Информационные технологии как инструмент выживания банков

ЕЛЕНА ГОРЕТКИНА

Нынешний год не обещает быть легким для российских банков. Остаются прежние проблемы в виде санкций, нехватки капитала, роста просрочки и повышенных отчислений в резервы, к ним добавляется более жесткое регулирование. Так, агентство Moody`s ухудшило прогноз падения российского ВВП с 1,5 до 2,5% и прогнозирует, что Центробанк РФ отзовет лицензии у каждого десятого банка.

ОБЗОРЫ

В таких условиях банкам предстоит трудная борьба за выживание, успешность которой во многом определяется эффективностью рабочих процессов. Важную роль в поддержке последних играют ИТ. Какими будут приоритеты банков в области информатизации в этом году? Какие решения может предложить сегодня ИТ-индустрия? На эти и другие вопросы отвечают эксперты, представляющие поставщиков ИТ-продуктов для финансового сектора и системных интеграторов.

Новая реальность — новые задачи

Несмотря на экономический кризис, банки не отказываются от развития своих ИТ-систем, но их приоритеты меняются. Впрочем, многие эксперты стараются избегать слова "кризис", считая, что оно всем уже надоело и к тому же не очень уместно говорить об этом, когда правила игры относительно стабильны, пусть и не позитивны.

По их мнению, финансовая сфера, как и многие другие отрасли экономики, живет в новой реальности и уже осознает это. "Задачи можно сформулировать так: быстро, еще быстрее и недорого. Проблемы не сильно трансформировались относительно ситуации в канун кризиса, они просто стали требовать более быстрых и эффективных решений", — считает Александр Сиркин, директор по развитию бизнеса компании IBS.

С ним согласен Юрий Корешков, руководитель управления по работе с банками Центра программных решений компании "Инфосистемы Джет", который отметил, что сейчас мы все чаще говорим о новой реальности и пора к этому привыкнуть. В ИТ-сфере тоже начинается новая реальность, для которой характерны две тенденции: во-первых, фокус на снижение стоимости владения ИТ-системами, в том числе желание сэкономить на классической организации ИТ-сервисов; во-вторых, стремление к повышению гибкости ИТ как на уровне бизнес-приложений, так и на уровне инфраструктуры за счет внедрения новых технологий разработки, управления изменениями, развития новых, более гибких и удобных сервисов для клиентов и т. п.

При этом многие банки переходят на режим максимальной экономии. "Они рассматривают вложения в информатизацию под лупой, давая ход только проектам, жизненно важным для бизнеса или повышающим его эффективность. На сомнительные или необязательные задачи бюджеты не выделяются. Даже рост мощностей для санации, апгрейд или дополнительный клиентский сервис анализируются с позиции необходимости", — пояснил Андрей Завада, директор по продажам ГК ХОСТ.

Это связано с тем, что ИТ-бюджеты большинства российских банков сократились на 20—30%, прежде всего из-за падения курса рубля. Лишь в некоторых небольших частных банках, исчисляющих ИТ-бюджеты в валюте, расходы на ИТ практически не снизились. По оценке Алексея Шалагинова, директора по отраслевым решениям департамента ИТ и ЦОД компании Huawei в России, в 2015-м ИТ-расходы российских банков упали по сравнению с 2013-м почти вдвое, до уровня немногим более 1 млрд. долл. В текущем году роста инвестиций в ИТ в банковской сфере не предвидится, лишь в 2017-м, при удачном стечении обстоятельств, может быть небольшой рост. Восстановления же ИТ-расходов в банках до уровня 2013 г. не следует ожидать ранее 2020 г.

"В таких условиях развитие ИТ в банковской отрасли представляется достаточно проблематичным. Следовательно, первоочередной задачей является оптимизация расходов на ИТ-обеспечение и превращение банковских ИТ-систем из обслуживающих в элемент генерации ценности", — считает Алексей Шалагинов.

Клиентский рынок не растет, поэтому между банками идет ожесточенная борьба за имеющихся клиентов. Чтобы сохранить своих и переманить чужих, им надо предлагать не только что-то "очень вкусное", но и быть в этом первыми. Поэтому резко сократилось время на выпуск релиза любой системы или продукта — с месяцев до недель. При этом цена не должна быть высокой, так как лишних денег ни у кого нет и низкая себестоимость системы или услуги актуальна как никогда.

Однако зачастую сокращение расходов влечет за собой снижение качества продукта. Банки это понимают. По словам Натальи Педчик, директора по работе с ключевыми клиентами подразделения IT Business компании Schneider Electric, в условиях кризиса наряду со снижением затрат на внедрение и эксплуатацию возрастают требования к уровню надежности и безопасности банковской информатизации. В связи с этим растет тенденция к централизации, стандартизации и обеспечению масштабируемости банковской ИТ-инфраструктуры, цель которой — оптимизировать стоимость владения и повысить скорость внедрения новых услуг.

В русле мировых ИТ-тенденций

Хотя рост мирового ВВП замедляется, банки всего мира наращивают инвестиции в ИТ. По прогнозу IDC, в 2016-м банковские ИТ-расходы составят 275 млрд. долл., а затем будут ежегодно расти на 4,5% в течение пяти лет. При этом IDC отмечает, что наиболее сильно на ИТ-бюджеты банков влияют основные компоненты цифровой трансформации, такие как облачные и мобильные технологии, Bid Data и аналитика (BI).

В нашей стране современные технологические тренды тоже актуальны, так как, несмотря на все проблемы, банкам нужно оптимизировать расходы. Так, Александр Сиркин считает, что облака и аутсорсинг услуг или процессов позволяют снизить затраты на собственные структуры на десятки процентов, а иногда и в разы.

Что касается мобильности, то по единодушному мнению экспертов, она уже давно не является каким-то модным трендом. Это суровая реальность и обязательное требование клиентов. Нравится это банкам или нет, но они идут в Сеть, так как за этим будущее. Как отметил Алексей Шалагинов, сейчас для банковской отрасли наиболее актуально повышать мобильность бизнеса и предоставлять услуги в режиме онлайн, прежде всего через мобильные сети. По прогнозу Алексея Шалагинова, в ближайшие два-три года среднегодовой рост расходов на банковскую "мобилизацию" составит 10—12%.

При этом банки применяют разные подходы. У многих из них есть собственные разработки, а кто-то предпочитает покупать готовые приложения. "Но в целом основные игроки понимают, что мобильные приложения — не дань моде, а очевидная потребность. При постоянном увеличении их функционала среди ключевых требований на первом месте остаются простота использования и безопасность", — констатирует Константин Савченко, руководитель отдела поддержки и развития продаж корпоративного ПО компании Axoft.

Поскольку мобильные услуги уже не являются особым конкурентным преимуществом, банкам приходится уделять больше внимания изучению других потребностей клиентов и двигаться в сторону повышения персонализации услуг. Пользователи оставляют в цифровой среде огромное количество информации. Но как извлечь из нее пользу для бизнеса? Здесь на первый план выходят технологии Big Data и BI, которые способны значительно повысить отдачу от банковских продуктов.

Правда, отметил Константин Савченко, некоторые компании еще только стоят на пороге осмысления предстоящей работы, однако практически все понимают, что данные, которые, по сути, сейчас "лежат под ногами", являются необходимыми для роста прибыли, более качественной работы с клиентами, обеспечения внутренней и внешней безопасности.

Однако, по мнению Алексея Шалагинова, реальные внедрения "больших данных" требуют больших инвестиций, а это пока проблематично. Тем не менее он полагает, что несмотря на общий тренд снижения ИТ-расходов, затраты на BI и Big Data будут расти в ближайшие два-три года быстрее других инвестиций в финансовые технологии в целом.

В числе других передовых технологий эксперты отметили так называемые видеобанкоматы, которые способны предоставить гораздо больший спектр услуг, чем обычные банкоматы, и применение Интернета вещей, например для отслеживания производственного цикла клиентов или для платежных сервисных устройств, которые сами совершают финансовые транзакции.

Таким образом, банки по-прежнему идут в авангарде освоения технологий. Однако, как справедливо заметил Андрей Завада, важно не то, что они используют, а то, как используют, насколько грамотно и гармонично эти решения вписаны в цикл банковских операций: "Технологии — не волшебная пилюля, а просто инструмент. Компьютер используют и для отправки ракет в космос, и для лайков в соцсетях".

С этой точки зрения эксперты рекомендуют использовать перечисленные технологии вместе, поскольку они сильно взаимосвязаны между собой и в совокупности могут способствовать повышению эффективности. Например, у любого банка есть огромное количество данных, которые необходимо хранить, а следовательно, приходится увеличивать издержки на аппаратные ресурсы. Если же перенести эти данные в облака, это позволит оптимизировать затраты на их хранение, сэкономив на закупке и обслуживании оборудования. Обработка их с помощью технологий машинного обучения сокращает время, а применение BI-инструментов позволяет делать различные аналитические выборки и представления обработанных данных, а затем на их основе через мобильный банкинг целенаправленно предлагать клиентам новые продукты и услуги. Каждый шаг на данной цепочке по-своему увеличивает эффективность банковской деятельности.

Комплексный аутсорсинг — лед тронулся

В мире усиливается тенденция передачи части или всех ИТ-операций на аутсорсинг профессиональным провайдерам ИТ-сервисов ради оптимизации затрат и рисков. До последнего времени российские банки с опасением относились к такой возможности. Но сейчас в связи с новой реальностью такое положение начинает меняться.

По мнению экспертов, многие коммерческие банки уже переходят на аутсорсинг, хотя и осторожно. Так, Андрей Завада отметил, что банки остаются консерваторами в отношении безопасности и не любят давать другим доступ к своей инфраструктуре: "В некоторых наших

Наши эксперты

АНДРЕЙ ЗАВАДА, *директор по продажам, ГК ХОСТ*

АЛЕКСЕЙ КАТРИЧ, *заместитель генерального директора, "Техносерв Консалтинг"*

ЮРИЙ КОРЕШКОВ, *руководитель управления по работе с банками, Центр программных решений компании "Инфосистемы Джет"*

НАТАЛЬЯ ПЕДЧИК, *директор по работе с ключевыми клиентами, подразделение IT Business компании Schneider Electric*

КОНСТАНТИН САВЧЕНКО, *руководитель отдела поддержки и развития продаж корпоративного ПО, Axoft*

АЛЕКСАНДР СИРКИН, *директор по развитию бизнеса, IBS*

РУСТЕМ ТУРСУНБАЕВ, *архитектор систем ИБ, ГК "Компьюлинк"*

АЛЕКСЕЙ ШАЛАГИНОВ, *директор по отраслевым решениям департамента ИТ и ЦОД, Huawei в России*

сервисных контрактах прямо прописано, что работы проводятся под наблюдением специалиста банка".

Тем не менее лед тронулся. Если раньше банки просто отмахивались от идеи аутсорсинга, то сейчас картина другая. Так, по мнению Юрия Корешкова, кризис повернул банки в сторону сервисных моделей, ориентированных на поддержку процессов, не относящихся к профильной деятельности банка.

Правда, считает Александр Сиркин, о победе комплексного аутсорсинга говорить еще рано, но банки все чаще отдают на аутсорсинг поддержку ИТ-систем и, что самое главное, получают от этого прямую финансовую выгоду без потери уровня сервиса. Все это вместе с учетом опыта развитых финансовых систем других стран дает основания полагать, что комплексный аутсорсинг не за горами.

Распространению аутсорсинга способствует и ситуация на ИТ-рынке, где в последнее время появилось несколько компаний, предоставляющих ИТ-услуги, в частности в области безопасности. "Например, услуга SOC является для многих единственным способом получить качественный анализ информационных событий, не инвестируя большие деньги в инфраструктуру и специалистов. Такая тенденция будет и дальше развиваться, так как количество и качество атак растет, а значит, обслуживание ИТ- и ИБ-систем за счет собственных ресурсов для многих заказчиков будет обременительным", — уверен Константин Савченко.

Импортозамещение — не самоцель

Относительно развития импортозамещения в банках мнения экспертов разделились. Одни считают, что ситуация меняется, правда, многое зависит от типа систем и задач. "АБС и процессинговые системы и так были российскими, а что касается углубленной аналитики, рисков, антифрода и ряда других областей, где критично наличие сложных математических моделей, алгоритмов и других наработок, то таких отечественных систем де-факто нет и создать их за несколько месяцев или даже пару лет крайне сложно", — пояснил Александр Сиркин. Поэтому здесь быстрого прорыва не случилось и ждать его не стоит. Зато в области инфраструктурных решений на рынке довольно быстро появились отечественные вычислительные платформы, которые вполне успешно конкурируют с дорогими западными продуктами.

По мнению других экспертов, общий курс на импортозамещение пока не оказывает заметного влияния на информатизацию банков, хотя сама по себе эта тема и вызывает у них интерес. Например, в центр компетенций ГК ХОСТ по свободному ПО уже выстроилась очередь из желающих посмотреть работу решений вживую. "Но от интереса до реальных проектов пока далеко. Банки только сравнивают плюсы и минусы перехода на отечественные продукты или свободное ПО, считают совокупную стоимость владения, оценивают риски", — поделился опытом Андрей Завада.

Такого же мнения придерживается и Наталья Педчик, которая отметила, что хотя банки серьезно рассматривают стратегию импортозамещения, в том числе и в сфере ИТ, но на крупных инвестиционных проектах предпочитают внедрять оборудование известных, проверенных мировых производителей.

В перспективе, считает Константин Савченко, тема импортозамещения будет переживать несколько циклов: от восторженных идей заменить все на "наше" до осмысления абсурдности этой затеи и поиска локальных ниш и сегментов, в которых мы сможем преуспеть или хотя бы не быть аутсайдерами: "Все мы знаем удачные примеры российских решений, которые заказчики выбирали осознанно по итогам сравнения с отечественными и зарубежными аналогами. Хочется верить, что банки и другие компании по-прежнему смогут руководствоваться коммерческой целесообразностью, а не местом происхождения решения".

Таким образом, эксперты считают, что стратегия импортозамещения и импортонезависимости не является самоцелью. Она должна рассматриваться только в рамках достижения общей цели снижения операционных и стратегических рисков, связанных с ИТ и ИБ, таких как риски неконтролируемого внешнего деструктивного воздействия на банковские ИТ. Поэтому оптимальным является рассмотрение каждого случая в отдельности, когда при реализации информационных систем и ИТ-инфраструктуры банковской организации учитывается вся совокупность рисков.

Open Source в банках — плюсы и минусы

Сейчас доминирующей моделью в области ИТ становится Open Source. По данным компании Black Duck, полученным в результате опроса 1300 компаний из разных стран мира, 65% организаций использует открытый софт для разработки, а 55% — применяет в своей ИТ-инфраструктуре. Правда, неясно, сколько среди них банков. Ведь традиционно финансовый сектор с некоторой настороженностью относится к открытому ПО.

Однако в России интерес к Open Source подогревается нашими национальными особенностями, такими как общий тренд на импортозамещение и значительное подорожание западного проприетарного ПО. По мнению Андрея Завады, многие банки уже используют Open-Source-разработки в ИТ-ландшафте, причем и в системной, и в прикладной частях.

С ним согласен Алексей Шалагинов, который отметил, что Open Source оказывается достаточно привлекательным для большого числа ИТ-директоров, в том числе и из банковской сферы: "Внедрение открытых решений, например Sugar CRM, в некоторых российских коммерческих банках уже привело к сокращению ИТ-расходов более чем в три раза по сравнению с использовавшимися ранее проприетарными решениями".

По его мнению, к другим преимуществам такого подхода относится ускорение некоторых операций (например, по обслуживанию клиентов), уменьшение затрат на обучение персонала и новые возможности для перекрестных продаж в банках.

Юрий Корешков тоже с оптимизмом смотрит на перспективы Open Source, считая, что в ближайшее время стратегия замены зарубежного ПО на российские разработки и Open Source будет набирать обороты: "Банки уже начали строить свои ИТ-системы на основе решений и компонентов с открытым кодом, стараясь найти возможность отказаться от дорогостоящей поддержки зарубежных продуктов".

Однако у Open Source есть не только сильные стороны. Так, при оценке возможности использования открытых решений не следует забывать о проблеме уязвимости такого ПО. В случае проприетарных решений известно, кто отвечает за устранение проблем, а при использовании Open Source все такие риски возложены на банковские организации или компании, осуществляющие внедрение.

Кроме того, следует учитывать и скрытые расходы по созданию неоптимальных решений, но максимально кастомизированных для сложившейся в организации текущей ситуации. "Все сильные и слабые стороны перехода на решения стека Open Source еще не просчитаны. Это аналог задачи, которую банки до сих пор так и не решили: что лучше — внедрить иностранную систему, воплощающую международный опыт, или российскую с максимально проработанной локальной спецификой", — отмечает Алексей Катрич, заместитель генерального директора компании "Техносерв Консалтинг".

Возможно, поэтому, несмотря на все перечисленные выше проблемы в банковской информатизации, особого бума в отношении открытого софта пока не наблюдается. "Крупные российские банки с осторожностью относятся к Open-Source-решениям и не стремятся использовать их в своей деятельности", — констатирует Наталья Педчик.

Но в перспективе такое отношение может измениться. На это есть причины, которые привел Константин Савченко: "Модель Open Source эволюционирует, появляются новые игроки, растет кооперация, возникают альянсы крупных производителей, расширяются сегменты присутствия — все это позволяет быть уверенными в перспективности модели Open Source, в том числе в весьма конкурентной банковской среде".

Спасение от хакеров

Банковский сегмент традиционно является целью атак со стороны злоумышленников. Только за период с октября 2015 г. по март 2016-го российские банки, по данным ЦБ, потеряли 2 млрд. руб. из-за хакерских атак. И несмотря на развитие законодательства в области ИБ и на меры, которые принимают сами банки, ситуация не улучшается.

По мнению некоторых экспертов, данные ЦБ — лишь верхушка айсберга. На самом деле потери гораздо больше. Рустем Турсунбаев, архитектор систем ИБ ГК "Компьюлинк", объяснил это тем, службы безопасности банка легко проверяют транзакции на большие суммы, но не могут отследить среди миллионов операций нелегитимные транзакции на маленькие суммы, потому эти данные не попадают в статистику.

Что касается причин плачевной ситуации с ИБ, то, по мнению экспертов, их немало, и одна из них связана с самими банковскими ИТ. Ведь для оперативного и прозрачного взаимодействия с пользователями современный банк использует систему "банк — клиент" в виде веб-портала, доступ к которому может получить каждый. Эти сайты взаимодействуют с серверами, в том числе осуществляющими финансовые транзакции и расположенными в сети банка. Данная взаимосвязь и является одним из возможных способов доступа к материалам банка.

Немаловажную роль играет пресловутый человеческий фактор: "Все чаще хакеры используют технологию фишинга, рассылая информационные письма якобы от имени ЦБ и регулятора, а во вложениях находятся зараженные файлы, при открытии которых на компьютерах сотрудников банков начинается подспудная вредоносная деятельность", — отмечает Алексей Шалагинов.

Еще одна причина, по мнению Алексея Катрича, заключается в том, что уровень подготовки специализированных хакерских компаний сегодня значительно превосходит возможность банков содержать специализированные подразделения для противодействия атакам.

Такой же точки зрения придерживается Андрей Завада: "Вместе с уровнем защиты растет и уровень атак, и злоумышленники выигрывают эту гонку. Какой бы комплексной не была защита, в ней найдутся "дыры". Чаще всего слабым звеном оказывается человек. Это подтверждают и удачные атаки с помощью вируса Buhtrap".

Недофинансирование обучения сотрудников также играет на руку хакерам. "Зачастую приобретаются системы за сотни тысяч или миллионов долларов, а их эксплуатация осуществляется без должной подготовки кадров. В решении этого вопроса есть существенный потенциал для улучшения защиты компаний", — считает Константин Савченко.

В частности, эксперты рекомендуют банкам применять хорошо зарекомендовавший себя опыт борьбы с подобным явлением в Австралии, где для всех сотрудников банков и госорганов введены правила "ИТ-гигиены", включающие примерно 40 элементарных действий по ИБ. Оказалось, что реализация только первых шести пунктов перечня уже позволяет сократить ущерб на 90%. Нелишне будет перенять этот опыт и в России вкупе с более интенсивным применением ИБ-систем.

Кроме того, стоит также обратить внимание на технологию распределенной верификации блоков транзакций блокчейн. Эта технология отличается тем, что в ней практически невозможно провести злонамеренную транзакцию, включая и почтовую рассылку. Она будет сразу же обнаружена, и ее источник будет верифицирован с точностью до IP-адреса. По словам Алексея Шалагинова, опыт использования блокчейн сейчас пристально изучают ведущие российские банки.

Могут пригодиться и услуги компаний, специализирующихся в сфере ИБ: банки должны следовать первоочередным мерам противодействия и защиты информационного контура банка, а профессиональные компании — производить онлайн-охрану и превентивный аналитический мониторинг информационных объектов банка. "Постоянное участие специального оборудования, искусственного интеллекта и опытных специалистов дает возможность предотвратить потенциальные угрозы взлома и финансовые потери", — считает Алексей Катрич.

Но главным, уверен Рустем Турсунбаев, является то, что меры по повышению эффективности защиты банковской сферы должны быть комплексными: начиная с построения правильной безопасной архитектуры системы, обеспечения круглосуточного мониторинга работы ее компонентов и использования специализированных антифрод-систем и заканчивая систематическим повышением уровня знаний обслуживающего персонала.

Кибербезопасность...

ПРОДОЛЖЕНИЕ СО С. 9

Причем фирма может быть не виновата. Все может делаться без ее ведома.

PC Week: Как выглядит организационная структура обеспечения кибербезопасности в РЖД?

Б. М.: Основным госрегулятором выступает ФСТЭК РФ. В ОАО "РЖД" создан и работает Экспертный совет по кибербезопасности, возглавляемый старшим вице-президентом ОАО "РЖД" — главным инженером компании. Экспертный совет определяет основные направления работы Центра кибербезопасности ОАО НИИАС. Кроме этого есть аккредитованный ФСТЭК орган (центр) по сертификации ОАО НИИАС, а также аккредитованные на безопасность информации испытательные лаборатории. И еще пул из 10—15 фирм, с которыми мы давно сотрудничаем и чья компетенция не вызывает у нас сомнения.

PC Week: Какие нужно предпринимать меры для противодействия возможным кибератакам?

Б. М.: Нужно развивать отечественное производство, осуществлять легендирование и централизацию закупок. Желательно иметь альтернативных поставщиков комплектующих и ПО для критических компонентов МПСУ и соответственно возможность альтернативной закупки, прежде всего в странах Таможенного союза и БРИКС. Ну и необходимо обязательно обеспечивать входной контроль, тестирование комплектующих и ПО. Сейчас об этом практически забыли, а в советские времена входной контроль был 100%-ным. Но и сегодня есть организации, которые этим занимаются.

PC Week: Спасибо за беседу.