

УДК 330.131.7 (575.2) (04)

РИСК-МЕНЕДЖМЕНТ В ЭЛЕКТРОННОМ БИЗНЕСЕ

В.А. Черкасова – канд. экон. наук,
Фирма ГУ – ВШЭ, г. Москва

Ambiguity, real socio-economic processes, variety of possible situations of realization of the decision, presence of the incomplete information creates the certain difficulties for any business, including electronic. In clause the basic risks, stirring to development of electronic business are considered. The reasons of occurrence of such risks come to light; their development in conditions of a varying environment business is traced.

Электронный бизнес, или электронная коммерция – это обмен данными через Интернет, это и электронная почта, и факсимильная связь, передача данных с одного компьютера на другой, сбор данных через Интернет. Во-вторых, это обмен электронными бланками, каталогами, справочниками, доски объявлений, информационные услуги, службы новостей и т.д. Электронная коммерция – это переводы денежных средств. И, наконец, это электронная торговля, осуществление сделок купли-продажи товаров и услуг через электронные сети, что предусматривает доступ в сеть, поиск коммерческого партнера, обеспечение гарантий платежа, поставку товаров, оказание услуг. Таким образом, электронная коммерция – это рынок осуществления конкретных сделок с реальным товаром.

Электронный бизнес – это новый тип взаимоотношений между покупателем и производителем, и поэтому развитие электронной коммерции влияет на изменение традиционного общественно-экономического уклада жизни всего общества. Как и практически любой другой вид хозяйственной деятельности, электронная коммерция не обходится без рисков, среди которых риск мошенничества, уклонение от налогов, риск несоблюдения конфиденциальности, нарушение права на интеллектуальную собственность и др. Большинство рисков электронной коммерции можно избежать

или минимизировать на ранних стадиях планирования, выработки стратегии, выявления рисков и их оценки. Электронная коммерция – это, в первую очередь, все-таки коммерция, хоть и электронная. Интернет же просто позволяет нам делать то, что и всегда, только более быстро, более дешево и различными путями. Поэтому, делая шаг в виртуальный мир, не надо отказываться от планирования и риск-менеджмента, лежащих в настоящее время в основе деятельности любых успешных компаний.

Риски, связанные с нарушением закона. Считается, что Интернет – это протяженная граница, где нет законов. На самом деле, существует огромное количество законов, касающихся деятельности в Интернете, что, в свою очередь, и является главным источником коммерческого риска, рисков электронной коммерции. Опасность заключается в том, что виртуальные компании неумышленно нарушают законы (в связи с их многочисленностью и разнообразностью) тех стран, где они торгуют, и им не удается привлечь во внимание новые методы ведения торговли.

Хорошим примером подобных трудностей является виртуальная торговля в Европейском Союзе. Направление по согласованию экономик стран Европейского Союза сосредоточило свое внимание на создании “поля игры” для производства и продажи товаров и услуг в другие страны (в пределах Евросоюза). Рань-

ше, без больших капиталовложений в создание торговых точек на иностранных рынках сбыта продукции, развития системы заказов по почте было невозможно экспортировать розничную продукцию, товары и услуги. Действуя таким образом, развивая подобную систему экспорта товаров и услуг, производитель (розничный продавец) должен исследовать местные требования, законы, принципы налогообложения. Интернет же позволяет экспортировать продукцию даже в те страны, о которых, возможно, производитель (розничный продавец) и не слышал, законы этих стран в таком случае ему не известны. Это может привести к проблемам у торговца, даже в случае такой Интернет развитой, лидирующей в этой отрасли экономики, как США. Например, недавно британская авиакомпания “Virgin Atlantic” испытала трудности в связи с размещением на своем web-сайте рекламы тарифа на перелет через Атлантику, общепринятого в Великобритании (“из Лондона в Нью-Йорк всего за £х плюс налоги и регистрационный сбор – за деталями обращайтесь в местные туристические агентства”). Однако, в соответствии с законами США, простое указание на тот факт, что дополнительные услуги оплачиваются, является недостаточным. Компания должна установить точную цену налога и регистрационного сбора. В то время как Virgin Atlantic заплатила стандартный для такой ситуации штраф, сама реклама оказалась по-настоящему убыточной. Также в Германии Закон “О защите прав потребителей” утвердил жесткие ограничения на установление скидок и бонусов, которые могут быть предложены розничным торговцем покупателям [1].

Новое законодательство Евросоюза должно обратить внимание на то, что риски электронной коммерции возникают также в связи с разными принципами налогообложения, разными режимами защиты прав потребителей в различных странах. В настоящее время пока не ясно, будет ли успешным новое законодательство. Неудачные попытки Евросоюза привести свои рынки сбыта в соответствие друг с другом являются результатом своей инфантильности – для избранных правительств трудно на политическом уровне изменить законы, защищающие права потребителей своих стран, так, чтобы поставить их в соответствие с по-

требностями международной коммерческой деятельности или просто других стран. Страны – члены Евросоюза – не имеют, вероятно, общей цели по согласованию законов об электронной коммерции. Даже если они и придут к согласию, то, возможно, не захотят делать это в условиях риска потери контроля над способами осуществления коммерческой деятельности и принципами налогообложения.

Вот некоторые текущие инициативы Евросоюза:

- Директива об электронной подписи, которая определяет нормы для обеспечения юридической силы электронной подписи;
- Директива об электронной коммерции, которая имеет своей целью поощрение электронной коммерции, управление продажей товаров и услуг через Интернет;
- Директива о продажах на дальние расстояния, которая обеспечивает дополнительную защиту потребителей (например, оговаривает сроки исполнения заказа), которые покупают товары и услуги, не сталкиваясь лицом к лицу с продавцом (производителем);
- Директива о предоставлении финансовых услуг;
- Директива об обработке личных данных и защите личной тайны в сфере электронных коммуникаций, обеспечивающая дополнительную защиту тем лицам, чьи персональные данные содержатся в Интернете.

Билль об электронной коммерции в Великобритании утверждает признание электронной подписи как доказательства подлинности документа.

Независимо от того, будут ли приняты какие-нибудь из директив, потребность в согласовании законов различных юрисдикций Евросоюза все равно остается. В любом случае, до тех пор, пока нет четкого согласования законодательств разных стран, любой производитель, любая компания, занимающаяся электронной коммерцией, несет риски.

На ранних стадиях планирования и выработки стратегий компании может потребоваться юридическая консультация, особенно в отношении заключения договоров с провайдерами, предоставляющими услуги для организации электронной торговли, со специалистами по высоким технологиям и в отношении под-

писания контрактов, касающихся интеграции систем ИТ. Остальными являются вопросы об определении предоставляемых услуг, сроков, критериев качества услуг и установлении процедур тестирования. Неосуществление всех этих процедур может привести к работам по устранению дефектов и недостатков, ремонтным работам и задержкам.

Прежде чем реализовывать выработанную стратегию компании должны учесть четыре вида рисков электронной коммерции, связанных с нарушением законов, потому что иначе она может случайно обнаружить, что нарушает законы тех стран, в которых продает свою продукцию. Необходимо отметить, что Интернет создает круг юридических ловушек, в которые попадают не только компании, начинающие дело, но и давно основанные. Итак, контрактный риск может возникнуть, когда условия договора оговорены нечетко и недоступны в понимании пользователям. Осуществление операций, не попадающих под местные законы, вызовет, скорее всего, появление юридических проблем, а торговые марки, зарегистрированные в одной стране, и интеллектуальная собственность могут не иметь никакого значения в другой. Наконец, страны имеют разные законы, касающиеся конфиденциальной информации, которая может распространяться через Интернет. Рассмотрим все эти риски подробнее.

Контрактный риск. До тех пор, пока контракт не относится к категории соглашений, которые должны быть скреплены подписями и печатями, не существует юридических препятствий к заключению договора через Интернет. Однако это опять же область, где компании могут попасть в ловушку, созданную местными законами. Предложенное американское законодательство (включая Акт о цифровых подписях (the Digital Signatures Act), Акт роста и развития сети Интернет (the Internet Growth And Development Act) и Акт об электронных подписях в мировой и национальной коммерции (the Electronic Signatures In Global And National Commerce Act)) обеспечит закрепление законом США использование электронной подписи. Директива Европейского Союза об электронной коммерции (the EU's E-Commerce Directive) требует, чтобы всем элек-

тронным договорам была дана такая же юридическая сила, как и письменным соглашениям. Эти положения, если будут приняты, помогут избежать недоразумений, но в то же время могут спровоцировать появление мнения в Европе и США, что электронные договоры действительно всегда, хотя в некоторых странах они действительно не будут [2].

Главный контрактный риск – часто незаметный – неполная договоренность об условиях, на основании которых действуют виртуальные компании. Если компания создает веб-сайт, чтобы заниматься коммерческой деятельностью, этот сайт должен выглядеть таким образом, чтобы покупатели не имели возможности сделать заказ до тех пор, пока они не согласятся с законами, которые регулируют деятельность компании. Законы должны быть представлены на рассмотрение покупателю до тех пор, пока он сможет что-нибудь заказать, также должно требоваться его одобрение, подпись.

Условия договора должны содержать пункт о компенсации за убытки в случае нарушения условий договора, часто это – самый важный пункт договора. Самые развитые правовые системы требуют, чтобы каждый такой пункт был четко донесен до потребителя. Например, в Великобритании в соответствии с Актом о “нечестных” условиях контракта (the Unfair Contract Terms Act) решение о “правильности” включения в электронный договор подобного пункта может принять суд. Если, например, он находится в труднодоступной части сайта, то, скорее всего, будет работать неэффективно.

Также для любой компании, предлагающей товары или услуги через Интернет, очень важно контролировать сам процесс заключения договора, приглашая покупателей, чтобы они делали предложение о покупке товара или услуги, о заключении договора с компанией, которое, в свою очередь, может быть компанией принято или отвергнуто. Другая альтернатива для компании – это самостоятельно делать предложение на сайте, которое может принять или отвергнуть покупатель.

Компания “Argos” из Великобритании намеренно разместила на своем веб-сайте предложение о продаже телевизоров за 3 фунта вместо 300. Неудивительно, что сайт был

“осажден” заказами, которые впоследствии компания отвергла на основании того факта, что web-сайт был аналогией изображения витрины магазина и просто “приглашал развлечься”, а также, что предложение, заказы были сделаны покупателями, а не компанией [3]. Это позволило Argos занять такую позицию, что компания могла сама или принять, или отвергнуть предложение покупателя о покупке, заказ. В данном случае передача заказа на рассмотрение не привязывала Argos к контракту, а если бы web-сайт был сделан иначе, как многие другие, то это было бы так.

Обращая внимание на контроль над процессом заключения договора, нужно отметить, что существуют юрисдикции, где компания не захочет действовать, торговать. Контролируя процесс заключения договора, компания может отказаться принять предложение покупателя, например, о доставке продукции в какую-нибудь юрисдикцию.

Риск, связанный с попаданием под юрисдикцию. Одним из аспектов ведения международного бизнеса является гарантия, что правовые системы компании относятся к определенным видам сделок. Некоторые юрисдикции, например, в США уже продемонстрировали желание осуществлять подсудность споров, связанных с деятельностью в Интернете, когда существует тонкая связь между странами. Это – фактор риска, установленный решениями жюри присяжных и возможностью компенсаций убытков в США.

В общем, сделки, которые совершаются в Интернете, будут регулироваться такими же правилами международного частного закона, как и любая другая сделка, заключаемая через границу. По этой причине компаниям рекомендуется оговаривать условия договора, который будет принят законами страны и юрисдикцией, в которой будет осуществляться спор (хотя выбор юрисдикции компанией может не быть распространенным).

С позиции риск-менеджмента обеим сторонам желательно точно определить юрисдикцию и закон, в соответствии с которым будет заключен договор и осуществляться их деятельность. Выбирая юрисдикцию, следует принять во внимание:

☞ как будет действовать закон в пределах выбранной юрисдикции?

☞ как точно может быть предсказан исход конфликта в выбранной юрисдикции?

☞ как много времени потребует, чтобы разрешить конфликт в выбранной юрисдикции?

☞ какова стоимость судебного разбирательства в выбранной юрисдикции?

☞ будет ли судейство в выбранной юрисдикции настроено против ответчика?

☞ в чем заключаются преимущества, активы ответчика?

Риск нарушения права на интеллектуальную собственность. Хотя это и кажется очевидным, но компании часто не обращают на это внимание. Эти права различны по своей природе в разных странах, защита одной торговой марки в пределах одной страны не означает существование права на использование этой торговой марки во всех других юрисдикциях. Создание web-сайта без регистрации торговой марки в основных юрисдикциях несет для компании риск нарушения чужого права на использование такого же товарного знака. Тем самым, важно получить право на интеллектуальную собственность в основных юрисдикциях и охранять это право.

Нерешенным в этой сфере остается вопрос, станут ли новые методы ведения бизнеса общепринятыми, международными, как можно этого ожидать, и будет ли традиционность законов тормозить такое развитие событий. Статья 27 Всемирной Торговой Организации Соглашения о связанных с торговлей правах на интеллектуальную собственность (Trade Related Aspects Of Intellectual Property Rights) утверждает, что получение патентов должно быть возможным при любом изобретательном процессе, даже если этот процесс – еще неизведанный путь предоставления услуг через Интернет. Таким образом, можно наблюдать увеличение количества монополий в связи с патентованием методов ведения бизнеса в Интернете (и с помощью других систем высоких технологий). Например, компания Amazon.com – виртуальный магазин – подала в суд иск против своего конкурента на рынке книг и видеопродукции BarnesandNoble.com. Amazon.com обвинил своего конкурента в том, что его система “экспресс контроля” нарушает патентное право Amazon.com на использование технологии “одного клика”.

Риск подрыва репутации. Пользование услугами электронной почты поощряет скорость и неформальность общения. При таких обстоятельствах, вероятно, распространяется клеветнический материал, и существует огромный риск нарушения конфиденциальности и авторского права. С точки зрения работодателя, доступ сотрудников к электронной почте увеличивает риск работодателя быть обвиненным через клеветнические письма, которые рассылаются работниками. Страховая группа “Norwich Union” в Великобритании и компания “British Gas”, предоставляющая коммунальные услуги, были обвинены в том, что они несут ответственность за клеветнические электронные письма своих сотрудников. С точки зрения риск-менеджмента, компаниям настоятельно рекомендуется составлять протокол об электронных письмах [1].

Интернет открыл новые аспекты риска подрыва репутации и вызывает распространение старых. Корпоративные web-сайты подделываются, сотрудники могут клеветать на своих работодателей, используя электронную почту. В дополнение ко всему этому, подающие жалобы могут использовать дешевые, мгновенные возможности Интернета, чтобы мобилизовать поддержку по всему миру.

Однако Интернет может работать на благо компании во времена кризиса. Например, когда случается авиакатастрофа, компания заинтересована в распространении точной, реальной информации в Интернете, размещении ее на web-сайтах, защищенных паролем, прежде чем “факты” по делу об авиакатастрофе будут представлены средствами массовой информации.

Компании создают “спящие” web-сайты, которые могут быть активизированы во времена кризиса. Эти “спрятанные” сайты могут содержать важную информацию, которая требуется в первые часы кризиса и может быть обновлена, когда другие факты станут доступными. Подобное предпланирование может сохранить жизненно важные часы в случае непредвиденных, чрезвычайных обстоятельств и способно продемонстрировать, что организация всецело контролирует ситуацию. Оно также может гарантировать, что компания служит лучшим источником информации о своих трудностях, снижая потребность средств мас-

совой информации распространять спекулятивную и часто недостоверную информацию о кризисе в компании.

Использование Интернета делает возможным для компании регулярно обновлять информацию, необходимую своим акционерам. Кризисные центры могут делать информацию доступной и в режиме реального времени, что, в свою очередь, помогает им управлять ситуацией. Это может гарантировать, что единственное заявление о текущей позиции компании используется представителями этой компании на каждом рынке, на котором она действует, снижая неточность и несодержательность информации. Использование Интернета может также сделать возможным проведение низкочастотных тренингов и использование опыта прошлого.

Главные менеджеры не могут себе позволить обращаться с одним из самых значимых активов компании в бесцеремонной манере. Ризику репутации должно уделяться не меньше внимания, чем другим традиционным коммерческим рискам. Генералы не ждут разгрома своей армии. Менеджеры должны действовать также.

Риск оказания “невинного” содействия. Компании-провайдеры услуг сети Интернет часто разрешают размещение публикаций третьих лиц на своих web-сайтах. Это подвергает сами компании дополнительным рискам, и не до конца ясно, до какой степени распространители информации могут показывать содержание подобных публикаций, размещенных на их web-сайтах.

Примером подобного риска может служить недавний случай в Англии “Godfrey против Demon Internet” [3]. Так, мистер Laurence Godfrey обнаружил, что на виртуальной доске объявлений провайдера “Demon Internet” была размещена “грязная, непристойная, клеветническая” информация о нем. Мистер Godfrey связался с менеджерами Demon Internet и попросил их убрать оскорбительный материал, но они отказались, и мистер Godfrey решил преследовать провайдера в судебном порядке. Суд постановил, что в то время как Demon Internet и не был автором материала, но он все-таки поместил информацию на своем web-сайте, и поэтому менеджеры не должны были го-

ворить, что не имеют к публикации никакого отношения. На основании этого защита “невинного распространения информации” была недоступна для Demon Internet.

Справедливо, что мистер Godfrey должен был получить некоторую компенсацию, если он столкнулся с грязной клеветой, а провайдеру не следовало просто так игнорировать его положение. Однако тот факт, что любую информацию, которая появляется на его сайте, провайдер услуг сети Интернет обязан просматривать, угрожает свободному распространению информации, что, в свою очередь, является фундаментальной характеристикой Интернета. Любой жалобы по поводу любого сообщения на сайте поставщика услуг сети Интернет будет, как предполагается, достаточно для того, чтобы рассмотреть ее в суде, и тогда она потребует, чтобы решить, является ли материал клеветническим. Слушание дела требует времени и других затрат, а практическое решение может заключаться просто в удалении с сайта той информации, по поводу которой возникла жалоба, ограничивая тем самым свободное распространение информации через Интернет.

Например, в США первая поправка к Закону о свободе слова вызвала различные отношения к этому вопросу. Статья 509 Акта о защите систем телекоммуникаций (the Telecommunication Decency Act) утверждает, что провайдер не является “издателем” материала, размещенного в Интернете третьим лицом, а также защищает провайдера в отношении любых правомерных действий, предпринятых им, чтобы ограничить доступ к материалу, который он может счесть “непристойным, развратным, похотливым, грязным, мерзким, насильственным или, так или иначе, нежелательным, неприятным, вызывающим возражения”.

Реальный эффект от принятия этого акта наблюдался в случае “Zeran против AOL”. Компания-провайдер “AOL” преследовалась в судебном порядке за размещенное третьим лицом рекламное сообщение. Суд постановил, что эффект от этого дела был направлен на создание “иммунитета к любой причине случая, который мог бы сделать провайдера ответственным за информацию, размещенную третьим лицом, любым пользователем Интер-

нета”. Суд также постановил, что все утверждения, направленные на толкование роли провайдера как издателя информации, должны быть запрещены.

На практике эффект от этого может быть таким, что основанные в США провайдеры, “выращенные” под защитой Акта о защите систем телекоммуникаций, не смогут оценить, что преследование их за клевету во всем мире гораздо сильнее, чем дома. Также провайдер может быть прощенным за неспособность осознать, что одна публикация может привести к многочисленным искам, судебным процессам по всему миру. Мистер Godfrey подал много исков, которые уже принесли ему \$10000, в соответствии с решением суда, от пользовательской группы “Australian PC” и другие победы – над New Zealand Telecom и виртуальной торговой компанией “Toronto Star” [2].

Кроме того, провайдеры – поставщики аукционных и биржевых услуг, содействующие продаже товаров и услуг, могут, при отсутствии жесткого самоконтроля, обнаружить, что они содействуют продаже незаконной продукции. Например, американский провайдер Yahoo! столкнулся с официальными протоколами японской компании, производящей компьютерные игры Sega и Nintendo, утверждающими, что поддельные игры были проданы на сайте-аукционе Yahoo!. Позднее Международный Союз, выступающий против расизма и антисемитизма, выпустил в Париже протоколы против Yahoo!, утверждающие, что провайдер содействует деятельности виртуальных аукционов, на которых продают нацистские “мелочи”. Во Франции продажа или даже показ вещей, относящихся к нацизму, незаконны.

Таким образом, Интернет может превратить мир в единый рынок, на котором сделки купли-продажи будет сложно отнести к какой-либо одной юрисдикции, прибыль подвергнуть налогообложению, принципы которого установлены для какой-нибудь определенной страны.

Необходимо решить множество вопросов, связанных с препятствиями развитию электронной коммерции. Это, например, проблема электронной подписи. Хотя уже существуют законы об электронной подписи, самой подписи еще не создано, и нет организаций, которые выдавали и проверяли бы электронную под-

пись, следовательно, нет и лицензирования этих организаций.

Очень много вопросов возникает в отношении и налогообложения электронной коммерции. Налогообложение не должно препятствовать электронной торговле, равно как создавать стимул для изменения характера и места осуществления сделок купли-продажи.

Наконец, особенно важно, чтобы стороны, имеющие доступ к персональным данным, были уверены в защищенности этих данных с гарантией сохранения конфиденциальности. Согласно положениям законов об информации и защите информации, должны существовать организации, участвующие в сборе профессиональных данных и передачи их этим лицам, и эти организации должны иметь лицензию на осуществление подобной деятельности, должна контролироваться защита частной информации. Эта сфера должна быть урегулирована достаточно тонко на законодательном уровне, потому что любая информация может быть частной или коммерческой тайной. Однако, открытость информации в электронной коммерции обеспечивает прозрачность деятельности, достаточно надежное осуществление сделок, платежей, отгрузок.

Развитие электронной коммерции вызывает заинтересованность одних и является причиной для беспокойства других, но, кажется, что отдельные страны, вероятно, не смогут

“плыть” против общего течения. Поэтому необходимо создание глобального подхода к регулированию электронной коммерции.

В создании такого подхода может помочь государство, которое не должно препятствовать развитию электронной коммерции. Государственное регулирование электронной коммерции должно сводиться к поддержке и внедрению внутренне согласованной и прозрачной правовой среды для развития данного сектора экономики, созданию необходимой для развития инфраструктуры, помощи в завоевании доверия к электронному рынку потребителей и производителей, вкладывающих средства в область современных Интернет-технологий и электронной коммерции.

Пока такой системы не существует любая компания будет нести риски и возможно значительные потери. Рисков, связанных с нарушением закона, и стратегических рисков можно избежать путем тщательного планирования деятельности.

Литература

1. *Nichols P.* Dealing with an eruption of corruption // *Mastering risk.* – 2005.
2. *Hutter B., Power M.* Power and influence in risk regulation // *Mastering risk.* – 2005.
3. *Randall J.* Digital buccaneers caught in a legal web // *Mastering risk.* – 2005.