УДК 338.1; 338.2
ГРНТИ 06.75.10; 06.81.12

Обеспечение экономической безопасности хозяйствующего субъекта в условиях угроз враждебного поглощения: анализ внутренней рейдактивности компании

Ш.М. Магомедов
e-mail: *mersedes-benz.88@mail.ru*

Аннотация
Тема. Обеспечение экономической безопасности хозяйствующего субъекта в условиях угроз рейдерского захвата требует стратегических мер противодействия. Любой рейдерский захват начинается с бизнес-разведки потенциального объекта. В процессе разведки агрессору крайне важно получить закрытую информацию, связанную с долгами компании перед кредитными и бюджетными организациями, наличием корпоративных конфликтов и их регулярностью. С финансовой точки зрения, такую информацию дешевле получить, привлекая на свою сторону персонал целевой компании. ***Цели.*** Основная цель исследования – разработка алгоритма противодействия внутренней угрозе поглощения. ***Методология.*** При выполнении исследования применялись методы научного познания: структурный анализ, классификация и агрегирование данных. В качестве методологической основы при разработке алгоритма противодействия внутренней угрозе поглощения использованы методы стратегического управления: swot-анализ, методика сегментации потребителей, анализ «слепых зон» при принятии управленческих решений. ***Результаты.*** Дано определение понятию «рейдпригодность сотрудников», проанализированы основные критерии рейдпригодности. Выделены ключевые параметры, на основе которых предлагается сегментировать персонал хозяйствующего субъекта. Представлен пример использования swot-анализа, в результате которого хозяйствующий субъект сможет понять, какие сегменты сотрудников представляют наибольшую опасность для компании. Предложены различные виды мероприятий по снижению внутреннего риска угрозы поглощения в зависимости от категории сотрудников. ***Выводы.*** Отсутствие профилактических мероприятий, направленных на выявление критериев рейдпригодности сотрудников создают реальные угрозы корпоративного захвата компании. *Р*аспространение недружественных поглощений в России вынуждает многие компании изменять первоначальную стратегию. ***Применение.*** Предлагаемый в работе алгоритм, в значительной степени, позволит повысить уровень экономической безопасности хозяйствующего субъекта, в том числе от угроз недружественного поглощения.

Ключевые слова: *стратегическое управление, угроза поглощения, защита бизнеса, недружественное поглощение, хозяйствующий субъект, swot-анализ*

Введение

Возможность выживания в условиях распространения недружественных поглощений в России дает долгосрочное планирование развития компании на несколько лет вперед. Такое планирование должно осуществляться в рамках стратегического менеджмента. **Стратегический менеджмент (управление)** – это процесс, заключающийся в регулярном планировании, контроле, анализе внешней и внутренней среды компании.

В современных условиях непросто одновременно обеспечить коммерческий успех организации и ее безопасность. Чем более успешным является бизнес, тем более он уязвим, подвержен ряду угроз, в том числе попыткам рейдерских захватов [3, с. 42].

Основная часть

Стратегический анализ внутренней среды компании – это количественная и качественная оценка внутренних ресурсов и возможностей компании, направленная на решение стратегических проблем развития [9, с. 24]. В целях снижения активности сотрудников компании в пособничестве рейдерским действиям предлагается проведение анализа внутренней рейдактивности. **Внутренняя рейдактивность** – это внутренний риск угрозы поглощения, который зависит от степени участия в рейдерском захвате действующих или бывших сотрудников, а также от принимаемых решений собственниками хозяйствующего субъекта.

Актуальность проведения подобного анализа подтверждается практическим опытом. Дело в том, что многие недружественные поглощения осуществляются с участием сотрудников целевой компании. Внутренние угрозы напрямую связаны с человеческим фактором и представляют наибольшую опасность для организаций [8, с. 14]. Разумеется, шансы атакующей стороны по получению корпоративного контроля значительно возрастут, если сотрудники компании-цели находятся в сговоре с рейдером. Это сильно облегчает процесс недружественного поглощения, так как действующие сотрудники хорошо осведомлены об уязвимых местах компании, особенно топ-менеджмент.

Таким образом, автор исследования предлагает следующий алгоритм противодействия внутренней угрозе поглощения хозяйствующего субъекта (рис. 1).

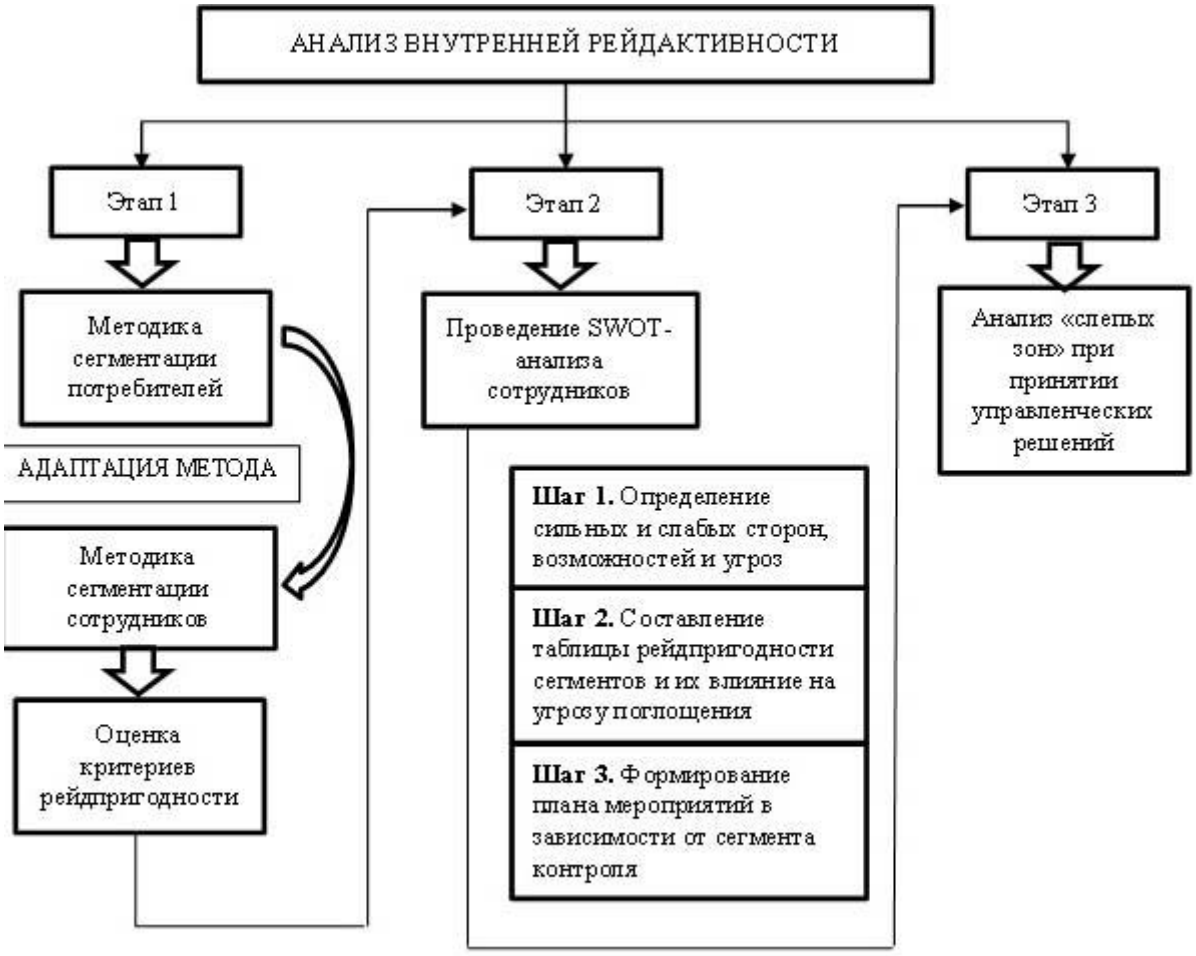

Рис. 1. Алгоритм проведения анализа внутренней рейдактивности

Критерии рейдпригодности

В стратегическом управлении можно встретить такой метод как **методика сегментации потребителей (рыночная сегментация)**, направленная на анализ целевой аудитории компании. Главная цель сегментации – сделать продаваемые товары или услуги компании более конкурентоспособными, дифференцируя потребительский (рыночный) сегмент на однородные группы. Как правильно отмечают Пашков Р. и Юденков Ю., сегментация рынка – это процесс разделения рынка на отдельные группы потребителей (покупателей), для которых могут потребоваться отдельные товары и (или) комплексы маркетинга по какому-либо критерию (признаку) [5, с. 36]. То есть, сегментация позволяет понять особенности и интересы потенциальных потребителей.

Оценивая потенциальную возможность поглощения как угрозу экономической безопасности, подобную методику можно использовать по отношению к персоналу организации, предварительно переименовав ее в **«методику сегментации сотрудников».** Методика будет

направлена на оценку определенных **критериев рейдпригодности**, благодаря чему, персонал компании можно классифицировать на однотипные группы, по которым будут разрабатываться соответствующие планы мероприятий, предупреждающих риск недружественного поглощения. **Рейдпригодность сотрудников** – это интерес компании-агрессора по отношению к сотрудникам целевой компании, их уровню доступа и возможностей для предоставления необходимой информации, либо принятия решений, выгодных рейдеру в целях осуществления недружественного поглощения. Для более качественной оценки предлагается анализировать следующие критерии рейдпригодности:

1) Объем предоставленного доступа к коммерческой информации, в том числе с использованием информационных ресурсов организации. Большая ответственность здесь ложится на службу информационной безопасности, которой необходимо на регулярной основе отслеживать нарушения, связанные с утечкой и разглашением коммерческой информации. С целью снижения рисков, связанных с недобросовестными действиями работников, с ними следует подписать соглашение о коммерческой тайне, прежде регламентировав, что к ней относится и каков порядок ее защиты [2, с.79].

В последнее время во многих компаниях участились случаи, связанные с продажей или передачей клиентских баз третьей стороне, в результате чего наносится серьезный финансовый ущерб из-за оттока потенциальных клиентов. Особенно это актуально для небольших компаний, где отсутствует должный контроль со стороны внутренних подразделений.

2) Объем принадлежащих голосующих акций (долей). Службу экономической безопасности должно насторожить, если один из миноритарных акционеров проявляет активную оппозицию по отношению к собственникам хозяйствующего субъекта (преднамеренно затягивает процесс принятия оперативных решений, подает иски о нарушении прав миноритарных акционеров, проявляет иные признаки «гринмейла»). Неожиданное проявление повышенного интереса миноритарного акционера к некоторым аспектам финансово-хозяйственной деятельности предприятия, особенно с попытками получения всевозможных правоустанавливающих документов, следует рассматривать как признак угрозы поглощения.

Так конфликт между основным акционером «Амстора» компанией Смарт-Холдинг (70%) и миноритарным акционером (15%) обусловлен желанием последнего отстранить мажоритарного акционера от участия в бизнесе «Амстора»[1]. Стратегической ошибкой мажоритарного акционера явилось то, что тот позволил своему партнеру, несмотря на небольшую долю, оставаться фактическим владельцем торговой сети.

3) Список ущемленных или «обиженных» сотрудников, в том числе бывших. Составить такой список не помешает любой организации, учитывая, что многие рейдерские захваты, осуществляются с участием внутренних противников компании. В такой список будут входить сотрудники, не лояльно исполняющие свои должностные полномочия, регулярно оставляющие жалобы на свое руководство. Данный список пополнят бывшие сотрудники, особенно те, которые не получили обещанных мотивационных выплат, выходного пособия.

Рейдеру, в поисках уязвимых мест рассматриваемой компании-цели, достаточно легко найти недовольных сотрудников. Их можно обнаружить в социальных сетях, на различных интернет-форумах, где они оставляют негативные отзывы по отношению к компании. По сути, рейдер проводит что-то вроде интернет-разведки и, в дальнейшем, формирует для подобного сотрудника персональное предложение, заручаясь, таким образом, внутренней поддержкой. К примеру, рейдерская компания может обратиться к одному из популярных, на текущий момент, Интернет-ресурсов https://antijob.net/, где сформирован список «черных» работодателей. Не сложно догадаться, что наличие интересующей компании в списке таких работодателей позволит использовать данный информационный ресурс в рейдерских целях. По данным анонимного опроса «Альфастрахования», в котором участвовали сотрудники 100 российских компаний с оборотом от 100 млн. руб., о желании отомстить бывшему работодателю заявило три четверти опрашиваемых [12].

[1] История торговой сети «Амстор», или кто он – мистер Вагоровский? // dsnews.ua [Электронный ресурс]. URL: http://www.dsnews.ua/economics/istoriya-torgovoy-seti-amstor-ili-kto-on-mister-vagorovskiy--02092015091100 (дата обращения: 20.02.2018)

Таким образом, при увольнении сотрудника, особенно по инициативе работодателя, нужно обратить повышенное внимание на возможные попытки отправки коммерческой информации или порочащие письма о компании на внешние электронные адреса, невозврат пропуска, с помощью которого сотрудник получал доступ к помещению. Первым шагом обеспечения безопасности компании будет немедленное закрытие доступа к корпоративной почте, отзыв полномочий ко всем предоставленным ранее информационным ресурсам, а также прочие организационные меры. Такие простые своевременные процедуры позволят минимизировать распространение негативной информации о хозяйствующем субъекте.

Особенно рейдпригодными будут являться сотрудники, владеющие некоторым количеством акций компании, поэтому при увольнении следует предусмотреть возможность их продажи хозяйствующему субъекту.

4) Наличие негативной или компрометирующей информации. Любая негативная информация, которую скрывают сотрудники или топ-менеджеры, может быть использована агрессором в форме вымогательства интересующих данных или принятии «нужных» управленческих решений.

5) Наличие финансовых проблем (высокая кредитная нагрузка, прочие долги). По большей части, мотив получения материального вознаграждения стимулирует сотрудника в пособничестве рейдерским действиям.

Итак, чтобы детально изучить характерные черты своих сотрудников, после оценки указанных критериев следует сегментировать их по ключевым параметрам, к примеру, наличию голосующих акций (долей) в хозяйствующем субъекте и уровню доступа к конфиденциальной информации. Выделим четыре сегмента сотрудников (табл. 1).

Таблица 1

Сегментирование персонала хозяйствующего субъекта

Номер сегмента	Объем принадлежащих акций (долей)	Уровень доступа к конфиденциальной информации
Сегмент №1	Отсутствие акций (долей)	Отсутствие доступа
Сегмент №2	Отсутствие акций (долей)	Средний уровень доступа
Сегмент №3	Незначительный объем акций (долей)	Высокий уровень доступа
Сегмент №4	Значительный объем акций (долей)	Полный уровень доступа

Проведение SWOT-анализа сотрудников

Итак, мы сегментировали сотрудников. Теперь попробуем провести SWOT-анализ, целью которого будет выступать оценка необходимых ресурсов для качественного анализа выделенных сегментов (сильные и слабые стороны), а также оценка потенциальных выгод для хозяйствующего субъекта проведения такой оценки (возможности) и возможных угроз, которые могут возникнуть в результате игнорирования анализа (угрозы). Главное удобство SWOT-анализ в том, что это универсальная методика стратегического управления, которую можно применять не только к компании в целом, но и к определенному проекту, отделу, продукту, даже к отдельным категориям сотрудников.

По результатам SWOT-анализа хозяйствующий субъект сможет понять, какие из указанных сегментов представляют наибольшую опасность для организации и, на основе анализа, составить план мероприятий для снижения внутренней рейдактивности.

На первом шаге опишем сильные и слабые стороны (S-Strengths and W-Weaknesses) по указанным сегментам. Здесь важно учитывать наличие или нехватку необходимых технических и финансовых ресурсов в компании. Такими ресурсами являются присутствие в компании управления по информационной безопасности, службы экономической безопасности, экспертов в области M&A, а также финансовые возможности по привлечению указанных специалистов в штат хозяйствующего субъекта.

В качестве потенциальных возможностей (O-Opportunities) можно выделить повышение уверенности и лояльности коллектива по отношении к компании, снижение частоты увольнения топ-менеджмента и ключевых сотрудников, получение новых знаний и практического опыта, пользующихся высоким спросом в российской бизнес-среде. В условиях риска рейдерского захвата важно понимать, что своевременно предотвращенная угроза становится возможностью для хозяйствующего субъекта.

Рассматривая потенциальные угрозы (**T-Threats**) особенное внимание следует уделить уже произошедшим событиям в компании, к примеру, отправки конфиденциальной информации на внешнюю почту, появление внутренних разногласий руководителей в отобранных сегментах.

Если взять сравнительно небольшую компанию, то SWOT-анализ по указанным сегментам будет выглядеть примерно следующим образом (рис. 2).

S (STRENGTHS) • Наличие службы экономической и информационной безопасности; • Наличие юридического департамента; • Оперативность принятия управленческих решений; • Наличие камер видеонаблюдения и прослушиваемых телефонных аппаратов; • Возможность привлечения инвестиционного или заемного капитала для проведения комплексной проверки сотрудников;	**W (WEAKNESSES)** • Отсутствие в компании специалистов в области M&A; • Отсутствие системы мотивации ключевых сотрудников и топ-менеджмента; • Отсутствие собственных финансовых возможностей по проведению качественной проверке сотрудников; • Отсутствие необходимых технологий по проверке сотрудников (наличие полиграфа, доступ к коммерческих ресурсам базам ГИБДД, НБКИ);
O (OPPORTUNITIES) • Повышение уверенности и лояльности коллектива по отношению к компании и его руководству, улучшение внутреннего корпоративного климата; • Снижение частоты увольнения топ-менеджмента и ключевых сотрудников; • Повышение квалификации персонала и надежности компании; • Снижение риска деловой репутации;	**T (THREATS)** • Повышение рисков утечки (разглашения) конфиденциальной информации; • Снижение возможностей компании по предотвращению скрытых корпоративных конфликтов; • Увеличение финансовых потерь в результате неправомерных действий сотрудников, находящихся в сговоре с атакующей стороной; • Рост степени угрозы поглощения;

Рис. 2. Применение SWOT-анализа к выделенным сегментам

Отметим, что создание отдельного подразделения экономической безопасности целесообразно на крупных предприятиях. Однако деятельность средних и малых предприятий также не лишена рисков, поэтому на различных специалистов могут возлагаться функции обеспечения экономической безопасности [11, с. 53].

Обратим внимание, что применение SWOT-анализа в текущем варианте имеет некоторые особенности. Дело в том, что такие элементы как «угрозы и возможности», в классическом варианте, рассматриваются в качестве факторов внешней среды, а элементы «сильные и слабые стороны» в качестве факторов внутренней среды. В нашем же примере все элементы рассматриваются как факторы внутренней среды, поскольку объектом выступает персонал хозяйствующего субъекта.

На втором шаге составим таблицу рейдпригодности сотрудников по выделенным сегментам (табл. 2).

Содействие таких сотрудников компании-агрессору, особенно третьего и четвертого сегмента, значительно увеличивает возможность поглощения как угрозу экономической безопасности компании, поскольку выход на таких сотрудников позволяет компании-агрессору сформировать эффективную стратегию захвата с учетом внутренних особенностей хозяйствующего субъекта. Подконтрольные рейдеру сегменты №3 или №4 наверняка будут иметь возможность получения доступа к таким правоустанавливающим документам как реестр акционеров, договоры купли-продажи недвижимости. Используя принадлежащий объем акций (долей) указан-

ных сегментов рейдер несомненно попробует провести в совет директоров своих кандидатов, получить доступ к коммерческой и иной закрытой информации, касающихся, в том числе, и деловых связей собственников компании-цели, их возможной аффилированности с органами власти. Кто-либо из топ-менеджеров может перейти на сторону захватчика, к примеру, после серьезного корпоративного конфликта, в ходе которого были затронуты его личные и финансовые интересы. Конфликтная ситуация, сама по себе, представляет большой интерес для компании-захватчика, когда между вчерашними партнерами появились существенные разногласия. В этом случае партнер, располагающий меньшими ресурсами, опасаясь проигрыша и полной потери своей части бизнеса или актива, может сам инициировать недружественное поглощение, обратившись к компании-захватчику.

Таблица 2

Степень рейдпригодности сегментов и их влияние на угрозу поглощения хозяйствующего субъекта

Номер сегмента	Степень рейдпригодности	Угроза поглощения
Сегмент №1,2	Данные сегменты не представляет столь значительного интереса для агрессора. Обычно таких сотрудников используют для получения негативной информации, позволяющей в дальнейшем оказывать давление на собственника	Незначительная
Сегмент №3	Данная категория сотрудников вызывает высокий интерес для компании-агрессора, однако для осуществления захвата понадобятся значительные финансовые ресурсы	Средняя
Сегмент №4	Данная категория сотрудников вызывает повышенный интерес для компании-агрессора, поскольку получение контроля хотя бы над несколькими сотрудниками указанного сегмента способно полностью парализовать деятельность предприятия и, таким образом, осуществить рейдерский захват с наименьшими затратами	Высокая

Так, к огромным последствиям привел корпоративный спор в середине 2004 года между владельцами и топ-менеджером ОАО Уралинвестэнерго (УИЭ), когда акционеры принимают решение разорвать контракт с генеральным директором. Затем гендиректор, утверждая, что он является единоличным владельцем УИЭ, обращается за помощью к стратегическому инвестору, а именно к Уральской горно-металлургической компании (УГМК), которая обладает серьезным «административным ресурсом». В обмен на помощь, бывший гендиректор передает свои акции УГМК и сам переходит туда на работу. Используя ресурсы УГМК, гендиректор подает многочисленные иски, в результате которых было заведено множество уголовных дел по отношению к текущему руководству УИЭ. В итоге, некоторые руководители были арестованы, а кто-то объявлен в международный розыск[2].

На третьем, последнем шаге SWOT-анализа сформируем конкретные предложения для снижения внутреннего риска угрозы поглощения в рамках указанных сегментов (рис. 3).

Активное участие в разработке плана мероприятий должны принимать служба экономической и информационной безопасности. Так, для каждого сегмента предлагается использовать различные виды мероприятий.

Базовые мероприятия – стандартная проверка, связанная с изучением общих сведений о сотрудниках и реализация соответствующих защитных мер. Здесь изучаются такие параметры как факты привлечения к уголовной и административной ответственности, виды принадлежащей недвижимости (квартира, дача, земельный участок), наличие финансовых проблем (высокая кредитная нагрузка, наличие неуплаченных штрафов, алиментов), уровень доходов, получаемый на последних местах работ. Как видно на рисунке 3, базовые мероприятия предлагается применять к сегменту №1 и №2.

[2] Из-за топ-менеджеров "Уралинвестэнерго", попросивших убежища в Украине, ругаются МВД двух стран // Компромат.ru [Электронный ресурс]. URL: http://www.compromat.ru/page_21748.htm (дата обращения: 01.03.2018)

Полагаем, что эффективным способом выявления признаков рейдерского захвата со стороны внутреннего рядового персонала будет введение в хозяйствующий субъект обязательного дистанционного курса со следующим названием «Признаки угрозы поглощения компании». В данном курсе необходимо описать:

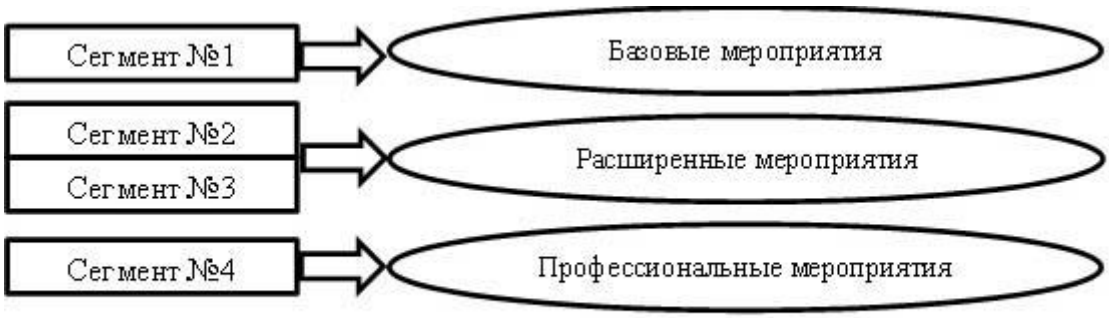

Рис. 3. План мероприятий в зависимости от сегмента контроля

1. Действия сотрудников, способные создать предпосылки или реальные угрозы для поглощения хозяйствующего субъекта.

2. Предпринимаемые меры в случае обнаружения сотрудником подозрительных действий своих коллег и руководства. В данной ситуации сотруднику следует незамедлительно сообщить в службу экономической безопасности о выявленных фактах, анонимность должна при этом гарантироваться.

3. Предусмотреть материальную ответственность за совершение действий, создающие предпосылки угрозы поглощения, а также за сокрытие такой информации.

Материал курса должен составляться на основе опыта многих компаний с указанием часто встречаемых практических кейсов. На завершающем этапе сотрудник проходит электронное тестирование, что будет свидетельствовать об усвоении пройденного материала.

Еще одним действенным методом противодействия внутренней угрозе поглощения является материальное вознаграждение сотрудникам, обнаружившим факты соучастия своих коллег в рейдерских действиях.

Расширенные мероприятия – расширенная проверка по установлению профессиональной репутации сотрудника: его деловых и личных качеств, а также составления плана превентивных мероприятий. Считаем, что в условиях повышенного риска угрозы поглощения необходимо расширение полномочий службы экономической и информационной безопасности с включением в их функционал некоторых разведывательных функций, чтобы они могли проводить комплексную проверку сотрудников. Сюда могут входить, интернет-активность сотрудника (к примеру, в каких социальных сетях зарегистрирован, регулярность их посещения, наличие собственного блога, степень распространения рабочей информации), проверка реальных причин ухода с предыдущих мест работ путем запроса рекомендаций, наличие долгов перед родственниками, друзьями, третьими лицами.

Можно прийти к выводу, что противостоять угрозам рейдерских захватов потенциально способны лишь те компании, которые имеют в составе своей организационной структуры эффективную службу безопасности, на которую возложена функция по противодействию рейдерским захватам. Именно они, как правило, выявляют каналы утечки информации, проводят комплексную проверку персонала, а также осуществляют сбор и анализ информации о внешних и внутренних угрозах предприятия [3, с. 44].

Профессиональные мероприятия – разработка превентивных мер защиты путем глубокого изучения биографии топ-менеджеров, их размеров бизнеса, ближайшего круга деловых партнеров. Предметом изучения станут следующие параметры:

1. Инициирование корпоративных конфликтов и их основные причины.

2. Степень аффилированности с собственниками компании, а также компаниями-конкурентами.

3. Психологический портрет личности с указанием сильных и слабых сторон.

4. Проверка образа жизни (азартные игры, часто посещаемые места).

5. Компромат и негативная информация в интернете, по линиям родственников, из других возможных источников.

Если по результатам анализа выяснится, что один из топ-менеджеров соответствует некоторым указанным параметрам, то можно ограничить его полномочия по сделкам, которые оказывают серьезное влияние на деятельность компании. Данный способ часто применяется в практике акционерного общества в отношении генеральных директоров. Как предлагает Оськина И. и Лупу А., в устав общества, к примеру, можно ввести запрет на совершение без одобрения совета директоров не только крупных, но и вообще любых сделок с недвижимостью [4, с. 13].

Профессиональные мероприятия, как правило, осуществляются с привлечением специализированных организаций: детективных агентств, консалтинговых фирм, антирейдерских компаний, имеющих специалистов в области M&A. Однако если речь идет о крупной финансово-промышленной группе, где имеются собственные службы экономической и информационной безопасности, разведывательные мероприятия по общему правилу находятся в компетенции таких подразделений.

При наличии весомых подозрений в аффилированности топ-менеджеров с рейдерами, в некоторых случаях оправдывают себя даже такие методы, как персональная слежка, что позволит понять склонности и привычки топ-менеджмента, а также возможные рычаги давления со стороны компании-агрессора.

«Слепые зоны» при принятии стратегических решений

Отметим, что знание и опыт работы собственников, и топ-менеджмента является одним из ключевых элементов при создании эффективного защитного механизма. Стратегия современного бизнеса предусматривает наличие эффективной системы корпоративного управления, а также нового креативного мышления топ-менеджмента [7, с. 25]. Однако при принятии управленческих решений существуют определенные **«слепые зоны»**, которые снижают эффективность стратегического менеджмента. Так, слепая зона «неправильные предположения» имеет место, когда многие стратегические и тактические решения принимаются на основе предположений, не имеющих тщательного анализа. Слепая зона «самоуверенность», включает в себя недооценку риска, что может привести к негативным последствиям. Существует множество «слепых зон», все зависит от личности и конкретных характеристик собственника компании.

Особенно отчетливо **«слепые зоны»** прослеживаются при рейдерских захватах. Для некоторых собственников иногда становится неожиданностью узнать, что их компания стала объектом рейдерских действий. Это становится возможным благодаря незнанию и ошибочным предположениям собственников компании.

В данном контексте хорошо привести некоторые заблуждения руководителей, описанные в книге «Антирейдер», которые сформировались в российской действительности. Так, В. Поляков и И. Туник выделяют следующие заблуждения («слепые зоны») [6, с. 11]:

1) **Мое предприятие не может заинтересовать рейдеров** является часто встречающимся заблуждением среди российских бизнесменов. Это проявляется в незнании собственником реальной рыночной стоимости компании, привлекательности ее основных активов, а также мотивов и способов рейдерского захвата.

2) **Мое предприятие находится под защитой государства и закона**. Возможно, за рубежом данное утверждение является более справедливым, где процессы слияний и поглощений не имеют явно криминального оттенка и, как правило, пресекаются на законодательном уровне. В подобной ситуации простое следование российского предпринимателя зарубежным принципам ведения бизнеса, неизбежно приведет его в тупиковую ситуацию.

3) **Финансирование и реализация защитных мер – это разовая процедура**. Некоторые собственники ошибочно полагают, что проведение превентивных мероприятий по защите хозяйствующего субъекта проводится только один раз, то есть данный процесс не требует регулярного контроля. В условиях недобросовестной конкуренции, компаниям часто приходится пересматривать свои стратегии, чтобы не стать жертвами рейдерских действий.

4) **«Это же неэтично»**. Многие руководители морально не готовы противостоять «черному» рейдерству, полагая, что корпоративный захват будет строиться на неких законных обычаях делового оборота.

Заключение

Чтобы избежать ошибочных предубеждений, руководителям следует принимать стратегические решения коллективно, используя не только собственный опыт, но и привлекая к проблеме специалистов.

Если в компании отсутствует четко сформулированная стратегия по противодействию внутренним угрозам поглощений, то ее финансово-хозяйственная деятельность всегда будет подвержена высокому риску корпоративного захвата. Кроме того, действия различных подразделений, при отсутствии единой стратегии, не будут согласованы при принятии стратегических решений. Таким образом, качество стратегического управления зависит от эффективно составленной стратегии, которая должна учитывает специфику деятельности компании [10, с. 19].

В текущих условиях сложно придерживаться какой-то одной стратегии, к примеру, стратегии резкого роста. Распространение недружественных поглощений и вовлечение представителей органов власти в данные процессы вынуждают многие хозяйствующие субъекты изменять первоначальную стратегию. Как правило, компании прибегают к стратегии сокращения (выживания), которая характеризуемая режимом экономии ресурсов, уменьшением объемов производства, сокращением персонала и снижением оплаты труда [1, с. 6]. Это связано с появлением новых непредвиденных факторов, которые не учитывались в ранее принятой концепции стратегии. Указанные факторы могут открыть перед хозяйствующим субъектом как новые возможности для дальнейшего роста, так и потенциальные угрозы, ограничивающие деятельность компании.

К сожалению, для российских предпринимателей характерен низкий уровень предпринимательской культуры. Возможность получения «быстрых» денег практически не учитывает долгосрочную перспективу бизнеса, и многие начинающие компании, не задумываясь о защите своих активов, сталкиваются с угрозой поглощения.

Литература

1. Васильева И.Е. Особенности разработки стратегии по управлению имущественными комплексами предприятий // Управление собственностью: теория и практика. – 2016. – № 2. – С. 2 - 6.

2. Елин С. Как предпринимателю обеспечить безопасность бизнеса // Арсенал предпринимателя. - 2013. - № 6. - С. 78-84.

3. Мохов А.А. Роль служб безопасности организаций в противодействии рейдерским захватам // Юрист. – 2015. – № 21. – С. 42-46.

4. Оськина И., Лупу А. Подконтрольный гендиректор. Как акционерам ограничить полномочия генерального директора? // Акционерный вестник. - 2011. - № 10 (88). - С. 13-17.

5. Пашков Р., Юденков Ю. Сегментация клиентской базы как элемент стратегии развития банка // Бухгалтерия и банки. - 2016. - № 6. - С. 36-40.

6. Поляков В., Туник И. Антирейдер. Пособие по противодействию корпоративным захватам. – СПб.: Питер Пресс, 2007. - 147 с.

7. Рыбалко О.А., Шалаева Л.В. Стратегическое планирование и бюджетирование как базовые элементы современной системы управления // Международный бухгалтерский учет. - 2012. - № 28. - С. 25-38.

8. Северин В.А. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере // Информационное право. - 2016. - № 4. - С. 13-19.

9. Сидоров М.Н. Стратегический менеджмент: учебник для прикладного бакалавриата. – 2-е изд. - М.: Издательство "Юрайт", 2016. - 146 с.

10. Тысячникова Н.А. Организация процесса стратегического планирования // Управление в кредитной организации. - 2013. - № 1. - С. 15-28.

11. Шигун М.М. Субъекты внутреннего контроля в системе экономической безопасности предприятия // Международный бухгалтерский учет. - 2014. - № 32. - С. 52-62.

12. Как работодателям мстят обиженные сотрудники // Электронная газета «Ведомости». [Электронный ресурс]. URL: https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki (дата обращения: 05.03.2018).

Ensuring the economic security of an economic entity in the face of threats of hostile takeover: an analysis of the internal raidactivity of the company

Shamil M. Magomedov
e-mail: *mersedes-benz.88@mail.ru*

Abstract

Topic. Ensuring economic security of an economic entity in the face of threats of raider seizure requires strategic countermeasures. Any raider seizure begins with a business intelligence of a potential company. During business intelligence, it is very important for the raider company to obtain confidential information related to the company's debts to credit and budget organizations, the presence of corporate conflicts and their regularity. From a financial point of view, this information is cheaper to get, attracting the target company's staff. ***Objectives.*** The main goal of the study is to develop an algorithm to counter the internal threat of absorption with the use of strategic management methods. ***Methodology.*** When performing studies used such methods of scientific knowledge as structural analysis, classification and aggregation of data. As a methodological basis for developing an algorithm for countering the internal threat of absorption, the author used methods of strategic management: swot analysis, method of consumer segmentation, and analysis of "blind zones" in making managerial decisions. ***Results.*** The definition of the concept of "raid-fit of employees" is given, the main criteria of raid-fit are analyzed. The key parameters are selected, on the basis of which it is proposed to segment the personnel of the business entity. An example of using swot analysis is presented, as a result of which the business entity will be able to understand which segments of personnel pose the greatest danger to the company. Various types of measures have been proposed to reduce the internal risk of the threat of takeover depending on the category of personnel. ***Conclusions.*** The absence in the business entity of preventive measures aimed at identifying the criteria of "raid-fit of employees" is creating real threats of corporate capture of the company. It is concluded that the spread of unfriendly takeovers leads many companies to change the initial strategy in Russia. ***Application.*** The algorithm, proposed in the study, in large part, will increase the level of economic security of the business entity, including against threats of hostile takeover.

Keywords: *strategic management, threat of absorption, protection of business, unfriendly takeover, business entity, swot-analysis*

Об авторе

Магомедов Шамиль Магомедович, главный специалист, Публичное акционерное общество «Промсвязьбанк», Москва.

About author

Shamil M. Magomedov, Chief Specialist, Public joint-stock company «Promsvyazbank», Moscow.