

ВОЗДЕЙСТВИЕ «ОБЛАЧНЫХ» ТЕХНОЛОГИЙ НА ОПЕРАЦИОННЫЕ РИСКИ БАНКА

Бобыль В. В.

ВПЛИВ «ХМАРНИХ» ТЕХНОЛОГІЙ НА ОПЕРАЦІЙНІ РИЗИКИ БАНКУ

Бобиль В. В.

IMPACT "CLOUD" TECHNOLOGIES AT THE OPERATIONAL RISKS OF THE BANK

Bobyl V.

**Днепропетровский национальный университет железнодорожного
транспорта имени академика В. Лазаряна, г. Днепропетровск**

В статье рассматривается проблема негативного влияния «облачных» технологий на операционную безопасность банка, предлагаются мероприятия по уменьшению операционных рисков банка.

Ключевые слова: «облачные» технологии, операционные риски, банк, риск-менеджмент

У статті розглядається проблема негативного впливу «хмарних» технологій на операційну безпеку банку, пропонуються заходи щодо зменшення операційних ризиків банку.

Ключові слова: «хмарні» технології, операційні ризики, банк, ризик-менеджмент

The article deals the problem of the negative influence of "cloud" technologies for the operating safety of the bank, offers measures to reduce the operational risks of the bank.

Key words: the "cloud" technology, operational risk, bank risk management

Проблему классификации и оценки операционных рисков банка в своих работах исследовали такие экономисты, как А. Богданов [1], Ю. Боруч [2], Б. Сазыкин [3], В. Харламов [4] и др.

Несмотря на достаточно большое количество научных разработок в области оценки и управления операционными рисками банка, следует отметить, что до конца не решенными остаются вопросы взаимосвязи и влияния современных IT- технологий (в том числе «облачных») на величину операционных рисков банка

Операционные риски банка – это внутренние риски кредитного учреждения, связанные с корпоративным управлением и организацией банковских операций. К ним относятся:

1. Технологический риск - вероятность отклонения от запланированных финансовых показателей банка из-за низкой эффективности информационных технологий и процессов обработки информации.

2. Риск исполнителя - вероятность отклонения от запланированных финансовых показателей банка, возникшая в результате непреднамеренного нарушения или небрежного выполнения профессиональных обязанностей работниками кредитного учреждения.

3. Мошенничество - финансовые потери банка, произошедшие в результате обмана или незаконного присвоения денежных средств, собственности и т.д.

4. Корпоративный риск - вероятность отклонения от запланированных финансовых показателей банка из-за ошибок в корпоративном управлении (конфликт интересов, ошибки в понимании бизнес-процессов, в распределении функциональных обязанностей и т.д.).

5. Инновационный риск - вероятность отклонения от запланированных финансовых показателей банка из-за ошибок на стадии разработки и внедрения новых (усовершенствования существующих) банковских продуктов.

6. Стратегический риск - вероятность отклонения от запланированных финансовых показателей банка из-за ошибок в формировании целей и стратегии развития банка, неэффективное реагирование на изменения в бизнес-среде банка.

Мероприятия по уменьшению вышеперечисленных операционных рисков
указаны в таблице 1

Таблица 1

Мероприятия по снижению операционных рисков банка

Операционные риски	Мероприятия по снижению рисков
технологический риск	- мониторить, обновлять и тестировать информационные системы, оборудование, каналы связи и т.д.; - внедрить план по восстановлению ИТ-сервиса в случае форс-мажора; - использовать систему архивации и сохранения банковских данных; - контролировать работу отделов, занимающихся разработкой программного обеспечения и обслуживанием информационных систем
риск исполнителя	- разработать и внедрить кодекс поведения банковского работника; - пересматривать периодически стандарты обслуживания клиентов банка; - ввести систему мотивации персонала; - проводить хронометраж предоставления банковских услуг; - анализировать показатели управления персоналом банка (текучесть кадров, количество обученных сотрудников и т.д.).
мошенничество	ввести механизм своевременного выявления и пресечения возможностей мошенничества с помощью банковских информационных систем
корпоративный риск	- гарантировать одинаковое отношение к акционерам независимо от количества принадлежащих им акций; - использовать международные принципы независимого внутреннего контроля; - разработать и внедрить систему оценки влияния управленческих решений на финансовый результат банка; - осуществить четкое распределение функциональных обязанностей подразделений банка; - четко описать бизнес-процессы банка; - обеспечить предоставление своевременной и полной финансовой информации
инновационный риск	- внедрить систему определения приоритетности разработки новых банковских продуктов (с учетом рисков); - установить стандарты качества нового или

	усовершенствованного банковского продукта (технологическая карта); - обеспечить подразделения банка необходимой нормативной документацией, техническим и программным обеспечением, рекламными материалами; - осуществить пробную продажу нового продукта лояльным клиентам; - разработать эффективную рекламную кампанию с целью стимулирования сбыта
стратегический риск	- разработать план структурной реорганизации банка в случае кризисной ситуации; - проводить мониторинг банков-конкурентов; - внедрить систему контроля за качеством реализации стратегических целей банка (выполнение стратегических планов и бюджетов); - разработать стратегический план по увеличению рыночного сегмента банка (диверсификация продуктов, регионов и клиентов); - проводить периодически маркетинговые исследования рынка

Внедрение «облачных» технологий потенциально может привести к увеличению операционных рисков банка. В первую очередь возрастет объем технологического риска.

Отметим, что к достоинствам «облачных» технологий можно отнести возможность банков отказаться от необходимости создавать и поддерживать собственную вычислительную инфраструктуру.

Таким образом, «облако» открывает новый подход к вычислениям, при котором ни оборудования, ни программное обеспечение не принадлежит банку. Вместо этого провайдер с помощью интернет-сервиса предоставляет банку - заказчику уже готовый продукт.

Рассмотрим преимущества применения «облачных» технологий в банке:

1. Экономичность. «Облачные» технологии позволяют существенно снизить капитальные затраты банка на построение центров обработки данных, закупку серверного и сетевого оборудования (значительную долю таких расходов берет на себя провайдер «облачных» услуг). Дополнительно банк экономит на содержании IT-персонала и администрирование.

2. Эластичность. «Облачные» технологии обеспечивают возможность оперативно менять конфигурацию корпоративной IT-инфраструктуры в зависимости от текущих потребностей банка (финансовое учреждение покупает столько ресурсов, сколько нужно в данный момент времени). Ресурсов «облака» вполне хватает для заказа виртуального «суперкомпьютера» или информационно-вычислительной инфраструктуры для банка, и при этом не возникает проблем с обновлением программного обеспечения (всегда доступны последние версии) и совместимостью различных операционных систем. В периоды пиковых нагрузок (например, при составлении годовой финансовой отчетности) отсутствует необходимость введения дополнительных информационных мощностей, поскольку «облачные» сервисы могут масштабироваться автоматически и практически неограниченно. Услуги могут быть предоставлены и расширены в любой момент времени, без дополнительных затрат на взаимодействие с провайдером (в автоматическом режиме).

3. Мобильность. «Облачные» технологии предоставляют возможность в буквальном смысле «носить свое рабочее место с собой» - при наличии мобильного терминального устройства и доступа к Интернету работник банка, независимо от своего местонахождения, всегда имеет доступ к собственному виртуальному компьютеру, корпоративной сети или базе данных.

4. Самообслуживание по требованию. Банк самостоятельно определяет и изменяет вычислительные потребности (серверное время, скорость доступа и обработки данных, объем хранимых данных) без взаимодействия с провайдером.

5. Сохранение данных. Работникам банка не нужно заботиться о резервировании информации, поскольку данные безопасно хранятся в «облаке».

Однако «облачные» технологии связаны с такими рисками:

1. Атаки на гипервизор. Основной функцией гипервизора является распределение ресурсов между виртуальными машинами. Атака на гипервизор

может привести к тому, что одна виртуальная машина сможет получить несанкционированный доступ к памяти и ресурсам другой.

2. Атаки на системы управления. Большое количество виртуальных машин, которые используются в «облачных» технологиях, требует наличия определенной системы управления, которая должна контролировать создание и ликвидацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин-шпионов, способных блокировать работу «легальных» виртуальных машин.

3. Нестабильное соединения с сервером. Использование «облачных» технологий требует длительного пребывания в онлайн-режиме. Соединение должно быть стабильным и, желательно, широкополосным. Частично риск отсутствия соединения может быть уменьшен путем кэширования данных или разработкой алгоритма перехода в режим медленной связи для обмена только критически важными данными.

4. Техническая зависимость от поставщика (провайдера) «облачных» технологий или риск его банкротстве. Если поставщик «облачных» решений по каким-либо критериям (например, возникновение проблем на маршрутах обмена данными) перестает соответствовать требованиям банка, тогда финансовое учреждение имеет право поменять провайдера. Однако этот процесс потенциально связан с рядом трудностей: во-первых, на рынке IT-технологий может отсутствовать провайдер, который в состоянии предложить соответствующий уровень «облачных» решений, во-вторых, денежные и временные затраты могут быть слишком большими для банка.

5. DDOS-атаки (нападение на компьютерную систему с целью сделать компьютерные ресурсы недоступными для пользователей). Одним из самых распространенных способов нападения является «насыщение» атакованного компьютера или сетевого оборудования большим количеством внешних запросов.

6. Безопасность данных. Большинство банков опасаются перехвата информации при передаче данных, потери контроля над данными и невозможности полного уничтожения информации в сети Интернета.

Основные риски «облачных» технологий и инструмент их уменьшения указаны в таблице 2.

Таблица 2

. Основные риски «облачных» технологий и способы их уменьшения

Риск	Характеристика	Способы уменьшения
Атаки на гипервизор	Риск того, что одна виртуальная машина получает несанкционированный доступ к памяти и ресурсам другой виртуальной машины	Стандартизация процедур доступа к управляющим средствам хост-сервера; применение встроенного брандмауэра (программа, осуществляющая защиту компьютерных сетей) хоста виртуализации
Атаки на системы управления	Риск появления виртуальных машин-шпионов, которые способны блокировать работу «легальных» виртуальных машин	Применение паролей, сертификатов и кодов
Стабильность соединения	Риск ухудшения (или отсутствия) подключения к Интернет-ресурсу	Кэширование данных; разработка алгоритма перехода в режим медленной связи
Зависимость от поставщика (провайдера) «облачных» технологий	Риск отсутствия возможности поменять поставщика «облачных» технологий из-за отсутствия на рынке других провайдеров, средств или времени	Тщательный подход к выбору провайдера; работа с несколькими провайдерами
Банкротство провайдера	Риск остановки предоставления «облачных» решений из-за банкротства провайдера	Работа с несколькими провайдерами; наличие плана мероприятий по смене провайдера
Потеря связи с провайдером	Риск остановки бизнес-процессов банка из-за отсутствия доступа к сервисам провайдера	Выбор провайдера, имеющего датацентры в нескольких странах; применение

		спутниковой интернет-связи; наличие резервной копии критических систем в частном «облаке»
Перехват информации	Риск несанкционированного доступа к информации в процессе передачи данных	Использование криптографии при передаче информации; обучение пользователей правилам информационной безопасности
Юридический риск	Риск получения штрафов и других санкций со стороны национального регулятора из-за нарушений требований действующего законодательства	Консультация с национальным регулятором и внешними аудиторами
Потеря контроля над данными или информационно-вычислительной инфраструктурой	Риск отсутствия возможности обеспечить надлежащий уровень информационной безопасности из-за потери контроля над данными или информационно-вычислительной инфраструктурой	Проведение аудита безопасности провайдера; заключение соглашения с провайдером по неразглашению конфиденциальных данных; мониторинг уровня сервиса и инцидентов нарушения информационной безопасности
Проблема полного уничтожения информации	Риск утечки информации из-за сложности полного уничтожения данных в «облачных» технологиях	Шифрование данных в «облаке»; маскировка информации; включение требований по процедуре уничтожения информации в SLA (договор про уровень предоставления услуг)
Взлом интерфейса управления	Риск мошенничества из-за взлома интерфейса управления «облачными» технологиями	Использование двухфакторной аутентификации; шифрование передаваемых данных
DDOS-атаки	Риск нападения на компьютерную систему с целью сделать	Выбор ddos-устойчивого

	компьютерные ресурсы недоступными для пользователей	провайдера; работа с несколькими провайдерами
Деятельность других пользователей «облака»	Риск несанкционированного доступа к информации и остановка бизнес-процессов банка из-за деятельности других пользователей «облачных» технологий	Тщательный подход к выбору провайдера; работа с несколькими провайдерами

Отметим, «облачные технологии» в ближайшем будущем выведут операционную деятельность банков на качественно новый уровень. Эта IT-технология потенциально может стать значительным фактором увеличения конкурентоспособности современных банков.

Но использование «облачных» решений связано с определенными операционными рисками: в первую очередь с технологическим.

На уровне банка (микроуровень) уменьшить размер рисков, возникающих в процессе применения «облачных» технологий, можно с помощью следующих основных управленческих решений: тщательный подход к выбору провайдера (поставщика) «облака»; разработка плана мероприятий по смене провайдера; внедрение двухфакторной аутентификации, шифрование и маскировка данных; обучение работников банка правилам информационной безопасности; проведение консультаций с регулятором и внешними аудиторами относительно рисков внедрения «облачных» технологий.

С позиции национального регулятора (макроуровень) целесообразно проведение комплексного анализа и оценки состояния, тенденций и перспектив внедрения «облачных» технологий в банки, а также разработка национальных стандартов, устанавливающих соответствующие требования к качеству и надежности «облачных» технологий и услуг на финансовом рынке России.

Список литературы

1. Богданов А. Операционный риск и его влияние на устойчивую работу финансовой организации / А. Богданов // Банковские технологии. – 2008. – №7. – С. 80 – 88.

2. Боруч Ю. Консорциум для сбора данных по операционным рискам как инструмент оценки и снижения риска / Ю. Боруч // Банковское дело. – 2009. – № 10. – С. 40.

3. Сазыкин Б. Управление операционным риском в коммерческом банке / Б. Сазыкин. – М.-СПб. : Вершина, 2008. – 291с.

4. Харламов В. Операционные риски и риски информационной безопасности / В. Харламов // Банковское дело. – 2009. – № 7. – С. 41 – 42.

5. Grosch, H.R.J., "Bibliography on Chebyshev Polynomials and Their Use as Optimum Approximation Functions", Proceeedings of the 1949 Scientific Computation Seminar, IBM (1951).