10.7. ИТ-АУТСОРСИНГ: ОЦЕНКА РИСКОВ БАНКОВСКОГО СЕКТОРА

Зубков В.В., аспирант кафедры
экономики управления ВГНА Минфина России

Всероссийская Государственная Налоговая Академия Минфина РФ

Рассматривается тенденция перехода на аутсорсинговую модель эксплуатации информационных систем. Приводится перечень возникающих в связи с этим рисков в банковском секторе; проводится анализ средств и методов управления этими рисками в сравнении моделей самостоятельной и сторонней эксплуатации ИТ-систем. В завершении дается ответ на актуальный вопрос о степени серьезности и оправданности рисков, возникающих при участии в аутсорсинговых проектах.

Необходимость ИТ-аутсорсинга каждый банк, оценивает, безусловно, исходя из собственных особенностей, однако если у потенциального заказчика еще нет опыта аутсорсинговых проектов, то, прежде всего, он сталкивается с двумя вопросами. Первый состоит в самой сути аутсорсинга – «что это?». В Российской Федерации особенно остро этот вопрос стоял в начале 2000-х гг. В этом отношении значительная часть бизнеса достигла понимания уже в середине прошлого десятилетия. Однако второй вопрос – каковы последствия аутсорсинга? – все еще актуален. Какие риски принимает на себя компания-заказчик? Насколько они серьезны, и оправданы ли?

В рамках данной статьи будет разобрана реализация функции эксплуатации ИТ-системы банка силами сторонней организации. Риски, связанные с аутсорсингом, весьма разнообразны и индивидуальны – они непосредственно зависят от особенностей конкретного бизнеса и условий деятельности компании, в данном случае банка:

- потеря контроля над эксплуатационными процессами;
- рост угроз в области информационной безопасности;
- опасения сотрудников относительно их карьерных перспектив;
- рост затрат на эксплуатацию ИТ-системы;
- зависимость от поставщика ИТ-услуг.

Передавая обслуживание корпоративной системы в руки специалистов другой компании, клиент теряет контроль над персоналом.Кроме того, если эксплуатация системы осуществляется удаленно, происходит потеря контроля над эксплуатационными процессами – возникают опасения за качество услуг, поскольку ответственность за эффективную работу бизнес-систем лежит на ИТ-директоре компании-клиента.

Если раньше в системе могли часто возникать сбои, а обслуживание требовало постоянного поиска квалифицированных кадров, то теперь эти проблемы исчезли, но появились новые. Необходимо ответить на вопрос, с какими из них ведение бизнеса является более комфортным и эффективным. Минимизация данной группы рисков в случае самостоятельной эксплуатации ИТ-систем требует увеличения расходов: постоянное повышение квалификации персонала и, как следствие, рост заработной платы.

Если же банк акцентирует внимание не на контроле работы технического персонала, а на качестве работы ИТ-систем, то механизм управления и контроля исполнителя через условия соглашения об уровне обслуживания (ServiceLevelAgreement, SLA) является очень эффективным инструментом. Суть такого подхода заключается в разработке регламента работы системы и проведении регулярных проверок практики эксплуатации систем на соответствие регламенту. Данный подход описан в ITIL (библиотека документов, содержащих лучшие из применяемых на практике способов организации работы ИТ-организаций и подразделений, разработанная Правительственным агентством коммерции Великобритании еще в 1980-х гг.).

Рост угроз в области информационной безопасности вызывает наибольшие опасения именно в банковском секторе и является распространенным аргументом против ИТ-аутсорсинга. Контроль сотрудников сторонней организации обычно представляется невыполнимой задачей.

Однако по данным исследований 60% утечек конфиденциальных данных происходит по вине собственного персонала бизнес-подразделений.

Если, как в предыдущем примере, сопоставить риски, возникающие при самостоятельной эксплуатации ИТ-систем с рисками в случае привлечения компании-аутсорсера и оценить способы их минимизации, то мы увидим, что повышение уровня информационной безопасности в обоих случаях требует одного и того же комплекса мероприятий – внедрения систем защиты информации от несанкционированного доступа. Однако компания-аутсорсер сможет распределить стоимость такой системы по нескольким проектам, сделав ее использование заказчиками менее затратным, в то время как банк будет вынужден оплатить полную стоимость. Для гарантии неразглашения конфиденциальных данных аутсорсеры подписывают соглашение о конфиденциальности и разрабатывают совместно с заказчиком политику информационной безопасности, согласованную обеими сторонами. Также существует практика введения регулярного контроля и отчетности по исполнению политики информационной безопасности.

Еще пять лет назад 80% потенциальных аутсорсинговых проектов заканчивали свое существование, столкнувшись с проблемой обеспечения конфиденциальности информации. Сейчас ситуация кардинально изменилась. Если банк не испытывает реальной потребности в переходе к аутсорсинговой модели, а просто исследует возможные варианты повышения эффективности бизнеса – вопрос организации системы информационной безопасности с максимально возможным уровнем является определяющим при принятии решения. Если же сложилась ситуация, угрожающая развитию основного бизнеса, требования к уровню информационной безопасности становятся более разумными и осуществимыми.

Еще одна группа рассматриваемых рисков – это возможность возникновения опасений сотрудников банка относительно их карьерных перспектив. ИТ-руководителей можно разделить на две группы: «стратегов» и «тактиков». Первых в основном интересуют показатели качества и эффективности работы ИТ-подразделения, вопросы развития ИТ-систем. Такие люди, как правило, тесно взаимодействуют с бизнес-подразделениями, выясняя, что необходимо бизнесу и, исходя из этого, ставят задачи ИТ-службе. Они занимаются организацией внедрения новых систем и решений. Вторые в большей степени заинтересованы в качественном выполнении текущей работы. Такому человеку необходимо понимать, кто в его подразделении чем занимается сейчас и чем будет заниматься завтра.

Перспектива вывода эксплуатации на аутсорсинг, как правило, находит поддержку среди «стратегов» поскольку развязывает им руки, освобождает от рутины, снижает затраты времени на управление персоналом и тем самым позволяет сосредоточить усилия на основной задаче ИТ-руководителя – формировании стратегии развития ИТ в компании и управлении этим развитием. Качество же эксплуатации систем можно контролировать через сервисный контракт.

«Тактик», как правило, становится в оппозицию к проекту, опасаясь, что с появлением аутсорсера его роль и значение в компании уменьшатся. Следует отметить, что подобные опасения не лишены оснований.

К сожалению, в нашей стране сложилось ошибочное представление о том, что переход на аутсорсинг сразу должен приводить к экономии. Однако первый же опыт аутсорсинговых проектов показал, что часто это не так. Это привело к распространению нового заблуждения: «аутсорсинг дорог и может применяться только корпорациями».

В условиях высокой культуры ведения бизнеса многие ключевые аспекты управления являются обязательными по умолчанию, поэтому говорят о них нечасто. Например, это консолидированный бюджет на ИТ или фиксированное и измеряемое качество работы ИТ-системы. В таких условиях в подавляющем большинстве случаев аутсорсер гарантирует снижение эксплуатационных издержек при переходе на аут-

сорсинг за счет оптимально построенных процессов эксплуатации, использования ресурсов в разделяемом режиме, налаженных рабочих связей с поставщиками оборудования и программного обеспечения и многих других преимуществ которыми не обладает банк. Если же у руководства банка нет точной информации о реальных расходах на содержание и развитие ИТ, потому что эти затраты разнесены по многим статьям бюджетов разных подразделений, то остается вопросом, что из существующего ИТ-хозяйства является действительно необходимым, а что было пущено на «самотек» и не приносит реальной пользы. В таких условиях эффект экономии, разумеется, заметен не будет, напротив, может наблюдаться рост затрат на эксплуатацию ИТ-системы. Дело в том, что аутсорсер, в отличие от внутренней службы ИТ компании-клиента, не может работать на уровне качества ниже определенной планки, поскольку связан контрактными обязательствами и вытекающей из них финансовой ответственностью за результат своей работы. Поэтому, если сравнить стоимость обслуживания системы, с одной стороны, силами местных инженеров, а с другой стороны, силами специализированной сервисной организации, заключающей гарантийные контракты с производителями обслуживаемого оборудования на поставку запчастей, имеющую фиксированные интервалы времени реакции, указанные в контракте, то очевидно, что стоимость обслуживания во втором случае будет выше. Аутсорсинг дешевле собственной эксплуатации только при одинаковом уровне гарантированного качества работы обслуживаемой системы. Риски роста затрат в случае самостоятельной эксплуатации минимизируются путем введения постоянно действующего механизма борьбы с издержками, планирования ресурсов. В случае же участия сторонней организации минимизация рисков требует лишь консолидации бюджета на эксплуатацию ИТ-инфраструктуры.

У многих потенциальных заказчиков риски возможного ущерба бизнеса от простоя ИТ-сервисов настолько малы, что тратить деньги на повышение их качества неразумно. Если когда-либо ситуация изменится, потенциальный заказчик вернется к этой теме, но уже на другом уровне понимания проблемы. В банковском же секторе цена сбоев настолько высока, что грозит не только санкциями со стороны контролирующих организаций, но и ухудшением отношений с клиентами, а затем и репутации, и, как следствие, потерей доли рынка.

Если успешное функционирование предприятия целиком зависит от поставщика ИТ-услуг, то последний неизбежно начнет диктовать свои условия. В этот момент может возникнуть зависимость от поставщика ИТ-услуг. Следует иметь это в виду при построении отношений с поставщиками ИТ-услуг и планировании будущих проектов. Чтобы свести подобный риск к минимуму, стоит следовать двум основным принципам: постоянный контроль за аутсорсером и обеспечение его «прозрачности» перед потребителем услуги. Поэтому ключевыми разделами аутсорсингового контракта являются, например, «Отчетность», «Эксплуатационные регламенты», «Измерение качества». К сожалению, не всегда есть возможность в момент заключения контракта приложить к нему эксплуатационные регламенты. Это документы, детали которых отражают реальные свойства обслуживаемой системы и чтобы учесть их в рабочих процессах и создать действительно работающие инструкции для администраторов, требуется, как правило, несколько месяцев работы в штатном режиме. Однако даже в этом случае требование их обязательного наличия должно иметь место. Наличие эксплуатационных регламентов и регулярная проверка их исполнения снижает степень зависимости компании от поставщика ИТ-услуг – при расторжении контракта новому сервисному партнеру будет проще наладить эксплуатацию системы.

Если контракт на передачу системы в аутсорсинг разбивается на несколько частей (этапов), то поставщик может снизить цену первой части, чтобы, добившись заключения контракта, существенно завысить цену исполнения остальной части работ. Для защиты от этого существует механизм метрик, при использовании которого для определения объема обслуживания предлагаются численные параметры, характеризующие величину и сложность обслуживаемой системы. Эти метрики фиксируются в контракте, что дает возможность контролировать удельную стоимость работ вне зависимости от величины или сложности системы и отдельных ее компонентов.

Разумеется, крайне важную роль в этом отношении играет выбор поставщика услуг. Проекты ИТ-аутсорсинга с ведущими системными интеграторами предполагают сотрудничество на уровне равноправного партнерства, в котором каждый его участник понимает и уважает интересы другой стороны.

Таким образом, риски, возникающие при передаче банком эксплуатации ИТ-систем сторонней компании, являются управляемыми и оправданными, но только в случае высокого уровня организации ИТ-инфраструктуры банка. Сейчас вряд ли найдется банк, не прибегающий к помощи системных интеграторов, однако во многих случаях банки становятся жертвами недобросовестности поставщика услуг или собственной недальновидности. Поэтому принимать решения об участии в аутсорсинговых проектах, а также говорить о пользе этого, можно только после разработки и утверждения качественной долгосрочной ИТ-стратегии.

Литература

1. Банковский аутсорсинг: теоретические и практические аспекты [Текст] : учеб. пособие / С.А. Волченков, Т.В. Никитина ; под ред. Г.Н. Белоглазовой. – СПб. : Изд-во Санкт-Петербургского гос. ун-та экономики и финансов, 2010. – 144 с.
2. Готтшальк П. ИТ-аутсорсинг. Построение взаимовыгодного сотрудничества [Текст] / П. Готтшальк, Х. Солли-Сетер. – М. : Альпина Бизнес Букс, 2007. – 394 с.
3. Зинкевич В. Информационные риски: анализ и количественная оценка [Текст] / В. Зинкевич, Д. Штатов // Бухгалтерия и банки. – 2007. – №2.
4. Ингланд Р. Овладевая ITIL. Скептическое руководство для ответственных лиц [Текст] / Р. Ингланд. – М. : Livebook / Гаятри, 2011. – 200 с.

Ключевые слова

ИТ-аутсорсинг; банковский риск-менеджмент; банковские информационные системы; аутсорсинговая модель; ИТ-инфраструктура.

Зубков Виктор Васильевич
E-mail: vvzubkov@gmail.com

РЕЦЕНЗИЯ

Статья Зубкова В.В. посвящена определению основных рисков, возникающих при передаче эксплуатационной функции информационной системы банка на аутсорсинг, и способов управления этими рисками.

Актуальность данной статьи не вызывает сомнения, поскольку информационное обеспечение современного бизнеса, в том числе банковского сектора, играет важнейшую роль в повышении эффективности деятельности, а расходы на внедрение и последующую эксплуатацию информационных систем крупными компаниями составляют значительную статью расходов. Сокращение эксплуатационных расходов с одновременным повышением качества эксплуатации является важнейшее задачей для любой крупной компании.

Автором проанализированы основные группы рисков, возникающих при участии банка в проектах ИТ-аутсорсинга, в сравнении с моделью независимой эксплуатации информационных систем, сопоставлены способы управления рисками для обеих моделей, а также сделаны выводы относительно целесообразности применения ИТ-аутсорсинга в той или иной ситуации.

Научная статья Зубкова В.В. «ИТ-аутсорсинг: оценка рисков банковского сектора» соответствует всем требованиям, предъявляемым к работам такого рода. Данная статья может быть рекомендована к публикации.

Годин А.М., д.э.н., профессор, профессор кафедры экономики управления Всероссийской государственной налоговой академии Министерства финансов РФ

10.7. IT OUTSOURCING: ASSESSING RISKS IN THE BANKING SECTOR

V.V. Zubkov, Post-graduate Student of Chair of Managerial Economics VGNA of the Ministry of Finance of Russia

All-Russian State Tax Academy of the Ministry of Finance of Russia

The tendency of transition to the outsourcing model of information systems maintenance is considered. The list of banking risks arising in this connection is resulted; the analysis of risk management tools and techniques is carried out with comparison of models: independent versus foreign maintenance of IT systems. In end the answer to pressing question about severity and propriety of taking risks of participation in outsourcing projectsis given.

Literature

1. V. Zinkevich. Information Risk: Analysis and Quantification / V. Zinkevich D. Shtatov // Accounting and banking. – 2007. – №2.
2. P.Gottschalk. / IT outsourcing. Building mutually beneficial cooperation / P. Gottschalk and H. Solli-Seter. – Moscow: Alpina Business Books, 2007. – 394 p.
3. Bank Outsourcing: Theoretical and Practical Aspects: Textbook. Manual / SA Volchenkov, T. Nikitina, ed. GN Beloglazova. – Spb. Publishing House of St. Petersburg University of Economics and Finance, 2010. – 144 p.
4. R. England. Owning ITIL: A Skeptical Guide for Decision-makers / R. England. – M.: Livebook/Gayatri, 2011. – 200 p.

Keywords

IT outsourcing; banking risk management; banking information system; outsourcing model; IT infrastructure.