ОПЕРАЦИОННЫЕ РИСКИ И ИТ-ИНФРАСТРУКТУРА БАНКА

OPERATIONAL RISKS AND IT INFRASTRUCTURE BANK

V.V. Zubkov

In article the analysis of the international and domestic experience on management of a bank IT Infrastructure from the point of view of operational risk management is carried out. Examples of the banks using modern approaches to the organization of IT Services, and also an estimation of quality, efficiency and results of work of IT Divisions are resulted.

Keywords: Banking risk management, operating risks, IT-infrastructure.

Зубков Виктор Васильевич
Всероссийская Государственная Налоговая Академия Минфина РФ

Аннотация::
В статье проводится анализ международного и отечественного опыта по управлению банковской ИТ-инфраструктурой с точки зрения операционного риск-менеджмента. Приводятся примеры учреждений банковского сектора, использующих современные подходы к организации ИТ-сервисов, а также оценке качества, эффективности и результатов работы ИТ-подразделений.

Ключевые слова:
Банковский риск-менеджмент, операционные риски, ИТ-инфраструктура.

Информационные технологии в сфере потребительского рынка развиваются крайне активно, регулярно появляются инновационные продукты. Внедрение новых продуктов, в том числе услуг, почти всегда рождает финансовые риски. Их правильная оценка получает большое значение в процессе бизнес-планирования. Особенно эта проблема актуальна для финансовых учреждений, в частности для банковского сектора.

С ростом объемов информации, расширением клиентской базы и введением новых банковских продуктов банки вынуждены пропорционально создавать новые структурные подразделения, расширяя организационную структуру. Зачастую это делается в ущерб качеству обслуживания. Оборудование, производительность которого изначально не была рассчитана на новые потребности банка, не справляется с возрастающей нагрузкой, что повышает частоту сбоев в работе. Подобные сбои могут вызвать серьезные финансовые потери.

Во избежание негативных последствий банковские учреждения активно используют информационные системы, к которым предъявляют довольно высокие требования. Одним из основных критериев выбора таких технологий является высокая производительность и надежность работы. Этим критериям полностью соответствует продукция крупных западных вендоров программного обеспечения, которая используется в большинстве крупных банков, имеющих разветвленную сеть филиалов. Мелкие кредитные и финансовые учреждения чаще используют более доступные аналоги от более мелких, часто местных вендоров. В любом случае, риски, связанные со сбоями IT-инфраструктуры, остаются актуальными всегда и для всех.

Степень операционного риска ("риска бремени") определяется способностью банка предоставлять финансовые услуги, получая прибыль, и контролировать расходы, связанные с предоставлением этих услуг. За рубежом банковское сообщество уделяет вопросам IT-инфраструктуры большое внимание. CIO (Chief Information Officer – ИТ-директор) обычно входят в состав руководящих органов банка и непосредственно участвуют в принятии большинства важных решений. При этом они действительно являются профессионалами в области ИТ, имеют профильное образование и регулярно проходят сертификацию.

В отечественном банковском секторе зачастую недооцениваются "риски бремени", поэтому в таких банках в случае сбоя или остановки компонентов информационной системы существенно замедляется или останавливается операционная деятельность, например, если банк проводит агрессивную экспансию в регионы. При этом рост ИТ-инфраструктуры предварительно не спланирован, и она растет экстенсивно. В этом случае банк сталкивается со значительными трудностями при проведении даже самых простых операций, поскольку программно-аппаратные системы не рассчитаны на нагрузку со стороны дополнительных отделений банка. Если на экране банкомата появляется сообщение о невозможности осуществления связи с процессинговым центром, или специалист отделения заявляет о невозможности проведения операция, значит, банк пренебрегает вопросами развития ИТ-инфраструктуры.

Рост филиальной сети, как правило, сопровождается снижением уровня обслуживания клиентов (снижается скорость обслуживания, доступность сервисов, показатели непрерывности предоставления услуг). При этом расчеты показывают, что бюджет срочного восстановления прежнего уровня эффективности ИТ–инфраструктуры серьезно превышает тот, который был бы затрачен на превентивные меры.

Часто в российских банках отсутствуют стратегии восстановления после сбоя, нет централизованной системы резервного копирования (или ее мощность недостаточна), нет дублирования или резервирования "узких мест" информационной системы, "холодного" или "горячего" аппаратного резерва, нет резервных каналов связи, не внедрены DWH (Data Warehouse – корпоративное хранилище данных).

По результатам независимых исследований, в случае преднамеренных или случайных действий системного администратора, вирусной атаки или аппаратного сбоя только 15% банков могут восстановить операционную деятельность в тот же день. Остальным 85% для восстановления понадобится порядка 4–х дней. Эти проблемы решаются медленно, не только по причине нехватки в банках квалифицированных ИТ–кадров и увеличения общего количества компьютеров на одного ИТ–специалиста, но и ввиду низкой ИТ–грамотности пользователей, что связано с нежеланием регулярно повышать квалификацию своего персонала.

Необходимо особо отметить проблемы, возникающие при слиянии банков. В этом случае затруднен информационный обмен, процессы интеграции информационных систем идут непозволительно медленно, их разнородность затрудняет анализ результатов. В этот период страдает и непрерывность сервиса, а вопросы информационной безопасности, встают на первое место (система защиты информации не функционирует, или ее возможности ограничены).

Сегодняшняя практика показывает, что за риски, связанные с ИТ–архитектурой, как правило, ответственен руководитель департамента информационных технологий банка. Но каковы критерии оценки качества работы этого ИТ–подразделения и, соответственно, его руководителя? У многих банков их не существует. Но, даже если они выработаны, при критичном сбое по вине сотрудников ИТ–подразделений никакие взыскания не компенсируют потерь банка.

Кроме того, в большинстве случаев результат работы ИТ–подразделения банка оценивает сам руководитель этого подразделения. Поэтому в процессах бизнес–планирования и разработки стратегии развития банка должны быть обязательно учтены проблемы ИТ–инфраструктуры. Необходимо понимать, что последствием недооценки рисков, связанных с информационными системами банка, может стать масштабный сбой в ИТ–инфраструктуре, который повлечет за собой остановку операционной деятельности. Однократные финансовые потери при таком развитии событий могут существенно превысить суммарный объем годового ИТ–бюджета банка.

Методы оптимального управления экономическими информационными системами были разработаны достаточно давно. В середине 1980–х годов по заказу Правительства Великобритании была создана методика оптимального и рационального управления ИТ–инфраструктурой. Она планомерно развивалась и превратилась в современную библиотеку управленческих ИТ–решений – ITIL. Несколько позже в США группой ведущих ИТ–экспертов была разработана методика CobIT, которая во многом дополняет библиотеку ITIL в части процедур взаимодействия топ–менеджмента с ИТ–специалистами. Она позволяет сократить информационный барьер между руководством предприятия и ИТ–подразделениями.

За последние пять лет несколько крупных банков СНГ провели серьезную работу по приведению процессов управления рисками, изменениями и функциями в ИТ–подразделениях в соответствие с CobIT и ITIL. Указанные методики успешно работают и в странах СНГ, особенно в тех банках, которые проводили работу по их внедрению при тесном взаимодействии с консалтинговыми компаниями и системными интеграторами. Они показали свою эффективность для решения проблем в информационных системах финансовых предприятий.

Так, например, в одном из крупных государственных банков СНГ, имеющем широкую региональную сеть по всей стране, было внедрено:

- набор документов, инструкций и регламентов, определяющих деятельность сотрудников службы ИТ;
- систему KPI (Key Performance Indicator– ключевой показатель эффективности) и KGI (Key Goal Indicator) для оценки качества, производительности и результатов работы ИТ–подразделений.

Другой пример успешного управления рисками – украинский филиал одного из крупнейших западных банков. Были реорганизованы SD (Service Desk – служба ИТ–поддержки пользователей) и ИТ–службы на базе стандартов ITIL. В результате внедрения было создано новое сервисное ИТ–подразделение и организована его работа:

- проведено обучение сотрудников подразделения;
- разработан комплект документации, регламентирующей деятельность подразделения и его взаимосвязи с другими подразделениями;

- внедрены средства автоматизации ИТ–процессов;
- проведено разграничение зон ответственности ИТ–сотрудников;
- организована обработка инцидентов в порядке приоритета для бизнеса.

Таким образом, были освобождены ИТ–ресурсы, необходимые для развития информационных систем банка, а банк получил эффективный инструмент для оценки деятельности и управления ИТ–подразделениями. Это дало ряд конкурентных преимуществ и привело к успешному росту и развитию финансового учреждения.

В целом в последние 3 года банки в России и СНГ стали проявлять активный интерес к построению надежной, масштабируемой ИТ–инфраструктуры, способной обеспечить рост бизнеса.

Большинство отечественных банков уже осознали важность вопроса эффективного управления ИТ–инфраструктурой, однако далеко не все знают, как достичь желаемого результата. Зачастую делается попытка решить проблемы, связанные с информационными системами банка, за счет масштабных инвестиций в "свою" группу ИТ–профессионалов. Но практика показывает, что такое решение не всегда эффективно, а также требует больших вложений. Типичным результатом ее применения будет некая система, выстроенная под одного или нескольких ИТ–директоров, которые узурпируют процессы принятия всех решений, в той или иной степени связанных с информационными технологиями. ИТ–инфраструктура такого банка и пути ее дальнейшего развития попадут в зависимость от личных предпочтений конкретных лиц. Ее работоспособность, а значит, и операционная деятельность банка в целом, будут во многом зависеть от субъективных факторов.

ИТ–инфраструктура является одной из подсистем, обеспечивающих эффективность бизнес–процессов банка, с ней связаны серьезные риски, и поэтому вопрос внедрения методологии управления в ИТ должен быть отнесен к ведению топ–менеджмента. Для достижения эффективности бизнеса, получения конкурентных преимуществ и стабильного развития без "болезней роста", должен быть широко использован международный опыт в области управленческих решений.