Официальная статистика показывает снижение объемов хищений с банковских карт в российских финансовых институтах, хотя во всем мире тенденция существует прямо противоположная, указывающая на рост объемов.

В 2017 году объем похищенных денежных средств с банковских карт в Великобритании достиг показателя в 1,32 миллиарда долларов, увеличившись по сравнению с предыдущим годом на 10,7%, поэтому по прогнозам экспертов, объемы хищений с банковских карт в Российской Федерации на порядок выше. В 2018 году по самым минимальным подсчетам объем составлял около 8,1 миллиарда рублей. [1, 3, 4]

Неслучайно во всем мире и в российских финансовых институтах в частности, повышают уровень сохранности денежных средств на банковских картах. С одной стороны, начинают использовать более надежные банковские карты – смарт-карты, а с другой стороны пытаются повысить безопасность выдачи денежных средств при использовании банковских карт, используя банкоматы с биометрической системой распознавания клиентов, в которой для идентификации клиента используют 3D сканирование лица клиента.

В заключении можно сделать следующие выводы:

в последние годы во всем мире наблюдается всеобъемлющее проникновение информационно-коммуникационных технологий во все экономические сферы, одним из лидеров цифровой трансформации является финансовый сектор;

одним из направлений внедрения цифровых технологий в финансовых институтах является сфера безналичных расчетов с помощью банковских карт, с ростом объемов операций растут объемы хищений с банковских карт, в 2018 году объемы похищенных денежных средств с банковских карт россиян превысил 8 миллиардов рублей.

1. Потери банков от киберпреступности [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index.php/Статья:Потери_банков_от_киберпреступности (Дата обращения: 03.09.2018).
2. Центробанк: объем хищений с банковских карт снизился в три раза. [Электронный ресурс]. Режим доступа: <https://www.mk.ru/incident/2017/07/28/centrobank-obem-khishheniy-s-bankovskikh-kart-snizilsya-v-tri-raza.html> (Дата обращения: 03.09.2018).
3. Ответственность за кражу средств с банковских карт ужесточена. [Электронный ресурс]. Режим доступа: <http://www.papajurist.ru/news/otvetstvennost-za-krazhu-sredstv-s-bankovskikh-kart-uzhestochena/> (Дата обращения: 03.09.2018).
4. Какие схемы используют при краже денег с карт. [Электронный ресурс]. Режим доступа: <https://rg.ru/2016/08/17/kakie-shemy-ispolzuiut-pri-krazhe-deneg-s-kart.html> (Дата обращения: 03.09.2018).

Ерохин В.В.

Бизнес-консалтинговые риски в области информационных технологий

*ФГАОУ ВО Московский государственный институт международных отношений
(университет) Министерства иностранных дел Российской Федерации
(Россия, Москва)*

doi:10.18411/lj-09-2018-30

idsp: 000001:lj-09-2018-30

Аннотация

Бизнес-консалтинг в области информационных технологий включает комплекс услуг по оптимизации информационной инфраструктуры и системы информационной безопасности организации. В деятельности ИТ-компаний существуют коммерческие риски. Управление рисками в ИТ-консалтинге реализуется на основе методологии риск-менеджмента.

Ключевые слова: бизнес-консалтинг; информационные технологии; управление рисками

В настоящее время в мировом сообществе проходят одновременно две крупные революции: в информационных технологиях и бизнесе, которые осуществляют глубокое взаимодействие друг с другом, обеспечивая прочную поддержку в развитии. Информационные технологии служат эффективным инструментом поддержки современного бизнеса [1, 2, 5].

Важнейшим средством решения управленческих проблем предприятия выступает бизнес-консалтинг. В общем случае проводится диагностика и выявляются проблемы, испытываемые заказчиком, разрабатываются практические рекомендации в виде проекта организационных изменений, осуществляется выбор эффективной стратегии в области информационных технологий, внедряется консалтинговый проект в практику деятельности предприятия.

Бизнес-консалтинг в информационных технологиях включает комплекс услуг по разработке рекомендаций и реализации системы мероприятий по оптимизации информационной инфраструктуры и системы информационной безопасности организации. Выделяют следующие направления:

- услуги по анализу и формированию информационной стратегии заказчика;
- разработка стратегии прикладных компьютерных систем;
- выбор и внедрение информационных систем (ИС);
- предпроектное обследование организации при создании ИС;
- разработка архитектуры корпоративных информационных систем (КИС);
- выбор программных продуктов для КИС;
- внедрение ИС [9].

Преимущественным спросом пользуются отдельные сервисы ИТ-консалтинговых компаний. В ходе анализа соответствия информационной инфраструктуры бизнес-процессам организации выполняется исследование организационной структуры заказчика, внутреннего документооборота, учетной политики, соответствия ИС стратегии развития бизнеса и в результате предлагается внедрение более эффективной ИС, отвечающей бизнес-целям функционирования хозяйствующего субъекта.

При разработке ИТ-концепции происходит согласование бизнес-целей заказчика, существующих рисков, учетной политики и потребности в информационном обеспечении. Использование ИТ-услуг обусловлено уровнем и темпами развития компании-заказчика, ее стратегическими целями, финансовыми ресурсами.

Несмотря на системный кризис экономики рынок ИТ-консалтинговых услуг имеет большие перспективы. Наибольший рост прогнозируется в области системной интеграции, которая предусматривает создание штатно функционирующей, функционально законченной, технически и финансово оптимизированной, управляемой и документированной ИТ-инфраструктуры либо ее отдельных модулей.

Системные интеграторы осуществляют решение комплексных проблем заказчика по эффективному управлению информационными потоками, оптимизации бизнес-процессов с целью создания мощных конкурентных преимуществ.

Выделяют несколько основных направлений системной интеграции:

- помощь в выборе оптимального ИТ-решения и вычислительной платформы;
- внедрение комплексных систем управления компанией;
- построение сетевой инфраструктуры заказчика;
- проектирование кабельных систем;
- внедрение прикладного программного обеспечения;
- поддержка и сопровождение компьютерных систем и др. [2]

Системная интеграция предусматривает реализацию следующих этапов.

На этапе изучения текущей и перспективной потребности заказчика в информационных ресурсах выполняется анализ эффективности деятельности заказчика с

точки зрения информационного обеспечения бизнес-процессов, оцениваются перспективы развития существующих бизнес-процессов и появления новых. Помимо этого, рассматриваются информационные потоки во внутренней среде, а также входящие и исходящие потоки во внешнюю среду. Для каждого потока определяются тип данных, объемы, интенсивность, способы передачи, форма представления информации, оцениваются перспективы развития информационных потоков, возникновение новых и удаление отдельных потоков, выявляются объемы и тенденции роста источников данных, изучаются требования по обеспечению безопасности обработки, хранения и передачи информации во внутренней и внешней среде.

На этапе анализа существующей информационной инфраструктуры оценивается полнота обеспечения бизнес-процессов программными и аппаратными средствами, выявляются морально устаревшие, подлежащие устранению, проводится выбор новых средств, обеспечивающих эффективную поддержку бизнеса, универсальность доступа к информационному обеспечению. В ходе создания проекта замены устаревших систем оцениваются затраты на создание новой системы, надежность и пропускная способность имеющихся каналов связи, внутренних сетей, определяются сроки перехода, включая подготовку персонала.

При создании проекта объединения отдельных систем определяются технологические решения для интеграции каждой системы или группы систем, необходимые программно-аппаратные средства. В дальнейшем осуществляются заказ, поставка и установка оборудования, проводится выбор поставщиков средств системной интеграции, разрабатывается план заказа, поставки и размещения. Реализация планового перехода к новой инфраструктуре предусматривает разработку плана поэтапной реализации ИТ-проекта. В более простых проектах системной интеграции отдельные этапы могут отсутствовать. Например, при внедрении электронного документооборота монтаж аппаратных средств не является обязательным. Крупнейшими системными интеграторами России являются компании Ай-Теко, Ай-Ти, Компьюлинк, ЛАНИТ, КРОК, IBS, R-Style и др.

Взаимосвязанными компонентами транзитивной экономической системы выступают управление и риск. Управление само может выступать мощным источником рискованной ситуации. Предпринимательская деятельность ИТ-компаний в условиях трансформации мировой экономики неразрывно связана с рисками. Риск – это возможность минимизации неблагоприятных экономических ситуаций в ходе реализации инновационных проектов [3]. Риск выполняет стимулирующую и защитную функции. Ему присущи противоречивость, альтернативность, неопределенность [4]. Основными свойствами риска являются всеобщность, системность и динамическая вероятность. Эффективное управление предпринимательским риском в современном бизнесе включает в себя стратегию и тактику риск-менеджмента [5].

В научной литературе присутствуют различные классификации рисков в экономике [3, 4, 5]. Анализ существующих подходов к данному феномену показывает, что авторы не рассматривают риски, имеющие место в деятельности консалтинговых компаний, оказывающих ИТ-услуги. Опираясь на выполненные исследования, мы считаем, что в бизнес-консалтинге в области информационных технологий присутствуют следующие виды предпринимательских рисков:

- по источнику появления: субъективный, обусловленный личностными качествами персонала ИТ-компаний (недостаток опыта, профессионализма, нарушение этики и стандарта профессионального поведения и др.), и объективный, связанный с низким качеством информационного обеспечения при разработке и принятии ИТ-инновации, динамикой внешней среды;

- по этапу реализации ИТ-решения: на этапе принятия решения (ошибки в применении средств и методов обработки информации, в ходе анализа информации, качественных и количественных методов оценки риска и др.), на этапе его реализации (ошибки при реализации ИТ-решения, неожиданные изменения во внешней и внутренней среде и др.);
- по области возникновения: внешний, обусловленный трансформацией транзитивной экономики, и внутренний, связанный с особенностью деятельности ИТ-компании;
- по возможности возмещения: страхуемый, количественно оцененный страховой компанией, и не страхуемый;
- по уровню допустимости: минимальный (возможны потери прибыли до 25%), повышенный (ущерб составляет до 50%, критический (возможен ущерб до 70%) и недопустимый.

Нами установлено, что в бизнес-консалтинге в области информационных технологий присутствуют следующие виды предпринимательских рисков: имущественный, обусловленный вероятными потерями аппаратно-программных средств по причине кражи, диверсий, повреждений, стихийных бедствий и др., производственный, связанный с повреждением используемых физических, аппаратных, программных, криптографических средств, нарушением целостности, доступности, конфиденциальности информации и др., торговый, обусловленный задержкой платежей, отказом от платежа недобросовестных заказчиков и др., финансовый, возникающий в случае потери финансовых ресурсов; инвестиционный, состоящий в обесценении инвестиционно-финансового портфеля ИТ-компании.

Информационной системе консалтинговой компании, оказывающей ИТ-услуги, присущи общесистемные (целостность, устойчивость, синергетика, адаптивность, наблюдаемость, управляемость, открытость, динамичность, безопасность и т.д.), структурные (состав, связность, сложность и др.) и функциональные (результативность, производительность, быстродействие, экономичность и др.) свойства. Информация, используемая при формировании ИТ-решения, по предметной принадлежности может быть разбита на следующие группы: характеристика объекта управления, характеристика внешней среды, характеристика ресурсов, нормативно-справочная информация.

Информационная среда ИТ-компании представляет собой множество взаимосвязанных информационных элементов, обеспечивающих сбор, обработку, хранение и передачу информации с целью достижения конкурентных преимуществ. Важнейшими информационными элементами выступают сотрудники, информационные ресурсы, компьютерные системы, аппаратные, программные, криптографические средства, непосредственно участвующие в информационном процессе либо обеспечивающие его эффективное функционирование. Внешняя информационная среда консалтинговой компании представлена объектами, субъектами, процессами и явлениями внешнего окружения, влияющими на элементы ее внутренней информационной среды. В ходе реализации случайных негативных событий во внутренней или во внешней информационной среде ИТ-компании может произойти нарушение целостности, доступности, конфиденциальности бизнес-информации.

Учитывая стратегическое значение информации в условиях когнитивной экономики, можно утверждать, что в предпринимательских рисках ИТ-компании присутствуют элементы информационного риска. Таким образом, методология риск-менеджмента может быть эффективно применена при управлении в том числе информационными рисками бизнес-консалтинга в области информационных технологий.

Рассмотрим основную задачу ИТ-компании по прогнозированию и выделению циклических изменений во временном ряде финансово-экономических показателей, связанных с управлением рисками. Решение задачи синтеза управления рисками, в первую очередь основывается на прогнозе различных финансовых показателей.

Спектральная плотность в отличие от ковариационной функции менее употребительна в практических задачах, однако она весьма полезна для анализа сезонности и периодичности процесса. В этом случае необходимо использовать оценку Барлета, которая основана на выборе спектрального окна $WN(\lambda)=aNB(aN\lambda)$, при этом:

$$a_N \rightarrow \infty, \quad \frac{a_N}{N} \rightarrow 0, \quad N \rightarrow \infty, \quad B(\lambda) = \frac{1}{2\pi} \left| \frac{\sin^2 \frac{\lambda}{4}}{\frac{\lambda}{2}} \right|.$$

В связи с полученными результатами анализа, решается задача прогнозирования временного ряда. Для диагностики динамической сезонной волны необходимо разделить изменения волны и изменения тренда так, чтобы динамическая волна и тренд были определены однозначно. Для определения динамического сезонного цикла необходимо выделить на интервале наблюдения K целых периодов длительностью T .

Исходную реализацию $y(t)$ и динамические сезонные циклы $s(t)$ на интервале $\{0, KT\}$ представляют в виде набора функций одного периода:

$$y_k(t) = y(t + (k-1)T),$$

$$s_k(t) = s(t + (k-1)T),$$

$$k = 1, \dots, K.$$

Каждому периоду соответствует своя часть исходной реализации и свой сезонный цикл.

В качестве метода исследования структурных зависимостей рисков используют факторный анализ и нечеткие множества. Каноническая модель факторного анализа выглядит следующим образом: $X_i = F_1 q_{i1} + F_2 q_{i2} + \dots + F_m q_{im} + \varepsilon_{ij}$, $i \in 1..m$, где $X_1, \dots, X_m$ – анализируемые признаки; общие факторы $F_1, \dots, F_k$ – некоррелированные случайные величины, имеющие математическое ожидание 0 и дисперсию 1; характерные факторы ε_i – некоррелированные случайные величины, имеющие математическое ожидание 0 и неизвестные дисперсии v_i , величины F_j и ε_i некоррелированы, q_{ij} факторные нагрузки, представляющие ковариацию между признаками и факторами.

При получении факторного решения производят ортогональное или косоугольное преобразование факторов для того, чтобы содержательно интерпретировать новые факторы. Это позволяет уменьшить сложность параметров, влияющих на факторы, и перейти к простым структурам (если можно подобрать систему координат таким образом, чтобы каждый вектор лежал в одной или более гиперплоскостях, то полученная система называется простой структурой). Используются следующие методы вращения факторов:

- «квартимакс» метод максимизирующий дисперсию факторов
- «варимакс» метод максимизирующий величину:
- модифицированный “варимакс” метод позволяющий получить решение близкое к простой структуре.

Процесс управления рисками в ИТ-консалтинге, опирающийся на системный и синергетический подходы, содержит ряд этапов: выявление риска; оценка риска; выбор методов управления риском; применение системы мер по управлению риском; оценка результатов деятельности.

Процессная модель управления рисками в бизнес-консалтинге в области информационных технологий включает планирование, реализацию, проверку, действие. На этапе планирования определяются политика и методология управления рисками ИТ-компаний, проводится качественная и количественная оценка рисков, включающая инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности противодействия потенциальным угрозам, возможного ущерба.

На этапе реализации осуществляется обработка предпринимательских рисков, используются методы и средства, снижающие их негативное воздействие на финансовые результаты. Руководством ИТ-компаний принимается одно из четырех решений по каждому установленному риску: игнорировать, избежать, передать внешней стороне, минимизировать. На этапе проверки контролируются изменения факторов риска. На этапе действия по результатам мониторинга выполняются различные корректирующие действия.

В мировой практике существует ряд общепризнанных стандартов и подходов к обеспечению информационной безопасности ИТ-компаний и управлению ее рисками. Наибольшую известность получили такие международные спецификации и стандарты как ISO 17799-2002 (BS 7799), ISO 27001, GAO, FISCAM, SCIP, COBIT, SAC, COSO и др. В настоящее время разработаны программные комплексы анализа и контроля информационных рисков: CRAMM (компания InsightConsulting, www.insight.co.uk), RiskWatch (компания RiskWatch, www.riskwatch.com), ГРИФ (компания DigitalSecurity, www.dsec.ru). [1, 4, 5]

1. Антохонова И.В., Полухина О.А. Об использовании информационных технологий и их влиянии на развитие экономики России // Вопросы статистики. – 2010. – №5. – С. 61-67.
2. Аверченков, В.И. Системы организационного управления / В.И. Аверченков, В.В. Ерохин. – Брянск: БГТУ, 2006. – 208 с.
3. Erokhin, V.V. Verification of Computer Systems of Commercial Bank / V.V. Erokhin, V.V. Fetshchenko, I.S. Panina, N.P. Kazimirova, S.P. Novikov, A.V. Novikova // International Journal of Applied Business and Economic Research. – 2017. – Т. 15. – № 12. – С. 297-306.
4. Erokhin, V.V. Controlling access to the information and software in a commercial bank / V.V. Erokhin, G.A. Kulikova, N.V. Mudrova, E.M. Shadoba, V.A. Romanov, N.V. Podobai // International Journal of Applied Business and Economic Research. – 2017. – Т. 15. – № 12. – С. 159-170.
5. Ерохин, В.В. Безопасность информационных систем / В.В. Ерохин, Д.А. Погonyшева, И.Г. Степченко. – Москва: ФЛИНТА, Наука, 2015. – 184 с.

Купцова П.А., Касьянова В.А.

Природа ссудного процента

Кубанский государственный аграрный университет имени И.Т. Трубилина

doi:10.18411/lj-09-2018-31

idsp: 000001:lj-09-2018-31

Аннотация

В данной статье мы рассмотрим понятие ссудного процента, его формы, историю возникновения и расскажем, как использовать данную информацию. Умение правильно распоряжаться данными знаниями будет рационально и полезно для многих студентов.

Ключевые слова: ссудный процент, денежная плата, банк, ссуда, процент, процентная ставка, государство.

Ссудный процент...а что же это такое? Как этим пользоваться? Откуда он появился? В этой статье вы найдете ответы на все эти вопросы. Итак, начнем с того, что само понятие ссуда говорит о передаче денежных средств во временное пользование,