тивнее распределить ресурсы и скорректировать инвестиционную политику на кратко- и долгосрочной перспективе. Кроме того, точное значение стоимости бренда очень важно в случае предложение о покупке компании. Это поможет акционерам и покупателю четко определить, является ли это предложение правильным или нет, необходимо ли увеличение цены, ее уменьшение или отказ от предложенной цены. Наконец, стоимость бренда используется для получения финансирования [5].

Список литературы

1. Кевин Дробо «Секреты сильного бренда: как добиться коммерческой уникальности», 2005.
2. Жукова Н.Ю., Матасов Г.М. Как оценить стоимость бренда: модификация модели, 2010.
3. Aaker D. Managing Brand Equity // Free Press. 2009.
4. Просвирина. И. Стоимость бренда: взгляд финансиста // Деловой журнал «Бизнес-Ключ», № 5 за 2007 год.
5. Алешина С. Неоценимая ценность // Секрет фирмы. – 01.11.2004.

ПРОБЛЕМА ОЦЕНКИ УРОВНЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ СЛИЯНИЯХ, ПОГЛОЩЕНИЯХ

Даниловских А.А, Кузьмичева И.А.

Владивостокский государственный университет экономики и сервиса, Владивосток, e-mail: danilovskikh75@mail.ru

Усиление конкуренции в современном бизнесе вынуждает компании искать все новые способы расширения. Проведение слияний (поглощений) с компаниями, у которых есть требуемый ресурс (активы, технологии, клиенты и т.п.) позволяет не только увеличить масштабы деятельности компании, но и получить дополнительно синергетический эффект. Обычно слияния и поглощения определяют как процедуру смены собственника или изменения структуры собственности компании.

В литературе представлена достаточно широкая классификация видов слияний и поглощений. Сущность понятий «слияние» и «поглощение» наиболее полно отражает классификация по критерию зависимости от отношения управленческого персонала к сделке. Так, выделяют дружественные и враждебные слияния, причем чаще всего «слияние» рассматривается в контексте «дружественного», а «поглощение» – «враждебного» объединения.

Основной целью слияний и поглощений называют получение синергетического эффекта, то есть ситуаций, в которых эффективность совместного использования активов двух компаний выше суммарной эффективности их использования по отдельности, а капитализированная стоимость вновь образованной компании превосходит сумму стоимостей компаний, участвовавших в слиянии [3].

Синергия возникает благодаря следующим факторам:

– операционная экономия, возникающая в результате возрастающей отдачи от масштаба управления, маркетинга, производства или распределения;

– финансовая экономия, проявляющаяся в снижении транзакционных затрат и лучшей подготовке контрактов;

– дифференцированная эффективность, означающая, что активы одной из фирм могут использоваться совместно с большей эффективностью;

– снижение конкурентных угроз и получение компанией большей рыночной власти;

– результаты обследований свидетельствуют, что слияния и поглощения во многих случаях открывают путь к повышению эффективности хозяйственных операций [3].

Сделки по слиянию/поглощению являются достаточно сложными с точки зрения управления, кроме того, особое внимание необходимо уделять вопросам экономической и информационной безопасности компании. Безопасность особенно важна, если речь идет о высокотехнологичных компаниях, в которых самое ценное (после людей) – интеллектуальная собственность, ноу-хау и т.д. [3]. Но и для любой другой компании это не менее актуально, ведь недовольные сделкой или уволенные работники компании могут разгласить конфиденциальную информацию. Сделка может не принести планируемого результата, если вопросам информационной безопасности не было уделено достаточно внимания.

В процессе подготовки сделки по слиянию/поглощению обязательно проводится процедура *due diligence* (англ. due diligence – должная добросовестность, сокращённо используют аббревиатуру DueD, DDG), то есть производственный, финансовый и юридический аудит приобретаемой/поглощаемой компании, который позволяет сформировать полное объективное представление об объекте инвестирования. В работе на данном этапе участвуют, в том числе, независимые оценщики, задача которых определить ориентировочную стоимость компании-мишени. В настоящее время разработан ряд методик оценки стоимости интегрированного бизнеса, человеческого капитала, нематериальных активов [2, 4]. Однако, как отмечают специалисты, при оценке поглощаемых активов крайне редко проводится оценка уровня автоматизации бизнес-процессов и обеспечения информационной безопасности. При покупке того или иного актива российскими инвесторами в большинстве случаев в первую очередь приобретается материальная составляющая (земля, здания, производственные фонды) и только потом бизнес как выстроенный процесс. В этих условиях риски информационной безопасности при оценке имущества практически не учитываются [5].

При подготовке сделки слияния/поглощения необходимо объединить стратегии информационной безопасности обоих компаний, доработав и модифицировав их. В плане развития информационных технологий объединенной компании, возможны различные варианты: 1) объединившиеся компании сразу переходят на одну общую систему и объединяют свои базы, для этого чаще используется система, уже имеющаяся в одной из компаний; 2) объединившиеся компании продолжают работать на собственных системах, а для синхронизации данных между ними разрабатываются дополнительные «мосты» и модули обмена данными. [5]

Выделяют следующие типичные проблемы обеспечения информационной безопасности при интеграции приобретённых компаний:

– различные уровни зрелости технологических процессов и информационной безопасности у приобретённой и головной компаний;

– различные подходы к обеспечению информационной безопасности;

– появление элементов корпоративной инфраструктуры с разным уровнем доверия;

– отсутствие единого уровня информационной безопасности в рамках всей компании;

– разная корпоративная культура, на уровне обработки и защиты данных.

Объединенное предприятие должно иметь общую монолитную информационную систему – только она позволит получить прозрачную отчетность и сократить издержки за счет выстраивания единых процессов. После заключения сделок и решения фи-

нансовых, юридических и кадровых вопросов перед управляющей компанией встает вопрос интеграции информационных систем объединенных активов. У объединяющихся компаний, как правило, разные стандарты обслуживания, методологии управления и т.д. Существенной проблемой также является наличие в большинстве компаний продуктов собственной либо частной разработки без должной поддержки со стороны разработчика. Зачастую – это совершенно независимые системы от разных разработчиков, функционирующие на различных аппаратных и программных платформах, плохо документированные или недокументированные вовсе. При объединении нескольких компаний ситуация разнородности информационных систем только усугубляется. Обеим сторонам приходится проводить огромную организационную работу, объединять очень большие объемы накопленных данных, унифицировать справочники, переводить разрозненные программы на единую платформу [1].

Таким образом, достижение планируемых в результате сделки по слиянию/поглощению результатов, во многом зависит как от первоначальной оценки уровня обеспечения информационной безопасности компании-мишени, так и от проведенных в дальнейшем работ по обеспечению информационной безопасности интегрированной компании.

Список литературы

1. Время идет, проблемы интеграции ИТ при M&A остаются // Электронный ресурс, режим доступа: http://www.asteros.ru/press/press/2063/

2. Кузьмичева И.А., Флик Е.Г. Становление оценки и оценочной деятельности в мире и в России // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2012. – № 2. – С. 119-123.

3. Куницкий А. Механизм слияний и поглощений как инструмент обеспечения экономической безопасности предприятий в период экономического кризиса // Электронный ресурс, режим доступа: http://pandia.org/text/78/031/12127.php.

4. Сакеян А.Г., Даниловских Т.Е. Определение сущности человеческого капитала в целях его оценки // Международный журнал прикладных и фундаментальных исследований. – 2015. – № 1-1. – С. 113-116.

5. Седов О. Информационная безопасность при слияниях и поглощениях // электронный ресурс, режим доступа: http://www.osp.ru/cio/2010/09/13004345/

ФИНАНСОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Даниловских А.А., Конвисарова Е.В.

Владивостокский государственный университет экономики и сервиса, Владивосток, e-mail: danilovskikh75@mail.ru

В условиях современной рыночной экономики обеспечение информационной безопасности коммерческого предприятия выступает неотъемлемым условием ведения бизнеса. С использованием современных информационных технологий у предприятий появляется все больше новых возможностей для автоматизации бизнес-процессов, расширения сотрудничества предприятия со своими партнерами, для продвижения своей продукции (услуг) и привлечения клиентов в сети Интернет. Редкая компания сегодня не имеет своего сайта, или не использует Интернет-банкинг. Однако, вместе с положительными сторонами, быстрое развитие информационных технологий порождает все больше угроз для безопасности предприятия.

Угрозы информационной безопасности предприятий условно можно разделить на две группы:

– традиционные угрозы безопасности информации, такие как нарушение конфиденциальности или неправомерное использование информации, реализуемые через новые механизмы, возникшие в результате использования информационных систем;

– новые угрозы, порожденные спецификой информационных систем – вирусы, сетевые атаки, нарушения функционирования и отказы разного рода, всевозможные нарушения персоналом установленных регламентов, инструкций и предписаний по эксплуатации и обслуживанию информационных систем. [1]

Под информационной безопасностью понимается состояние защищенности корпоративных данных, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность. [6]

При этом под конфиденциальностью понимается свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц. Целостность – это свойство информационных ресурсов, в том числе информации, определяющее их точность и полноту. В свою очередь доступность информации – это свойство, определяющее возможность получения и использования информации по требованию уполномоченных лиц [4].

Аутентичность информации – свойство, гарантирующее, что субъект или ресурс идентичны заявленным. Данные критерии являются базисом защиты информации, без которых нормальная деятельность предприятия невозможна. Так, повреждение бухгалтерских баз является примером нарушения целостности, которое повлечет за собой негативные последствия для предприятия, а разглашение информации или утечка данных – это нарушение конфиденциальности. Отказ в обслуживании, вызываемый вирусной активностью, влечет за собой нарушение доступности информации предприятия. Причем, любое из нарушений может быть вызвано, как внутренними, так и внешними угрозами. По мнению специалистов в области информационной безопасности, в настоящее время предприятия терпят ущерб в основном вследствие как преднамеренных, так и случайных действий инсайдеров.

Основной целью создания системы информационной безопасности является обеспечение защищенного хранения информации на разных носителях, защита данных, передаваемых по каналам связи, разграничение доступа к различным видам документов, создание резервных копий, послеаварийное восстановление и т.д.

Защита корпоративных данных достигается путем реализации комплекса организационных (документированные процедуры и правила работы с разными видами информации, средствами защиты и т.п.) и технических (аппаратные и программные средства контроля доступа, антивирусная защита и т.п.) мероприятий.

Обеспечение информационной безопасности – это деятельность, направленная на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Рассматривая информацию как товар, можно сказать, что обеспечение информационной безопасности в целом может привести к значительной экономии средств, в то время как ущерб, нанесенный ей, приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и как следствие нарушения информационной безопасности, владелец технологии, а может быть и автор, потеряют часть рынка и т.д. [7].

В соответствии с международными стандартами обеспечение информационной безопасности предпо-