Раздел VII
Гуманитарные аспекты информационной безопасности

С.В. Блохина
Россия, г. Москва, ОАО «Хьюман Профит»

ФОРМИРОВАНИЕ ОРГАНИЗАЦИОННОЙ КУЛЬТУРЫ, ОРИЕНТИРОВАННОЙ НА УСИЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

В последние годы наблюдается тенденция возрастания значимости организационной культуры, ее влияние на управление организациями, ее роль в процессе слияния и поглощения компаний. Корпоративные слияния и поглощения (M&A) становятся мощным фактором дальнейшей трансформации социальной и экономической жизни и с 1999 г. находятся на пике активности, что привело к фундаментальным изменениям в ряде отраслей, в том числе химической, телекоммуникационной и банковской см. табл.1.

Таблица 1

Данные по сделкам M&A с участием российских компаний за 2006 г. в сравнении с 2003, 2004, 2005 г.г., млн. $ [1]

Отрасли	**Итоги за 2003 г.**		**Итоги за 2004 г.**		**Итоги за 2005 г.**		**Итоги за 2006 г.**	
	Число сделок	Сумма сделок	Число сделок	Сумма	Число сделок	Сумма	Число сделок	Сумма
Добыча полезных ископаемых	10	422,50	11	933,40	8	2 537,70	10	1674,50
Информационные технологии	2	20,00	3	111,00	7	88,00	3	367,00
Машиностроение	11	593,00	19	537,60	25	1 221,80	20	511,10
Металлургия	21	3 453,00	16	1 051,50	16	1 554,50	20	15866,00
Наука	1	7,00	2	11,50	-	-	1	5,00
Нефтегазовая	14	11 297,40	23	14 080,70	22	17 438,00	26	8380,80
Пищевая	31	428,90	23	821,10	37	1 452,30	36	1254,38
Прочие производства	6	116,50	12	195,50	11	1 025,00	15	589,10
Реклама	2	33,00	-	-	6	97,00	3	140,80
Связь	18	1 057,20	22	1 762,50	19	735,20	27	2008,80
Сельское хозяйство	5	87,00	7	64,30	5	37,80	8	147,50
СМИ	4	98,00	7	153,50	9	322,00	23	1292,70
Спорт	1	97,00	2	100,00	1	15,00	1	15,00
Страхование	4	75,70	4	42,00	6	144,90	5	127,20
Строительная	4	62,00	9	144,00	14	1 537,00	14	567,90
Торговля	7	130,70	13	357,50	27	630,00	39	2697,90
Транспорт	9	352,00	22	652,60	4	225,00	14	927,70
Услуги	3	105,00	6	142,60	10	579,70	26	1580,10
Финансы	16	556,90	21	1 022,80	22	1 367,10	32	2530,80
Химическая	6	105,00	10	409,80	15	1 106,66	9	283,60
Лесопромышленный комплекс	4	52,00	4	192,00	5	166,50	6	723,70
Электроэнергетика	1	200,00	1	70,00	2	173,00	3	472,70
ИТОГО	**180**	**19349,8**	**238**	**22862,6**	**273**	**32482,16**	**344**	**42277,28**

В результате слияния (поглощение новой фирмой несколько действующих) компаний происходит создание нового предприятия с передачей ему всех прав и обязанностей двух или нескольких юридических лиц. Поглощением (takeover, acquisition) принято называть «переход контроля над корпорацией»[2].

Существуют различные классификации сделок по переходу корпоративного контроля. Наиболее популярной является классификация, зависящая от необходимости согласия менеджмента приобретаемой компании. Например, дружественные поглощения и управленческие выкупы долговым финансированием происходят с согласия и при активном участии менеджмента приобретаемой компании. Выкупы долговым финансированием обычно происходят в виде тендерных предложений, не требующих согласия менеджеров (рис.1):

Рис. 1. Варианты поглощений

Граница между двумя типами слияний — обеспечивающими рост компании или разрушающими ее стоимость — очень тонка. И несмотря на популярность и большое количество сделок по слиянию и поглощению, большинство компаний не достигают эффекта желаемой синергии при объединении капиталов, причем доля неудачных сделок достигает 60%. Большинство компаний так и не стали развиваться в хорошем темпе, а рост доходов многих компаний, до слияния показывавших приличные результаты, приостановился.

Исследования консалтинговой компании McKinsey показывают, что в 70% случаев потенциально выигрышные сделки губит низкое качество подготовки и проведения интеграции. Почти половина приобретенных компаний продается в течение следующих пяти лет, а 90 % объединений, по утверждению экспертов, никогда не достигают планируемых показателей. Как правило, интеграция финансовых систем и производственных технологий не представляет затруднений. Проблемы возникают при попытке соединения неписаных норм и ценностей, в значительной степени определяющих конечный успех новой организации[3].

По наблюдениям сотрудников консалтинговой компании RHR International Экопси[4] можно выделить ряд основополагающих причин неудач (рис.2). Как видно из рис.1 основной причиной 80% неудачных слияний становится невозможность преодолеть противоречия организационных культур объединяющихся компаний[5] и решение культурных приобретает определяющее значение для любой интеграции - как успешной, так и неудачной. Для этого необходимо в краткосрочном периоде выявить "культурные проблемы", связанные с сотрудниками, общением, структурными преобразованиями, приоритетами в создании стоимости и т.д., и заняться их решением; в

долгосрочном периоде сформировать организационную культуру, при которой сотрудники старались бы эффективнее трудиться и выполнять задачи, поставленные "Новой компанией".

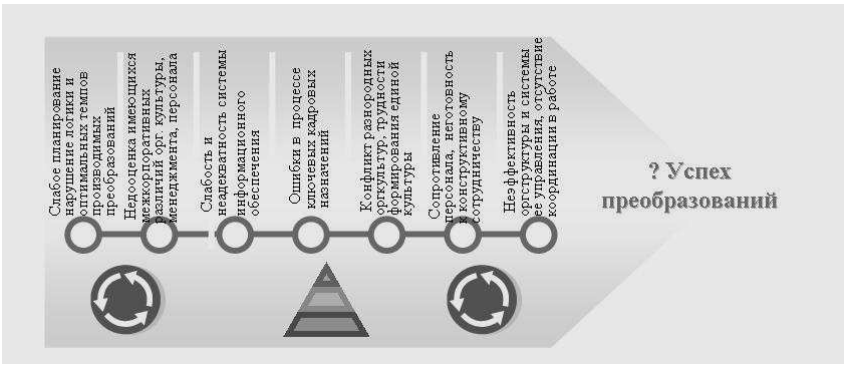

Рис.2. Перечень причин, влияющих на успешное развитие компаний после слияния и поглощения

Грамотно решать эти задачи особенно важно, если объединяются компании из разных стран или отраслей и если стоимость сделки создают люди, а не только активы. Не удивительно, например, что при слияниях Альфа Групп и БР разгорелся культурный конфликт. Примеры успешного объединения, такие как создание промышленного конгломерата ABB из шведской Asea и швейцарской Brown Boveri или слияние фармацевтических компаний Smithkline и Beecham (которые затем объединились с Glaxo Wellcome) показывают, что культурные препятствия вполне преодолимы, нужно лишь применить соответствующие методы.

Совершенствование организационной культуры, превращение ее в мощное побуждающее и объединяющее начало - важный рычаг повышения эффективности функционирования компаний, один из основных показателей их управляемости.

Однако не стоит забывать и о другом важном факторе успешности слияния и поглощений - обеспечении безопасности созданного предприятия, т.к. на этом этапе заметно уменьшается лояльность персонала обеих организаций, наблюдается отток кадров и есть «обиженные» сотрудники.

Безопасность любой организации включает в себя: финансовую безопасность, силовую безопасность, информационную безопасность, технико-технологическую безопасность, правовую безопасность (рис 3.). Главной целью обеспечения экономической и информационной безопасности предприятия является достижение максимальной стабильности функционирования, а также создание основы и перспектив роста для выполнения целей бизнеса, вне зависимости от объективных и субъективных угрожающих факторов (негативных воздействий, факторов риска). Кадровая безопасность является одной из составляющих экономической и информационной безопасности.

Большая часть ущерба материальным активам компаний наносится их собственным персоналом. Только 20 % попыток взлома сетей и получения несанкционированного доступа к компьютерной информации приходит извне. Остальные 80% случаев спровоцированы с участием персонала компаний[6] .

Мошенничество сотрудников стало основной причиной вынужденного закрытия около 100 американских банков за последние 20 лет. 95 % ущерба, понесенного в банковской сфере США, образуется при непосредственном участии персонала банков и только 5 % за счет действий клиентов и иных лиц,

несмотря на наличие передовой системы safety & security и огромных средств, выделяемых на защиту активов. В среднем подобные проблемы стоят от 6 до 9 % прибыли компании.

Рис.3. Основные направления деятельности подразделений, обеспечивающих безопасность организаций

По данным аналитиков CERT[7] в 92 % случаев саботажу и мошенничеству предшествует неприятный инцидент или целая серия таких инцидентов на работе. В 47 % случаев – увольнение, в 20 % – спор с нынешними или бывшими коллегами, 13 % – перевод в должности или, наоборот, отсутствие повышения. 85 % всех внутренних диверсантов рассержены на кого-то, кого они ассоциируют с компанией. Так в 57 % случаев сослуживцы саботажника характеризовали его, как чрезвычайно рассерженного и раздраженного человека. Рост злоупотреблений наблюдается в период слияния компаний и первые годы ее реструктуризации после совершения сделки.

Итак, 84 % злоумышленников руководствуются хотя бы частично местью. В 41 % случаев они хотят донести свою ярость до обидчика, в 12 % требуют признание собственной значимости и уважения, в 12 % выражают свое несогласие с политикой компании, а еще в 12 % – несогласие с культурой компании. В общем, в 57 % случаев сотрудники руководствуются более чем одним мотивом.

Мошенничество по отношению к работодателю настолько обычное явление, что компания Ernst & Young исследование этого вопроса сделало ежегодным. Комментируя результаты девятого международного исследования вопросов противодействия мошенничеству: "Риск мошенничества на развивающихся рынках", Дэвид Сталб подчеркнул: "Информация о громких скандалах, связанных с мошенничеством и коррупцией, занимает первые полосы газет в разных странах. Их влияние на капитализацию кампаний и состояние рынка огромно. Принимая во внимание, что наибольшие опасения в отношении мошенничества связаны с ведением бизнеса на развивающихся рынках, и что 20% всех компаний уже стали жертвами мошенничества, организации, продолжающие недооценивать указанный риск, могут столкнуться с тяжелыми последствиями»[8]. Результаты исследований Ernst & Young, изложенные в отчете "Мошенничество: как бороться с реальной угрозой"[9], показало, что восприятие риска мо-

шенничества и фактический риск возникновения многих видов мошенничества могут не совпадать. Специалисты компании Ernst & Young считают, что организация, в которой царит атмосфера открытости и доверия, гораздо меньше подвержена риску мошеннических действий со стороны сотрудников, чем та, в которой господствуют секретность, страх, недоверие и авторитарность, т.е. речь идет о силе и здоровье организационной культуры. Данные этого исследования опосредованно подтверждаются данными исследований по странам СНГ в рамках международного опроса по информационной безопасности. Основной вывод, согласно эмпирической информации полученной в ходе опроса заключается в том, что во всем мире компании сталкиваются с одинаковыми проблемами по информационной безопасности, которые включают [10]:

1. Недостаточную информированность руководства компании и совета директоров о проблемах информационной безопасности, а также недостаточное финансирование.
2. Недостаточное внимание вопросам развития персонала, таким как обучение и повышение квалификации сотрудников, обеспечение информированности персонала для повышения уровня подготовки в области безопасности и информационных рисков.
3. Недостаточное понимание того, что информационная безопасность является вопросом ведения бизнеса, а не просто вопросом информационных технологий.
4. Компании не требуют от деловых партнеров внедрения достаточных стандартов безопасности, отсутствие которых может подвергнуть риску их собственную безопасность.

Представляет интерес опыт слияния Компании IBS и Консалтинговой группы "Борлас" с целью создания уникальной по своим финансовым, человеческим и технологическим ресурсам структуры, консолидированная выручка которой за 2006 финансовый год оценивается в 370 млн. долларов США (по US GAAP), с общим количеством сотрудников – более 2700 (из них – более 1500 сертифицированных консультантов) и суммарной долей услуг в обороте – более 50%. Интеграция ресурсов должна обеспечить объединенной команде абсолютное лидерство на рынке бизнес-приложений и управленческого консалтинга (более 20% рынка) и сделать ее крупнейшей компанией России и Восточной Европы в области оказания ИТ-услуг. В качестве независимого сертифицирующего органа выступила международная корпорация Lloyd's Register Quality Assurance (LRQA) [1], признавший систему бизнес-менеджмента IBS DataFort, интегрирующего в единое целое системы менеджмента качества, менеджмента ИТ-услуг и информационной безопасности, одной из образцовых в Европе.

Руководством компании предпринимаются усилия по формированию атмосферы информационной открытости, сохраняются основные традиции и положительные ценности обеих компаний. И хотя говорить сегодня об успехе слияния пока рано, эксперты и сотрудники обеих компаний дают положительные прогнозы. При слиянии и поглощении компаний необходимо составить "культурную базу данных", включающую в себя различия и сходства в организационных культурах компаний. Анализировать культурные проявления событий в обеих компаниях следует с учетом групповых различий. Даже в рамках одной компании можно найти различные субкультуры, например субкультура в подразделении, где работают актуарии и отделы страховых агентов одной страховой компании. Если при создании "культурной базы данных" игнорировать различия такого рода, то аналитическая работа будет иметь минимальную ценность.

Таким образом, в новой объединенной компании при формировании организационной культуры, ориентированной на создание информационной безопасности, и чувстве приверженности сотрудников компании, необходимо следующее. 1) Сформировать сплоченную руководящую команду, приверженную задачам и

ценностям "Новой компании". Члены этой команды должны стать примером для остальных сотрудников. 2) Проанализировать основные методы управления, чтобы они отвечали задачам формирования новой культуры. 3) Провести ротацию членов команды, проводящей интеграцию в наиболее сопротивляющиеся подразделения. 4) Разработка и внедрение программ внутреннего PR по поддержке изменений. Например, введение еженедельных совещаний по ходу преобразований. Рассылка информационных писем от директората и пр. 5) Создание системы мер по материальному и нематериальному стимулированию сотрудников, при которых работнику будет невыгодно осуществлять действия, наносящие ущерб организации и ее руководству. Внедрение программ "золотые наручники", дополнительно "привязывающих" работника к компании, которые он не сможет получить в конкурирующих организациях. 6) Формирование лояльности и приверженности работников. 7) Разработка программ заботы о сотрудниках в ситуациях, при которых работник или близкие ему люди могут оказаться в безвыходном критическом положении при возникновении острых жизненных проблем. 8) Развитие управленческих навыков и навыков мотивации подчиненных у руководителей компании. 9) Проведение сплачивающих командных мероприятий и укрепление психологического климата, не допускающих возникновение случаев нарушения лояльности и благоприятного для эффективной работы каждого. 10) Внедрение процедуры регулярной оценки достижений работников на основании объективных показателей деятельности (KPI). 11) Проведение регулярных опросов по удовлетворенности трудом и скрытой текучести. 12) Ведение в практику стандартов работы со служебной информацией и правил поведения, препятствующих случаям проявления ненадежности. Контроль за соблюдением стандартов. 13) Разработка и внедрения процедур "цивилизованного увольнения" работника за грубые нарушения дисциплины и нелояльность. 14) Разработка и внедрения программ обратной связи для сотрудников. 15) Введение технологии реагирования на нарушение технологических и информационных сбоев.

Вывод. Совершенствование организационной культуры значительно повышает эффективность функционирования компаний. Важным фактором успешности слияния и поглощений является обеспечение безопасности новой компании, так как при этом заметно уменьшается лояльность персонала. Предложен перечень необходимых действий для новой объединенной компании, который обеспечит информационную безопасность и чувство приверженности сотрудников компании.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Журнал «Слияния и Поглощения» http://www.ma-journal.ru/statma/

2. *Downes J., Goodman J.E*., Barron's finance and investment handbook/ NY, 1995 p. С.625.

3. *Пэлтер Р., Шринивасан Д*., Уроки поглотителей // Вестник McKinsey. №14. (2006), McKinsey on Finance, 2006, http://www.mckinsey.com/russianquarterly/articles/issue14/04_0306.aspx

4. *В. Столин*, Менеджмент корпоративных слияний // "Банковское дело в Москве" , N9 (45) 1998 г., http://www.bdm.ru/arhiv/1998/09/43-45.html

5. *Пэлтер Р., Шринивасан Д*., Уроки поглотителей // Вестник McKinsey №14 (2006), McKinsey on Finance, 2006, http://www.mckinsey.com/russianquarterly/articles/issue14/04_0306.aspx

6. http://www.cert.ru/about.html

7. http://www.cert.ru/about.html

8. *Денщикова Л.* Компании опасаются мошенничества на развивающихся рынках, но не принимают эффективных мер Лондон, Москва, 15 июня 2006 г http://www.ey.com/global/Content.nsf/Russia/Press-Release_-_15_06_2006

9. www.ey.com/ru/InfoSecuritySurvey.

10. www.ey.com/ru/InfoSecuritySurvey

11. http://www.datafort.ru .