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-

лагает следующее. В первую очередь, предприятию необходимо сформулировать ясную политику информационной безопасности, концептуально отражающую принятые в компании цели, принципы, подходы и методы обеспечения информационной безопасности. Такая политика должна эффективно поддерживаться руководством компании и адекватно пониматься всеми ее сотрудниками [2].

Под политикой безопасности понимают совокупность технических, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, четко регламентирующих все вопросы обеспечения безопасности информации [8].

Следующим шагом является структуризация информации и пользователей:

1) разделение информации по степени конфиденциальности;

2) разделение информации по месту расположения;

3) разделение пользователей по уровню доступа к данным.

Далее, в соответствии с политикой и требованиями безопасности, необходимо выбрать адекватные средства защиты и правильно интегрировать их в информационную систему.

Целями политики информационной безопасности будут являться следующие:

1) обеспечение непрерывности основных бизнес-процессов предприятия;

2) минимизация возможных потерь и ущерба от нарушений в области информационной безопасности.

Эффективность системы обеспечения информационной безопасности предприятия зависит от системности принимаемых мер, перечня задач, и, не в последнюю очередь, от выделяемого бюджета денежных средств. Рассматривая финансовые аспекты обеспечения информационной безопасности предприятия, необходимо отметить, что затраты на внедрение и сопровождение данной системы не должны превышать возможного ущерба от потери информации. Для этого информация предприятия должна быть четко структурирована на подлежащую защите и не составляющую коммерческой тайны, однако, как отмечают специалисты, в российском бизнесе до сих пор преобладает мнение, что защищать нужно абсолютно все. При таком подходе совершенно очевидно, что узнав суммы расходов на информационную безопасность предприятия, руководитель среднего и малого бизнеса машет рукой и надеется на «авось». [3]

К финансовым аспектам обеспечения информационной безопасности бизнеса можно отнести также следующие факторы, влияющие на прибыль:

– величина внутренних издержек, в том числе на содержание коллектива и затрат на обеспечение безопасности в том числе. В результате задания неправильных требований по безопасности, величина издержек может стать настолько обременительной, что сделает бизнес не эффективным. Следовательно, при анализе финансовых результатов компании необходимо обращать внимание на эту группу затрат [5];

– качество управления собственным активом. Если кроме собственника актива или его представителя активом может управлять еще кто-то в собственных интересах, то актив может разворовываться, а бизнес – существенно ухудшаться;

– качество работы коллектива, обеспечивающего бизнес;

– скорость реакции коллектива на внешние факторы, влияющие на бизнес, или на управляющие воздействия;

– стратегия и качество ведения самого бизнеса;

– выбранная стратегия управления рисками, в том числе экономическими рисками и рисками информационной безопасности [1].

Расчет финансовых вложений в обеспечение информационной безопасности предприятия осуществляется чаще всего на основе технологий анализа рисков, далее сравниваются расходы на обеспечение информационной безопасности с потенциальным ущербом, а также вероятностью его возникновения. Кроме количественных характеристик в понятие эффективной политики безопасности будет включаться следующий набор требований: минимальное влияние на производительность труда, учёт особенностей бизнес-процессов предприятия, поддержка руководством, позитивное восприятие и исполнение сотрудниками предприятия.

Таким образом, наличие на предприятии эффективной политики информационной безопасности обеспечивает его устойчивое функционирование, предотвращает угрозы его безопасности, тем самым способствует улучшению его финансового состояния.

Список литературы

1. Андрианов В.В. Обеспечение информационной безопасности бизнеса // электронный ресурс, режим доступа:http://bezopasnik.org/article/book/andrianov_infobez_biz_2011.pdf.

2. Астахов А. Разработка и внедрение эффективных политик информационной безопасности предприятия // электронный ресурс, режим доступа: http://bre.ru/security/20198.html.

3. Информационная безопасность предприятия: внутренняя угроза // электронный ресурс, режим доступа: http://www.safensoft.ru/security.phtml?c=775.

4. Королев М.И. Информационная безопасность предприятия // электронный ресурс, режим доступа: http://www.globez.ru/press/148-informatsionnaya-bezopasnost-predpriyatiya.html.

5. Некрасов С.О., Кузьмичева И.А. Анализ финансовых результатов коммерческой организации // Экономические науки в России и за рубежом. – 2014. – № XV. – С. 75-77.

6. Обеспечение информационной безопасности предприятия // электронный ресурс, режим доступа: http://www.arinteg.ru/articles/detail.php?ELEMENT_ID=25799.

7. Обеспечение информационной безопасности // электронный ресурс, режим доступа: http://www.microtest.ru/it-infrastruktura/informacyonnaya-bezopasnost/

8. Политика информационной безопасности организации // электронный ресурс, режим доступа: http://dehack.ru/razrab_szi/politika_inf_bezop/

ОЦЕНКА ВОЗДЕЙСТВИЯ ПРЕДПРИЯТИЙ СФЕРЫ УСЛУГ НА ЭКОНОМИКУ ПРИМОРСКОГО КРАЯ НА ПРИМЕРЕ ООО «ВВП»

Дворник Г.А., Кравченко А.В.

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

Была проведена оценка воздействия предприятия ресторанного бизнеса на экономику Приморского края на примере кафе «Драшакон». Проведены сравнительные исследования на примере других кафе на территории острова Русский. Предложен комплекс мероприятий для выхода на следующий уровень конкуренции.

Развитие рыночных отношений в нашем крае, да и в стране, во многом зависит от формирования сервисной экономики, в рамках которой основным фактором, является способность максимально удовлетворять потребности потребителя. Стратегия ориентации на потребителя означает, что клиент является центром внимания организации, которая должна стремиться к тому, чтобы как можно лучше понимать тенденции развития системы значимости заказчика. Оценка воздействия сферы услуг на экономику является необходимым условием для выбора сферы деятельности предприятия и его эффективного развития. Объектом данного исследования является кафе «Драшакон», расположенное на кампусе ДВФУ острова Русский. Основными клиентами данного кафе явля-