п.н., доцент,
доцент кафедры экономики и финансов
Андреева А.В., магистрант гр. зЭЭм-17-2
ФГБОУ ВО «МГТУ им. Г.И. Носова»
e-mail: twins08@yandex.ru, andreevaandreeva1@mail.ru
Россия, Магнитогорск

Аннотация: В статье рассматривается проблема актуальности систем контроллинга промышленных предприятий путем анализа существующих методов управления стандартными рисками и выявления новейших угроз, требующих новых решений. В результате исследования были предложены рекомендации по управлению современными рисками.

Ключевые слова: системы контроллинга, современный риск, внешние угрозы, терроризм, экстремизм, киберугроза, киберриски.

В настоящее время управление рисками с помощью системы контроллинга является неотъемлемым элементом корпоративного управления промышленного предприятия. В условиях воздействия большого числа постоянно меняющихся факторов комплексная система управления рисками должна быть гибкой и соответствовать текущим тенденциям.

Актуализировать систему контроллинга под влиянием новых современных угроз и опасностей, которые появляются с течением времени, становится всё более необходимым для эффективного управления хозяйствующим субъектом. В промышленности управление рисками становится более значимым, так как отрасль черной металлургии является одной из ключевых для поддержания оборонного комплекса нашей страны [1].

К угрозам деятельности промышленного предприятия принято относить стандартные факторы, возникающие в разных сферах его деятельности. Российские и зарубежные исследователи, как правило, разделяют риски по сфере возникновения на внешние и внутренние.

В качестве примера, приведем классификацию рисков, предложенную профессорами Б. Мильнером и Ф. Лиисом [2]. К внешним факторам риска авторы относят причины, влияющие извне:

- политические;
- законодательные;
- природные;
- региональные;
- отраслевые;
- макроэкономические.

Внутренними Б. Мильнер и Ф. Лиис называют факторы, возникающие в процессе деятельности самого предприятия:

1. Производственные (квалификационные, технологические, транспортные);
2. Коммерческие (ценовая дискриминация, потеря конкурентоспособности);
3. Инвестиционные (риск снижения доходности, деловой риск, временной и селективный риск).

С учетом таких типичных опасных факторов были разработаны многие системы контроллинга отечественных промышленных предприятий. Это объясняется отсутствием теоретической информационной основы в течение длительного периода, нехваткой соответствующих исследований и опыта в сфере управления рисками на предприятиях России [3]. Системы контроллинга ориентированы на выявление и минимизацию общепринятых рисков, не учитывая быстрое изменение внешней среды.

Рассмотрим категории рисков, которые охватывает система контроллинга одного из крупнейших промышленных холдингов России ПАО «ММК». Магнитогорский металлургический комбинат одним из первых предприятий чёрной металлургии внедрил комплексную систему управления рисками, удовлетворяющую международным стандартам и лучшим практикам риск-менеджмента. На рисунке 1 представлены категории опасных факторов для промышленного предприятия, для которых разработаны соответствующие методы управления [4]:

Категории рисков
Отраслевые риски: - **Изменение спроса и цен на производимую металлопродукцию** - **Рост цен на сырье, материалы, услуги** - **Внутриотраслевая конкуренция**
Страновые риски
Социальные риски
Финансовые риски: - **Валютный риск** - **Процентный риск** - **Кредитный риск**
Правовые риски: - **Риски, связанные с изменением налогового законодательства** - **Риски, связанные с изменением валютного регулирования** - **Риски, связанные с изменением правил таможенного контроля и пошлин**
Риски, связанные с экологией, охраной труда, промышленной безопасностью

Рисунок 1 – Система управления рисками ПАО «ММК»

Подробное описание методов и решений, которые применяются для управления данными рисками, содержит таблица 1:

Таблица 1 – Система управления рисками ПАО «ММК»

Риск	Управление риском
Изменение спроса и цен на производимую металлопродукцию	Диверсификация круга потребителей, активная маркетинговая политика, заключение долгосрочных контрактов, развитие сбытовой сети, переориентация производства на более востребованные виды продукции, расширение сортамента производимой продукции.
Рост цен на сырье, материалы, услуги	Расширение собственной базы, заключение долгосрочных договоров на поставку сырья с фиксированными условиями и формулами ценообразования, диверсификация ключевых поставщиков сырья.
Внутриотраслевая конкуренция	Главные факторы конкурентоспособности, позволяющие снижать риски: цена, качество, местоположение относительно ключевых потребителей и поставщиков, налаженная логистическая инфраструктура, удержание темпа роста условнопостоянных расходов ниже инфляционного уровня.
Страновые риски	Мониторинг ситуации на привлекательных рынках. Для минимизации возможных последствий реализации страновых рисков компания предпримет все необходимые разумные меры по взаимодействию с регуляторами, отраслевыми организациями и объединениями, приоритетными контрагентами.
Социальные риски	Реализация программ лечения и медицинского обслуживания работников; поддержка многодетных семей, материнства и стимулирования рождаемости; реализация жилищных и молодежных программ, организация культурно-массовых и спортивных мероприятий.
Валютный риск	В настоящее время расходы и поступления ПАО «ММК» в иностранных валютах сбалансированы. Предпринимаются меры по естественному снижению валютных рисков путем оптимизации валютной позиции по каждой из валют.
Процентный риск	Поддержание оптимальной структуры кредитного портфеля в различных валютах в сочетании с типом процентной ставки: фиксированной и плавающей, а также мониторинга уровня процентного риска.

Кредитный риск	Оценка кредитоспособности покупателей при поставке продукции с отсрочкой платежа, устанавливаются лимиты и различные виды обеспечения, применяется факторинговая схема оплаты.
Риски, связанные с изменением налогового законодательства	Мониторинг изменений налогового законодательства, изменений в правоприменении действующих законоположений. Оценка и прогноз степени возможного негативного влияния изменений налогового законодательства.
Риски, связанные с изменением валютного регулирования	Компания на постоянной основе осуществляет мониторинг изменений в валютном законодательстве, оценивается их возможное влияние на компанию.
Риски, связанные с изменением правил таможенного контроля и пошлин	Компания выполняет требования таможенного контроля, своевременно оформляет всю документацию, необходимую для осуществления как экспортных, так и импортных операций, и располагает достаточными финансовыми и кадровыми ресурсами для соблюдения норм и правил в сфере таможенного регулирования.
Риски экологии	ПАО «ММК» имеет всю разрешительную документацию в области охраны окружающей среды. Все инвестиционные проекты, проходят необходимую государственную экологическую экспертизу, общественные слушания по вопросам охраны окружающей среды. Контроль реализации экологической политики и мероприятий по снижению воздействия на окружающую среду ежегодно рассматривается на совете директоров ПАО «ММК», что позволяет эффективно управлять экологическим риском.
Риски охраны труда и промышленной безопасности	Соответствующие службы комбината уделяют пристальное внимание условиям труда, состоянию санитарно-бытовых помещений, обеспечению работников средствами индивидуальной защиты и прочим. В соответствии с Политикой в области промышленной безопасности и охраны труда ПАО «ММК» непрерывно совершенствует СУПБОТ, рассматривая ее как одну из составляющих устойчивого развития предприятия. Ежегодно проводятся смотры-конкурсы по безопасности труда и снижению производственного травматизма, специальная оценка условий труда, медицинские

	осмотры, обучение персонала принципам промышленной безопасности и охраны труда.

Таким образом, можно сделать вывод, что система контроллинга ПАО «ММК» включает в управление многие стандартные риски: финансовые, отраслевые, экономические, правовые, социальные, экологические и т.д. Современные реалии таковы, что новейшие угрозы приобретают все больший охват и несут опасность не только для функционирования экономических субъектов, но и для экономики всей страны. Рассмотрим некоторые из них, например, террористические атаки и киберриски.

Терроризм - идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий [5].

Террористический акт, произошедший на предприятиях промышленности, может быть направлен, как правило, на вывод из строя технологических систем объекта особой стратегической важности. Теракт также может быть устроен с целью дестабилизации выпуска, переработки, перевозки, хранения продукции; химического и радиоактивного заражения местности; захвата заложников и уничтожение людей, сеяния паники среди населения; давления на государственные органы для удовлетворения политических и экономических требований и т.д. В связи с этим любое предприятие должно включать в систему контроллинга меры по антитеррористической защищенности объекта.

В процессе глобализации все больший масштаб приобретает новый вид угрозы – киберпреступность. К киберрискам относятся риски, ставшие последствием реализации преднамеренных злоумышленных действий, посредством использования IT, и направленных на неавторизованное раскрытие, изменение или разрушение цифровых активов.

К таким рискам можно отнести [6]:

- риск хищения конфиденциальной информации и ее дальнейшего использования работниками организации;
- риск хищения преступниками информации о клиентов банков, такой как номера кредитных карт и счетов;
- риск кражи денег со счетов клиентов банков;
- риск разглашения секретной информации сотрудников компании;
- риск остановки работы предприятия из-за сбоев компьютерной сети, сайта организации и т. п.;
- получения убытка организацией, в связи с размещением ложной информации и др.

Исходя из выше сказанного, в условиях воздействия внешних угроз системы контроллинга современных промышленных холдингов должны быть усовершенствованы путем внедрения мероприятий по управлению новейшими рисками. Поэтому для комплексной системы управления рисками

ПАО «ММК» разработаны и предложены специальные меры для минимизации данных рисков.

Для управления риском террористической атаки необходима разработка особого документа, так называемого «паспорта безопасности» объекта, который будет предназначен для прогнозирования и оценки степени поражения объекта от воздействия террористических актов в виде взрыва, пожара и выброса отравляющих и радиоактивных веществ. А также для оценки надежности системы защиты производственного персонала, оценки степени поражения технологических систем и оборудования, инженерных коммуникаций и энергетических сетей. Данный нормативный документ отвечает за обеспечение безопасности предприятия.

Кроме того, необходимо обеспечить выполнение профилактических мероприятий:

1) Обеспечение персонала компании информацией о действиях во время террористического акта и обучение эвакуации.

2) Проведение учений и тренировок по защите объекта от террористической угрозы.

3) Создание возможностей для оперативного оповещения всех людей, находящихся на территории организации, об экстренной ситуации, их инструктирование.

4) Установление особого порядка доступа на предприятие и к его отдельным частям. Осуществляется путем разработки особой документации, внедрением технических средств контроля на КПП и входах в особо важные узлы объекта.

5) Монтаж наибольшего количества инженерно-технических средств защиты на местах, приближенных к критическим для объекта зонам, а также на участках, которые сложно просмотреть с помощью средств видеонаблюдения.

6) Обеспечение оперативной связи с органами быстрого реагирования посредством современных средств коммуникации.

Управление кибер-рисками будет представлять собой комплекс специальных действий. Во-первых, необходимо серьезное обучение конечных пользователей, подразумевающее практику соблюдения требований к обработке данных, распознавание попыток фишинга и процедур для противодействия попыткам социнженерии. Во-вторых, для управления кибер-рисками необходимо обновление программного обеспечения, обязательное наличие брандмауэра и антивирусной программы, установка на все ПК IDS / IPS - систем обнаружения вторжений и систем предотвращения вторжений [7]. В-третьих, нужен постоянный мониторинг событий безопасности и разработка плана реагирования на инциденты. И неотъемлемой частью управления кибер-рисками является современное направление - киберстрахование.

Таким образом, актуализация системы контроллинга промышленного предприятия является важным современным подходом к управлению. Эффективное присутствие промышленных предприятий на рынке возможно благодаря повышению гибкости компании, возможности предвидения

существенных перемен и формирования системного управления бизнес-процессами организации.

Список литературы:

1. Скворцова Н.В., Рахлис Т.П. Инвестиционная привлекательность как фактор социально-экономического развития // В сборнике: Российские регионы в фокусе перемен сборник докладов XII Международной конференции. Министерство образования и науки Российской Федерации; Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, Высшая школа экономики и менеджмента. Екатеринбург, 2018. С. 69-78.
2. Мильнер Б. Управление современной компанией: Учебник // Б. Мильнер [и др.] – М.: ИНФРА-М, 2001. — 350 с.
3. Скворцова Н.В., Рахлис Т.П. Микроэлектроника как вектор инновационного развития экономики // Экономика и предпринимательство. 2016. № 4-2 (69-2). С. 135-141.
4. Годовой отчет ПАО «ММК» за 2017 год [Электронный ресурс]. URL: http://www.mmk.ru/upload/iblock/9dd/1%20%D0%93%D0%9E%202017.pdf (дата обращения: 20.05.2019)
5. Федеральный закон "О противодействии терроризму" от 06.03.2006 N 35-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_58840 (дата обращения: 10.05.2019)
6. Волкова Т.А., Суслякова О.Н. Страхование информационных рисков (киберстрахование) // Инновационная экономика: перспективы развития и совершенствования. 2018. №7 (33).
7. Медведев В.В. Возможность выработки требований к системе защиты от вредоносных программ // Прикладная информатика. 2015. №3 (57).

Контактный телефон +79026035924