институты независимой оценки. В целом нефинансовая отчетность в корпоративном секторе в России развивается поступательно, в соответствии с мировыми тенденциями, становится все более распространенной практикой.

Список использованной литературы.

1. Нефинансовая отчетность [Электронный ресурс] // Сайт Агентства социальной информации «Социальная ответственность бизнеса». 2012. URL: http://www.soc-otvet.ru/asi/nonfinancialreporting (дата обращения: 1.10.2014 г.).

2. Нефинансовая отчетность [Электронный ресурс] // Российский союз промышленников и предпринимателей. 2014. URL: http://rspp.ru/simplepage/475 (дата обращения: 3.10.2014 г.).

3. Доклад о состоянии делового климата в России в 2010-2013 годах [Электронный ресурс] // Российский союз промышленников и предпринимателей. 2014. URL: http://media.rspp.ru/document/1/0/5/052e120269d00aa294ee8c2aa1c311df.pdf (дата обращения: 3.10.2014 г.).

4. Социальная отчетность корпораций [Электронный ресурс] // МСФО ФМ. 2013. URL: http://www.msfofm.ru/library/191-social-responcibility-of-companies (дата обращения: 29.09.2014 г.).

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ ПРЕДПРИЯТИЯ В УСЛОВИЯХ СЕТЕВОЙ ЭКОНОМИКИ

Л.М. Борисова

Томский политехнический университет, г. Томск
E-mail: unexx@rambler.ru

В наше время возникновение сетевых особенностей в экономике связывают с развитием информационных технологий, что приводит к эволюции современных экономических систем, развитию нерыночных механизмов регулирования и сетевых организационных структур. Другими словами, сетевые экономические отношения играют особую роль в процессе координации экономических взаимодействий. Данные изменения обостряют проблему экономической безопасности предприятия в условиях развития межорганизационных взаимодействий формального и неформального характера с позиции сетевой экономики.

Реалии современной хозяйственной жизни вызывают существенные изменения в координации экономических взаимодействий. Нарастание динамики экономических процессов и увеличение плотности экономических отношений предопределяют возрастание роли новых механизмов координации. Усиливаются процессы институционализации экономических взаимодействий, происходит самоорганизация экономических взаимодействий на фоне запаздывания формальных экономических институтов. При этом возрастает роль сетевых экономических отношений, которые оказывают существенное влияние на экономическую безопасность предприятия.

Использование сетевого принципа организации деятельности предприятия позволяет обеспечить эффективное его функционирование как системы в целом и его элементов в отдельности.

В любой социально-экономической системе субъекты вступают во взаимодействия. Устойчивое повторение этих взаимодействий приводит к формированию определенных правил и принципов. В свою очередь сформированные правила и принципы можно рассматривать как механизм координации экономических взаимодействий.

Новые модели действия и информационные сети позволяют облегчить действия в пределах и между предприятиями практически во всех отраслях. Возможности, свойственные информационной сети для маркетинга продуктов производства могут также помочь предприятиям малого и среднего бизнеса (ПМСБ), ранее обслуживавших только местных клиентов. Предприятия могут формировать сети для производства предметов потребления и услуг, которые позволят им дать более гибкий ответ на изменения спроса.

1. Чтобы улучшить свою конкурентоспособность и усилить деятельность, организации должны демонтировать жесткую иерархическую структуру и работать в сети. Основываясь на взаимном доверии, они могут сократить накладки в деятельности и объединять свое специализированное ноу-хау с развитием производства продукта и процессом покупки, таким образом улучшая свою способность быстро реагировать на изменения в эксплуатационной среде и на изменяющиеся потребности своих клиентов.

2. Предприятия, организации и общественные службы должны совместно продвигать создание сетей в пределах и между различными отраслями. Социальные партнеры должны поддержать своих членов в таком обновлении. Модели экономики сети должны далее развиваться через экспериментирование и исследования. В то же время, необходимо прилагать усилия для исследования путей удаления препятствий по применению моделей действия.

3. Условия, способствующие предпринимательству и деловой организации сети, должны продвигаться с созданием электронного обслуживания и сделок для потребностей ПМСБ. Должны быть приняты меры по продвижению использования информационных сетей как каналов для международного маркетинга.

4. С целью развития спроса и предложения на труд и гибких рабочих методов, организации должны обеспечить полноценное использование возможностей, предлагаемых телекоммуникациями, и стремиться идентифицировать и развивать рабочие места, которые позволяют использовать телекоммуникации. В то же время, должны быть приняты меры по поощрению развития услуг вербовки для телекоммуникационных работ и временных рабочих телекоммуникаций.

В таблице проведено сравнение иерархических и сетевых экономических отношений по таким критериям как: связи, организация, основа взаимодействия, ответственность. Подобный сравнительный анализ позволяет более точно понять, что значит «демонтировать жесткую иерархическую структуру и работать в сети».

Таблица 1 – Сравнение иерархических и сетевых экономических отношений

Критерий сравнения	**Иерархия**	**Сеть**
1. Связи	Вертикальные	Горизонтальные
2. Организация	Сверху	Снизу/самоорганизация
3. Основа взаимодействия	Подчинение	Сотрудничество/доверие
4. Ответственность	Возложенная	Воспринятая

Иерархия использует сетевые отношения в качестве «средств стабилизации». При этом, сетевые структуры способны модифицировать иерархические вертикальные отношения, повышая их гибкость. А при определенных условиях в кризисных ситуациях сети способны заменить собой иерархию и со временем трансформироваться в новую вертикаль. Возникает невидимая сеть поддержки, позволяющая предприятию выжить в кризисных ситуациях.

В условиях сетевой экономики ключевыми факторами экономической безопасности предприятий выступают: степень инновационности бизнес-модели, возможности и скорость адаптации бизнес-модели и стратегии в постоянно меняющихся условиях внутренней и внешней среды, число компетенций и звеньев цепочки ценности, уровень технологического лидерства, использование передовых методов эффективного воздействия на целевой сегмент потребителей для обеспечения роста прибыли, наличие и развитие электронной цепочки, обеспечивающей лидерство за счет дифференциации, по издержкам или на основе оптимальных издержек.

Данные факторы говорят о том, что с одной стороны рост сложности системы сетевых взаимодействий порождает рост количества рисков, а с другой – делает объекты более устойчивыми и мобильными, что положительно отражается на их безопасности. Соответственно, с учетом изменения функционирования предприятия в новых условиях и с ростом количества рисков, показатели оценивающие безопасность и эффективность предприятия немного меняют свое направление и состав. Что касается прежних показателей, то они по-прежнему имеют место.

На сегодняшний день не существует общепринятой в мире и достаточно достоверной методики определения экономической эффективности и безопасности предприятия в условиях сетевой экономики. Можно выделить основные показатели обеспечения экономической безопасности предприятия в условиях сетевого взаимодействия, используя в том числе показатели информационной безопасности.

Разделим показатели на три основные группы:

1) показатели оценки эффективности инвестиционного проекта;

2) показатели оценки стоимости бизнеса;

3) показатели экономического обоснования затрат на информационную безопасность.

К *первой группе* показателей относятся:

- стартовые инвестиции (единовременные, а также, возможно, и распределенные во времени, т. е неоднократные), израсходованные на создание инновационного проекта;
- эксплуатационные расходы, связанные с обеспечением нормального постоянного функционирования предприятия;
- соотношение инвестиционных и эксплуатационных затрат;
- показатели, общепринятые в мире и в России для оценки эффективности инвестиционных проектов или бизнес-проектов (чистая приведенная стоимость, дисконтированный срок окупаемости, внутренняя норма доходности, индекс рентабельности, модифицированная внутренняя норма доходности и др.).
- маркетинговые исследования рынка, реклама, презентации новых товаров и услуг и др.

Вторая группа показателей. С помощью показателей стоимостной оценки бизнеса определяется рыночная стоимость предприятия. Эта стоимость представля-

ет собой наиболее вероятную цену, согласно которой объект оценки может быть продан на открытом рынке в условиях имеющей место конкуренции. Причем стороны действуют разумно и располагают необходимой информацией, а на величине бизнес-сделки не могут отразиться какие-либо чрезвычайные обстоятельства.

Оценка предприятия профессиональными экспертами включает в себя три взаимодополняющие составляющие:

- оценку будущей экономической выгоды (объема прибыли);
- оценку рейтингового места на фондовом рынке компании;
- стоимостную оценку материально-технической и технологической базы.

Показатели *третьей группы* включают в себя совокупные показатели [1]:

- показателя ROI (Return on Investment – отдача от инвестиций) или ROSI (отдача от инвестиций в информационную безопасность) за определенный период времени. Однако, применяя показатель ROI для расчета эффективности вложений в информационную безопасность, следует понимать, что прямого влияния на рост доходов система информационной безопасности не имеет. Поэтому, как правило, не стоит ожидать увеличения выручки компании после инвестиций в сферу информационной защищенности;
- показателя TCO (Total Cost of Ownership – совокупной стоимости владения активов). Показатель TCO определяется как сумма прямых и косвенных затрат, которые несет владелец системы на протяжении всего жизненного цикла эксплуатируемой системы. Как правило, считается, нормальный жизненный цикл составляет в среднем от 3 до 5 лет.
- Payback (окупаемость, период времени, необходимый чтобы доходы, полученные в результате инвестиций, покрыли затраты на эти инвестиции).

Среди прочих TCO является весьма важным критерием, что обусловлено следующим. Во-первых, он дает возможность обосновать расходы на информационную безопасность. Во-вторых, позволяет оперативно решать задачи контроля и коррекции показателей экономической эффективности деятельности службы безопасности, т.к. делает «измеримой» оценку экономической эффективности системы защиты информации.

Немаловажный аспект – при оценке стоимости внедрения какого-либо решения большое внимание уделяется стоимости его приобретения (капитальные затраты), а то, сколько денег позволяет сэкономить его эксплуатация, как правило, остается в тени.

Экономия происходит не только за счет снижения прямых затрат (применения новых технологий и алгоритмов, повышающих производительность и позволяющих получить больших требуемых результатов в единицу времени), но и за счет снижения косвенных издержек (к примеру, электроэнергия, аренда, техническое сопровождение, обучение персонала). Функциональность продукта сильно влияет на второй тип затрат (косвенные затраты).

Параметр TCO, в данном случае, позиционируется как инструмент, позволяющий выбирать лучшее решение из имеющихся аналогичных вариантов.

Однако у показателя TCO есть и недостатки. Например, при выборе из двух проектов, которые оба ведут к снижению издержек, и вопрос какой из них выбрать при прочих равных условиях остается открытым. Поэтому, для полноценного анализа и принятия решения используются все приведенные показатели.

Показатель Payback (окупаемость) характеризует период времени, необходимый чтобы доходы, полученные в результате инвестиций, покрыли затраты на эти самые инвестиции. Иначе говоря, если деньги на проект заемные, то возврат произойдет через срок, который называется payback. Доход от инвестиции должен быть «чистым», поскольку вкладывается конечная и собственная «чистая» сумма денег.

Окупаемость оценивает также и риски невозврата инвестиций – т.е. чем больше период окупаемости, тем больше риски (например, если окупаемость приближается к времени жизни системы - то риски считаются очень большими). Однако, показатель окупаемость тоже не универсален: в целом, он не показывает инвестиционную привлекательность проекта с точки зрения дальнейшего дохода (т.е. после истечения срока окупаемости). Если окупаемость равна одному году, это не означает, что проект через два года и более лет будет приносить доход на том же уровне.

Правильное использование инструментов финансового планирования и параметров оценки эффективности внедряемых проектов позволяют выбрать наиболее оптимальное решение и существенно сэкономить на финансовых затратах компании в информационную безопасность.

В результате анализа показателей специалисты имеют возможность сделать обоснованный выбор в пользу того или иного проекта, а так же прогнозировать перспективы своей деятельности на обозримый срок вперед, что существенно снижает риски и способствует стабильному функционированию предприятия.

Итак, наиболее оптимальным выбором будет тот проект, в котором присутствует комбинация следующих показателей:

1. Наиболее низкий TCO (снижение затрат на содержание проекта системы защиты);
2. Увеличение ROI (процента возврата финансовых вложений в проект);
3. Уменьшение Payback – как можно меньший период, желательно, не больше года, т.к. это позволит обосновать вложения в рамках годового бюджета.

Приведенные выше показатели и методика расчета, безусловно, не являются конечными, существует еще множество дополнительных критериев позволяющих проверить оптимальность принятого решения и определения экономической безопасности предприятия в условиях сетевой экономики.

Список использованной литературы.

1. Планирование затрат на информационную безопасность [Электронный ресурс] / URL: http://www.anti-alware.ru/analytics/Technology_Analysis/economic_planning#part3 (дата обращения: 06.06.2014 г.).