Журнал правовых и экономических исследований, 2012, 3: 106–110
© Е.В. Попова, 2012

УДК 338.28

Е.В. Попова

ПОВЫШЕНИЕ КОНКУРЕНТОСПОСОБНОСТИ МАЛЫХ ПРЕДПРИЯТИЙ СФЕРЫ УСЛУГ ПУТЁМ УСИЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСЛЕ ПРИНЯТИЯ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматривается влияние информационной безопасности на повышение уровня конкурентоспособности малых предприятий сферы услуг после принятия Федерального закона «О персональных данных». Обосновывается тезис о том, что закон стимулирует дальнейшее развитие комплекса мероприятий по усилению информационной безопасности, повышая этим уровень конкурентоспособности предприятия.

Ключевые слова: *конкурентоспособность; малые предприятия сферы услуг; конкурентные преимущества; информация; клиентские базы данных; информационная безопасность; ФЗ РФ «О персональных данных».*

We consider the influence of information security on increasing the level of competitiveness of small business in service sphere after passing the federal law of the Russian Federation "On personal data". We prove the idea that the law contributes to further development of a set of measures to improve information security for increasing business competitiveness.

Keywords: *competitive ability; small businesses of service sphere; competitive advantage; information; client database; information security; federal law of the Russian Federation "On personal data".*

В последние годы проявляется постоянно возрастающая конкуренция во всех областях российского рынка. Либерализация импорта, появление иностранных компаний, достигнутые договорённости о вступлении нашей страны во Всемирную торговую организацию трансформируют рыночную ситуацию. Рост предложения товаров и услуг, одновременное уменьшение платежеспособного спроса, ожидание новой волны кризиса вывели проблемы конкурентоспособности предприятия на первое место. Для преодоления возникающих трудностей необходимо создание конкурентоспособного производства, ориентированного на нужды потребителей. Начиная с 90-х годов прошлого века, приоритетным направлением развития фирм и конкурентных стратегий становится «ресурсная школа» [10]. Происходит возврат на обновлённой интеллектуальной основе к внутренним возможностям фирмы. Особую ценность приобретают уникальные ресурсы компании, которые невозможно или чрезвычайно дорого сымитировать. Эти ресурсы способны приносить в течение длительного времени ренту, которая позволяет компании сохранять устойчивые конкурентные преимущества на рынке. Базовой характеристикой таких ресурсов является их нематериальный характер, поэтому понижается возможность имитации и воспроизведения ключевых ресурсов конкурентами. Возрастает роль нематериальных активов в формировании потенциала конкурентоспособности. Это знания, умения, репутация, бренды, взаимоотношения с потребителями, атмосфера доверия и сотрудничества. Для развития важна также система устойчивых связей, посредством которых происходят рыночные взаимодействия. Поэтому основными движущими силами конкуренции на сегодня являются знания и технологии. Происходит сокращение планируемого горизонта, исследуется постоянно меняющаяся окружающаяся среда, используются новые методы управления – сохранение стратегических ориентиров при постоянном мониторинге изменений, гибкая адаптация к этим

изменениям [8]. Основная стратегическая проблема при этом – как достичь и сохранить конкурентоспособность в избранной области деятельности.

Экономисты В.Д. Грибов и В.П. Грузинов в работе «Экономика предприятия» рассматривают понятие конкурентоспособности как преимущество по отношению к другим предприятиям данной отрасли внутри страны и за ее пределами [5]. Задача компании заключается в обеспечении потребителей более высокой по сравнению с конкурентами ценностью, в развитии долгосрочных взаимоотношений с покупателями. Конкурентоспособность малых предприятий сферы услуг обусловлена персонифицированным характером взаимодействия с клиентами, отсутствием массового, обезличенного производства товаров и услуг [9]. На рынок поступают индивидуализированные товары и услуги, ориентированные на узкие вкусовые предпочтения потенциальных потребителей. Поэтому информация и персональные данные играют огромную роль в увеличении полезного эффекта предоставляемой услуги [11], а защита информации, усиление информационной безопасности повышают уровень конкурентоспособности малых предприятий сферы услуг.

Ещё в конце прошлого столетия во всех компаниях происходил процесс миграции материальных активов в сторону информационных. Информация стала ключевым звеном при решении всех бизнес-задач [7], укреплении репутации и повышении конкурентоспособности. В малых предприятиях сферы сервиса появляются информационные системы, новые информационные технологии, активнее используется Интернет, который даёт возможность удалённого общения с потребителями, поставщиками, ведения электронного бизнеса, взаимодействия с налоговыми и контролирующими органами посредством технологии электронной подписи. Можно снизить издержки благодаря более эффективному управлению материальными запасами, предложению индивидуальных цен и рекламы [3]. Кроме того, Web-сайты компании помогают наиболее дёшево, быстро и эффективно охватить целевые рынки, круглосуточно взаимодействовать с клиентами и поставщиками, размещать необходимую информацию о предоставляемых товарах и услугах [4]. Благодаря этому происходит накопление информации об индивидуальных профилях каждого клиента, создаётся клиентская база данных, в которой отражены жизненные ценности клиентов, причины ухода бывших клиентов, психологические, географические, гендерные и возрастные особенности клиентов. Всё это способствует тому, что на рынке поставляются наиболее конкурентоспособные товары и услуги. Но параллельно всё больше появляется желающих украсть, повредить базы данных, попытаться завладеть информационными ресурсами конкурента. Возрастает вероятность нарушений информационной безопасности, которые провоцируют болезненные изменения в ведении бизнеса, понижение уровня конкурентоспособности предприятия. Вследствие этих процессов и усиления роли государства в формировании информационной безопасности не только крупные и средние, но и малые предприятия сферы услуг сегодня вынуждены уделять больше внимания вопросам информационной безопасности. Государство инициирует программы по переходу к электронному взаимодействию с государственными и коммерческими структурами, принимает и вносит поправки в ФЗ-152 «О защите персональных данных». В этой ситуации все предприятия вынуждены уделять проблеме сохранности данных своих клиентов больше внимания. Информационная безопасность перешла из разряда чего-то второстепенного в необходимый, важный для бизнеса инструмент, повышающий конкурентоспособность компании.

Закон о персональных данных принимался не только в связи с возросшим числом инцидентов, связанных с утечкой конфиденциальной информации, но и для устранения барьеров в торговле со странами Евросоюза. Персональные данные могут передаваться из Европы только в страны, обеспечивающие такой же уровень защиты, как и в самих европейских странах. Для ликвидации затруднений по выполнению многих проектов в 2006 году был

принят закон ФЗ-152 «О защите персональных данных» [1]. Он вступил в действие в 2007 году и представляет собой перечень требований к защите персональной информации. В 2008 году вышло несколько уточнений к этому закону, например, «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Это было вызвано тем, что в кризисные времена активизируется недобросовестная конкуренция и инциденты с базами данных клиентов значительно увеличиваются. В соответствии с этим законом каждое предприятие должно обеспечить защиту персональных данных своих сотрудников, клиентов и партнеров и принять все необходимые меры во избежание следующих правонарушений: кража персональных данных; изменение; блокирование; копирование; разглашение информации и другие незаконные действия, указанные в ФЗ РФ № 152-ФЗ «О персональных данных».

Ст. 22 ФЗ РФ «О персональных данных» обязывает организации до начала обработки персональных данных уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. В случае нарушения требований ФЗ РФ «О персональных данных» оператор персональных данных может быть привлечен к гражданской, уголовной, административной либо дисциплинарной ответственности, а уполномоченный орган по правам субъектов персональных данных может ходатайствовать о приостановлении лицензии организации по основному виду деятельности либо об ее отзыве. Более того, ст. 17 ФЗ РФ «О персональных данных» разрешает гражданам подавать в суд на операторов персональных данных и требовать возмещение убытков и компенсацию морального вреда в случаях, когда оператор нарушает требования данного закона. В 2011 г. были приняты новые поправки [2]. Внесены изменения в ряд определений, устранены некоторые противоречия, имевшиеся в предыдущей редакции закона.

В настоящее время под персональными данными понимают любую информацию, относящуюся к определенному физическому лицу (субъекту персональных данных). Персональными данными является только совокупность фактов, точно идентифицирующих физическое лицо. Оператор обязан назначить ответственного за организацию обработки персональных данных; издать документы, определяющие политику в отношении обработки персональных данных; провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства; ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных. Также оператор обязан провести маркировку документов, содержащих персональные данные, вести учёт доступа к этим документам. Впервые в отечественной практике устанавливается максимальный срок хранения информации, необходимость предварительной фиксации в документах понятия «обработки» персональных данных, соблюдение весьма жестких сроков исполнения всех обращений граждан, связанных с обработкой персональных данных.

Одним из самых обременительных требований для организаций является требование ст. 6 о необходимости получить согласие субъекта на обработку персональных данных, либо иметь доказательства того, что собранные данные взяты из общедоступных источников (ст. 9). В ст. 15 говорится, что прежде чем посылать рекламу, необходимо получить предварительное согласие гражданина. Блокировка данных должна быть осуществлена с момента обращения или с момента получения запроса, а устранение нарушений – в течение трёх рабочих дней. Но трудность заключается в том, что и блокировка, и уничтожение персональных данных в эксплуатируемых информационных системах и базах данных раньше не проводилась. Обязанностью оператора, согласно ст. 19, является также обеспечение безопасности персональных данных при их обработке [1]. То есть необходимо заранее разработать и за-

крепить в нормативных документах все организационные и технические меры по обеспечению информационной безопасности.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) после проведения проверок может наложить штраф, конфисковать несертифицированные средства защиты или вынести требование о прекращении обработки персональных данных, что может негативно сказаться на всех бизнес-процессах предприятия. Кроме того, при нарушении закона возможна подача судебных исков к компании, которые чреваты финансовыми и репутационными потерями, и, в конечном итоге, понижением уровня конкурентоспособности компании. Но вместе с тем ФЗ-152 «О персональных данных» способствует формированию культуры защиты персональных данных, приближает нас к европейским стандартам обработки персональных данных, инициирует дальнейшее развитие информационной безопасности и раскрывает связь между уровнем информационной безопасности и конкурентоспособностью предприятия.

Под информационной безопасностью понимают комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы: конфиденциальность, целостность, доступность, учёт и неотрекаемость [6]. Информационную безопасность можно представить как реализацию и совершенствование наиболее рациональных методов и способов развития системы защиты, которая состоит из следующих этапов: разработка политики безопасности, текущий ситуационный контроль, выявление слабых мест, реагирование на происходящие изменения. Политика безопасности начинается с анализа возможных угроз и последующей выработки системы управления рисками. На этой основе вырабатываются технологии для защиты информации и процедуры, которые будут обеспечивать работу этих технологий.

Часто вопросы повышения информационной безопасности малого предприятия сферы услуг рассматриваются исходя из бюджетных ограничений. Поэтому решения по обеспечению информационной безопасности должны иметь минимальную стоимость или входить в состав операционной системы. Важно максимально использовать возможности имеющегося программного обеспечения, выбранного браузера, вовремя проводить обновления и резервное копирование, наделить пользователей через учётную запись нужными правами доступа и запустить механизм идентификации пользователей. Запрещение использования слабых паролей и беспроводной связи уменьшает вероятность непреднамеренных угроз и локальных атак, либо у пользователей мобильных устройств должны быть установлены агент-клиенты, правильные пароли, устройства идентификации. Соотношение внутренних и внешних угроз сейчас оценивается как восемь к двум, но на малых предприятиях вероятность возникновения инсайдеров резко понижается в связи с меньшим количеством работников и возможностью контролировать каждого. Чем больше устройств, которыми пользуются работники предприятия, имеют выход в Интернет, и чем более эти устройства взаимодействуют между собой, тем больше точек уязвимости имеет вся система в целом. Поэтому небольшие корпоративные системы малых предприятий сферы сервиса, имеющие ограниченное количество серверов, связанных с Интернетом, имеют преимущества перед гигантскими сложными системами крупных предприятий.

Сегодня существует целый комплекс технологий, позволяющих управлять рисками информационной безопасности. Это антивирусы, файерволы, средства защиты от утечек Data Leakage Prevention (DLP), средства контроля доступа к сети (NAC), системы обнаружения вторжений Intrusion Detection System (IDS). На сервере, имеющем доступ к Интернету, следует установить межсетевой экран для того, чтобы пакеты из локальной сети не попадали наружу и наоборот. При его настройке можно разрешить обмен данными с Интернетом только по тем протоколам, которые реально используются на предприятии, и ограничить время работы маршрутизатора

временем работы предприятия. На корпоративный сервер электронной почты следует поставить антивирус и установить пользователям e-mail-клиент, который не даёт показывать вложенные в письма HTML, причем существуют и бесплатные программы такого рода. Антивирусное программное обеспечение и локальный firewall следует установить на каждый компьютер, и здесь тоже есть бесплатные предложения для малых предприятий. Также необходимо создать точку восстановления системы на случай сбоя. Можно установить корпоративный Proxy-сервер, что позволит скрыть внутренние имена и адреса компьютеров, сократить интернет-трафик и запаролить доступ к ресурсам Интернета. Данные лучше хранить с помощью системы управления версиями документов и файлов с открытыми кодами, таких как бесплатные системы CVS или Subversion.

Помимо всего прочего, актуальной угрозой остается взлом веб-приложений. Здесь лучше всего справляются решения класса Web Application Firewall, также следует использовать навыки безопасного программирования при создании Web-сайтов. Сотрудники периодически должны получать инструктаж об основных правилах проведения политики информационной безопасности и возможных угрозах. И, наконец, в соответствии с требованиями ФЗ РФ «О персональных данных» необходимо определить статус хранящихся персональных данных; уточнить и зафиксировать состав персональных данных и источники их получения; установить сроки хранения и сроки обработки данных; определить способы обработки; определить лиц, имеющих доступ к данным, и порядок реагирования на обращения. Клиентов можно заранее информировать об озабоченности фирмы вопросами информационной безопасности, выполнении требований ФЗ РФ «О персональных данных» и бережном отношении к конфиденциальной информации клиентов.

Накопление клиентских баз данных, вызванное увеличением роли информации и данных о клиентах в бизнес-процессах и возрастанием нарушений информационной безопасности, стимулировало принятие ФЗ-152 «О персональных данных». В свою очередь этот закон способствовал повышению значимости информационной безопасности в малых предприятиях сферы услуг и усилению влияния информационной безопасности на повышение уровня конкурентоспособности предприятий.

ЛИТЕРАТУРА

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. Фед. выпуск. 2006. 29 июля. № 4131.

2. Федеральный закон Российской Федерации «О персональных данных» с учетом изменений от 25.07.2011 г. Полный текст // Аргументы и факты. 2011. 27 июля.

3. *Анн Х., Багиев Г.Л., Тарасевич В.М.* Маркетинг. 3-е изд. / под общ. ред. Г.Л. Багиева. СПб.: Питер, 2005. 736 с.: ил. (Серия «Учебник для вузов»).

4. *Басовский Л.Е.* Финансовый менеджмент. М.: ИНФРА-М, 2008. 240 с.

5. *Грибов В.Д., Грузинов В.П.* Экономика предприятия. 3-е изд., перераб. и доп. М.: Финансы и статистика, 2008. 336 с.: ил.

6. *Конеев И.Р., Беляев А.В.* Информационная безопасность предприятия. СПб.: БХВ – Санкт-Петербург, 2003. 752 с.: ил.

7. *Мескон М.Х. , Альберт М., Хедоури Ф.* Основы менеджмента / пер с англ. М.: Дело, 2006. 720 с.

8. Основы маркетинга / Г. Амстронг, В. Вонг, Ф. Котлер, Д. Сондерс; пер. с англ. 4-е европейское издание. М.: Издат. дом «Вильямс», 2008. 1200 с.: ил.

9. Предпринимательство: учебник для вузов / под ред. проф. В.Я. Горфинкеля, проф. Г. Б. Поляка, проф. В.А. Швандара.- 4-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА, 2008. 735 с. (Серия «Золотой фонд российских учебников»).

10. *Третьяк О.А.* Маркетинг: новые ориентиры модели управления. М.: ИНФРА-М, 2005.

11. *Фатхутдинов Р.А.* Конкурентоспособность организации в условиях кризиса: экономика, маркетинг, менеджмент. М.: ИКЦ «Маркетинг», 2002. 892 с.