УДК 339.5

103. РИСКИ ЭЛЕКТРОННОГО БИЗНЕСА И СПОСОБЫ ИХ МИНИМИЗАЦИИ

Кропотин Д. Д.[1], студент гр.173901

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Шинкевич Е. А. – канд. физ.-мат. наук

Аннотация. В данной статье рассматриваются особенности электронного бизнеса, выделяются общие риски, а также риски, связанные с функционированием электронного бизнеса, приведены способы их минимизации. Особое внимание уделяется расчету надежности системы электронного бизнеса как одному из методов снижения риска.

Ключевые слова. электронный бизнес, риски, минимизация риска, надежность системы, функционирование, анализ, технологии, оценка, стратегия

В эпоху цифровизации, охватывающей все сферы человеческой жизни, электронный бизнес становится неотъемлемой составляющей современной экономики.

Сфера электронного бизнеса в настоящее время является одной из наиболее динамично развивающихся в мире. Электронный бизнес не только переопределяет традиционные представления о бизнесе и экономике в целом, но и создает новые способы взаимодействия между бизнесом и потребителем. Виртуальные магазины, онлайн-платформы и цифровые рынки преобразуют вид современной торговли, обеспечивая доступность и удобство для потребителей, а также новые возможности для предпринимателей. Вместе с тем, электронный бизнес несет в себе ряд вызовов, связанных с безопасностью данных, конкуренцией и изменяющимися потребительскими ожиданиями. В контексте этих изменений и вызовов, понимание и анализ сущности электронного бизнеса, умение управлять рисками и минимизировать их становится важным как для бизнеса, так и для всего общества, определяя динамику и перспективы развития современной экономики.

Существует множество подходов к определению понятия «электронный бизнес». Одно из определений электронного бизнеса, которое отражает его суть, звучит следующим образом:

Электронный бизнес – это совокупность различных бизнес-процессов, в которых использование сети Интернет, а также связанных с ней телекоммуникационных сетей, информационных и компьютерных технологий является необходимым условием для организации, осуществления и обеспечения одной или сразу нескольких стадий предпринимательской деятельности [1]. Он должен удовлетворять следующим требованиям:

- информационная природа продукта;
- закупка и продажа должна осуществляться в цифровом виде по интернет-каналам;
- отсутствие традиционных производственных активов;
- отсутствие потребности в торговых и офисных площадях;
- организация рекламных кампаний только в Интернете;
- осуществление закупок товара у поставщиков посредством сети Интернет [2].

Опыт ведущих международных компаний убедительно доказывает, что стабильность развития бизнеса и повышение эффективности управления невозможны без активного использования риск-менеджмента как составной части системы управления компанией вне зависимости от ее масштабов и специфики производства или предоставления услуг.

Система риск-менеджмента (система управления рисками) направлена на достижение необходимого баланса между получением прибыли и сокращением убытков предпринимательской деятельности и призвана стать составной частью системы менеджмента организации, т.е. должна быть интегрирована в общую политику компании, ее бизнес-планы и деятельность. Только при выполнении этого условия применение системы риск-менеджмента является эффективным.

Любая деятельность связана с рисками. Риск — соотношение вероятности возникновения рисковых ситуаций и их возможных последствий. Реализация риска приводит к отклонению фактических результатов деятельности от запланированных. Теория риск-менеджмента рассматривает риск как с позиции негативных отклонений фактических результатов деятельности от запланированных, так и со стороны ее возможных позитивных последствий. В том случае, если рисковое событие приводит к негативным последствиям, управление рисками направлено на гарантированное уменьшение нежелательного отклонения, а в случае, если рисковое событие приводит к позитивным последствиям, инструментарий риск-менеджмента позволяет управлять потенциальной выгодой, возникающей в результате рисковой ситуации.

Выделяют множество различных классификаций рисков, которые, как правило, классифицируются по времени возникновения, основным факторам возникновения, характеру учета, характеру последствий, сфере возникновения и другим критериям.

При классификации по времени возникновения выделяют ретроспективные, текущие и перспективные риски, по факторам возникновения риски подразделяются на политические и экономические (коммерческие).

По характеру учета выделяют внешние (риски, непосредственно не связанные с деятельностью предприятия или его контактной аудиторией) и внутренние (риски, обусловленные деятельностью самого предприятия и его контактной аудиторией) риски.

По характеру последствий риски подразделяются на чистые и спекулятивные. Чистые риски практически всегда несут в себе потери для предпринимательской деятельности, а спекулятивные риски могут приносить как потери, так и дополнительную прибыль для предпринимателя по отношению к ожидаемому результату.

По сфере возникновения выделяют производственный, коммерческий, финансовый риски, а также риск страхования.

Производственный риск связан с невыполнением предприятием своих планов и обязательств по производству продукции, товаров, услуг, других видов производственной деятельности.

Коммерческий риск возникает в процессе реализации товаров и услуг, произведенных или закупленных предпринимателем.

Финансовый риск связан с возможностью невыполнения фирмой своих финансовых обязательств. К причинам финансового риска относят обесценивание инвестиционно-финансового портфеля из-за изменения валютных курсов, неосуществление платежей, войны, беспорядки, катастрофы и т.д.

Страховой риск – риск наступления предусмотренного условиями страхования события, в результате чего страховщик обязан выплатить страховое возмещение (страховую сумму). Основными причинами страхового риска являются неправильно определенные страховые тарифы, азартная методология страхователя, войны, беспорядки, катастрофы и прочее.

Все виды рисков взаимосвязаны, поэтому изменение одного вида риска вызывает изменение большинства остальных, в связи с чем затрудняется анализ и систематизация рисков.

Однако в контексте электронного бизнеса можно также говорить о вероятности возникновения других рисков, связанных с использованием банковских карт (киберпреступность, технические неполадки и пр.). Кроме того, изменения в законодательстве также может оказать значительное воздействие на деятельность компании в электронной среде.

Стоит отметить, что в электронной коммерции по банковским картам осуществляется подавляющая часть всех операций (в среднем около 90% от общего числа операций), а также банковские карты несут в себе существенно больший риск по сравнению с другими видами оплаты. В этом случае риск понимается как событие, которое влечет за собой негативные последствия, выражающиеся в той или иной форме. Схема основных рисков электронного бизнеса представлена на рисунке 1.

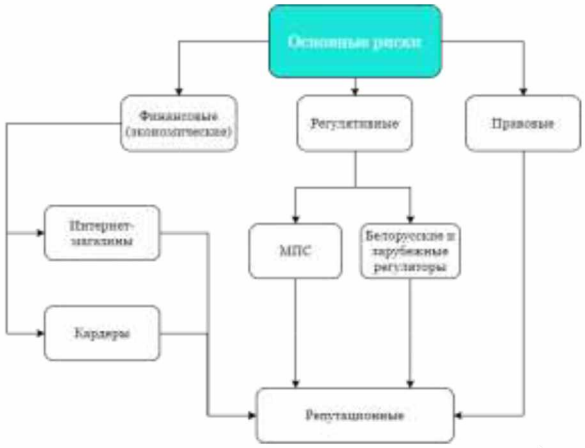

Рисунок 1 – Схема основных рисков электронного бизнеса

Рассмотрим виды рисков электронного бизнеса:

Финансовый риск связан с тем, что каждый участник международной платежной системы (МПС) не застрахован от мошеннических действий со стороны интернет-магазинов и кардеров. Кардером называют преступника, занимающегося мошенничеством с платежными картами. Держатель банковской карты может оспорить операцию, совершенную по его карте, в своем банке, а причина, по

которой оспаривается та или иная операция, может быть практически любой. Финансовый риск исходит как от самого интернет-магазина, так и со стороны кардеров. Именно поэтому в правилах МПС есть специальный раздел, претензионной работе, где описаны различные коды опротестований, под которые подходит практически любая ситуация, от недоставки товара до мошеннической операции. Дальнейший ход событий будет зависеть от грамотного анализа ситуации эквайером и полноты предоставленных документов интернет-магазином.

К регулятивным рискам относятся все риски, связанные с возможными последствиями от действий регуляторов внутри страны и зарубежных регуляторов этого рынка. Точное количество регуляторов и полноту их влияния описать для всех не предоставляется возможным, так как здесь все зависит от того, какой именно участник МПС и каким образом организован бизнес-процесс. К зарубежным регуляторам относят международные платежные системы. Весь процесс оплаты банковскими картами детально описан и четко соответствует правилам МПС. Любое отклонение от правил влечет за собой не только финансовые потери, но и в некоторых случаях дискредитацию как участника МПС с запретом заниматься бизнесом, связанным с банковскими картами.

Под правовыми понимают риски, связанные с судебными тяжбами и разбирательствами.

Репутационные риски аккумулируют в себе все негативные исходы по любым видам рисков. Согласно статистике, потери банков от мошеннических операций злоумышленников с картами в разы ниже потерь от невозврата кредитов заемщиками. Но при этом мошеннические операции подрывают репутацию банка и снижают доверие клиентов к банковской карте как у удобному и безопасному финансовому инструменты.

Как упоминалось ранее, все риски часто пересекаются друг с другом, и поэтому сказать точно, что именно этот риск относится к какой-либо из групп достаточно затруднительно.

Примерами финансовых рисков со стороны кардеров являются отмывание и вывод средств, использование большого количества скомпрометированных карт, а также friendly-fraud (мошеннический возврат средств).

К рискам со стороны МПС можно отнести штрафы (за превышение уровня пороговых значений по заявленным мошенническим транзакциям, уровня опротестованных операций, за BRAM, т.н. запрещенную деятельност, неправильно оформленную деятельность), а также финансовые потери sanon-compliance (несоответствие любым правилам МПС, в результате которых другие участники рынка понесли убытки).

Примерами рисков, возникающих из-за интернет-магазинов, являются прием платежей с последующим исчезновением, обман пользователей, замена заявленной деятельности иной, замена заявленной деятельности на незаконную, а также осуществление требующей лицензирования деятельности без наличия соответствующих лицензий и (или) разрешений.

Так как помимо основных рисков у электронного бизнеса выделяют специфические риски, представляется целесообразным выделить следующие группы угроз:

1. Вирусы и вредоносные программы;
2. Хакерские атаки;
3. Мошенничества с использованием различных средств передачи данных;
4. Выход из строя устройств, обеспечивающих работу участников электронной коммерции.

Первые две группы угроз вполне могут быть отправной точкой для мошенничества с использованием различных средств передачи данных (наиболее значимой группы), поскольку времена написания «шуточных» вирусов и хакерских атак развлекательного характера постепенно уходят в прошлое и основной целью девиантных субъектов компьютерного мира становится обогащение с использованием не слишком законных методов [3].

К способам минимизации рисков электронного бизнеса различного вида относят:

1. Мониторинг всех операций участников платежного процесса;
2. Создание антифрод-системы (оценки финансовых транзакций в Интернете) и ее постоянная оптимизация;
3. Дублирование некоторых критических лимитов и ограничений, работающих независимо друг от друга;
4. Правильное построение отношений с интернет-магазинами, оказание им консультационной и иной поддержки;
5. Проверка интернет-магазинов при подключении к платежной системе с целью соблюдения всех требований законодательства, а также правил МПС. Периодическая их перепроверка;
6. Анализ невыявленных мошеннических операций, ведение статистики на постоянной основе по мошенническим и опротестованным операциям;
7. Минимизация рисков выхода устройств из строя.

Рассмотрим расчет надежности системы электронного бизнеса как способ минимизации риска.

В первую очередь необходимо составить схему работы такой системы. Разработанная схема работы основной части системы электронного бизнеса представлена на рисунке 2.

Как видно на рисунке 2, система включает в себя 9 элементов с разным типом соединения. Предположим, что вероятности отказа (выхода их строя) этих блоков, следующие: для основного сервера (блок 1) – p1 = 0,01; для серверов базы данных – p2 = 0,09; p3 = 0,07; p4 = 0,08; для маршрутизаторов: p5 = 0,05; p6 = 0,04; для коммутатора – p7 = 0,01; для балансировщиков нагрузки – p8 = 0,07; p9 = 0,06.

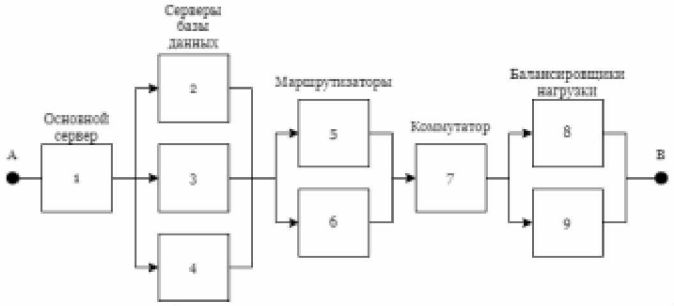

Рисунок 2 – Схема работы основной части системы электронного бизнеса

Далее необходимо рассчитать надежность данной системы. Для расчетов было использовано универсальное программное средство Excel из пакета Microsoft Office.

Предварительно была составлена таблица со значениями по каждому блоку и их вероятностями. Часть таблицы представлена на рисунке 3.

x1	p1	x2	p2	x3	p3	x4	p4	x5	p5	x6	p6
0	0,99	0	0,91	0	0,93	0	0,92	0	0,95	0	0,96
1	0,01	1	0,09	1	0,07	1	0,08	1	0,05	1	0,04

Рисунок 3 – Вероятности работоспособности элементов системы

Далее необходимо сгенерировать значения. Было сгенерировано по 1000 значений для каждой из случайных величин согласно заранее определенным вероятностям. Затем в столбец Y необходимо ввести формулу для расчета работоспособности системы. Из схемы, представленной на рисунке 2 видно, что наша система полностью выйдет из строя при следующих исходах: отказ основного сервера (блок 1), отказ всех серверов базы данных (блоки 2, 3, 4), выход из строя всех маршрутизаторов (блоки 5, 6), отказ коммутатора (блок 7), выход из строя всех балансировщиков нагрузки (блоки 8, 9).

В результате вычислений число выходов системы из строя составило 23 раза из 1000. Часть результата генерации и расчета значения работоспособности системы представлена на рисунке 4.

x1	x2	x3	x4	x5	x6	x7	x8	x9	y
0	0	0	0	0	0	1	0	0	1
0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	1	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

Рисунок 4 – Генерация значений работы системы

Затем определим возможность отказа системы, учитывая все ситуации, и вычислим вероятность отказа системы аналитическим методом расчета надежности по формуле 1:

$$Q = p_1 + p_2 p_3 p_4 (1 - p_1) + p_5 p_6 \left(1 - p_1 - p_2 p_3 p_4 (1 - p_1)\right) + p_7 \Big(1 - p_1 - p_2 p_3 p_4 (1 - p_1) - p_5 p_6 \left(1 - p_1 - p_2 p_3 p_4 (1 - p_1)\right)\Big) + p_8 p_9 (1 - p_1 - p_2 p_3 p_4 (1 - p_1) - p_5 p_6 \left(1 - p_1 - p_2 p_3 p_4 (1 - p_1)\right) - p_7 \left(1 - p_1 - p_2 p_3 p_4 (1 - p_1) - p_5 p_6 \left(1 - p_1 - p_2 p_3 p_4 (1 - p_1)\right)\right)\Big), \quad (1)$$

где p_n – вероятность выхода из строя n-го блока системы.

Значение вероятности отказа системы, рассчитанное по формуле 1, составило 0,02646. Также рассчитаем значение вероятности отказа системы методом статистического расчета надежности по формуле 2:

$$\hat{Q} = \frac{N_{\text{отк}}}{N}, \tag{2}$$

где $N_{\text{отк}}$ – число наблюдаемых отказов системы, N – общее число наблюдений.

Значение вероятности отказа системы, рассчитанное по формуле 2, составило 0,023. Стоит отметить, что трудоемкость расчета, выражаемая числом опытов при использовании метода статического моделирования не зависит от N, в то время как при аналитическом расчете она растет как 2 в степени N, где N – число элементов в системе.

Далее рассчитаем значение относительной погрешности (формула 3). Погрешность оценки в соответствии с правилом «трёх сигм» находится с вероятностью 1-0,0027 в пределах:

$$|\Delta| \leq 3\sigma_n = 3\sqrt{\frac{D(y)}{n}} = 3\sqrt{\frac{Q(1-Q)}{n}}, \tag{3}$$

С учетом того, что обычно вероятность отказа системы Q близка к 0, то можно пренебречь множителем (1-Q), близким к единице, а также по этой причине от абсолютной погрешности переходят к относительной. В результате замен и дальнейших преобразований неравенство принимает следующий вид:

$$|\delta| \leq \frac{3}{\sqrt{n_{\text{отк}}}}, \tag{4}$$

Это неравенство позволяет достаточно легко контролировать относительную ошибку в ходе статистического эксперимента по числу наблюдаемых отказов системы. Полученное значение в 0,62254 свидетельствует о том, что рассматриваемая система является достаточно надежной.

Изучение электронного бизнеса и связанных с ним рисков является важным шагом для успешного функционирования предприятий в эпоху цифровизации. В ходе исследования было выявлено, что электронный бизнес представляет собой уникальное направление, характеризующееся высокой динамикой и инновационностью, но также сопряженное с рядом серьезных рисков. Однако, риски электронного бизнеса могут быть эффективно управляемы при помощи систематического анализа и принятия соответствующих мер по их минимизации. Разработка и реализация стратегий по обеспечению безопасности данных, внедрение современных технологий защиты информации, а также контроль и обучение сотрудников в области кибербезопасности играют ключевую роль в снижении рисков и повышении устойчивости электронного бизнеса. Кроме того, методы анализа и расчета надежности системы электронного бизнеса, представленные в работе, позволяют эффективно оценивать риски и управлять ими, повышая уровень доверия как со стороны клиентов, так и партнеров. Таким образом, понимание и применение методов минимизации рисков являются необходимым условием для успешного развития и конкурентоспособности в сфере электронного бизнеса.

Список использованных источников:

1. Грабауров В. А. Электронный бизнес. Учебное пособие. – Минск.: БГЭУ, 2010 – 345 с.

2. Беляцкая, Т. Н. Электронная экономика: теория, методология, системный анализ / Т. Н. Беляцкая. – Минск : Право и экономика, 2017. – 284 с.

3. Волгушева А. А. Электронная коммерция: от идеи до реализации / А. А. Волгушева – Санкт-Петербург : Изд-во СКИФ, 2018. – 221 с.

UDC 339.5

E-BUSINESS RISKS AND WAYS TO MINIMIZE THEM

Krapotsin D. D.

Belarusian State University of Informatics and Radioelectronics1, Minsk, Republic of Belarus

Shinkevich E.A. – PhD in Physics and Mathematics

Annotation. This article examines the features of e-business, highlights common risks, as well as risks associated with the functioning of e-business, and provides ways to minimize them. Special attention is paid to calculating the reliability of an e-business system as one of the methods of reducing risk.

Keywords. e-business, risks, risk minimization, system reliability, operation, analysis, technology