ИТ в финансовом секторе: проверка на прочность

ЕЛЕНА ГОРЕТКИНА

ОБЗОРЫ

Хотя по итогам 2013 г. динамика развития банковского сектора в России была на правительственном уровне признана в целом нормальной, начало 2014-го сопровождалось нарастанием проблем в этой сфере в связи с экономической нестабильностью и возросшими политическими рисками. В числе ключевых проблем сектора эксперты отмечают волатильность на валютном рынке, отток капитала, ухудшение качества кредитных портфелей на фоне низких темпов роста экономики, удорожание финансирования на внутреннем облигационном рынке. И хотя эти проблемы обусловлены главным образом внешнеполитическими факторами, решать их придется за счет внутренних резервов.

Дополнительные угрозы для банков и других учреждений финансового сектора несут в себе и возможные проблемы (в связи с санкциями) с поддержкой и лицензированием технических систем и ПО, приобретенных у зарубежных компаний и используемых учреждениями для поддержания внутренних бизнес-процессов и операционной деятельности в целом. Реальность этих угроз подтверждают, в частности, имевший место инцидент с временным прекращением обслуживания ряда российских банков международными платежными системами Visa и MasterCard (вследствие чего активизировались дискуссии о необходимости создания национальной платежной системы), а также инициация депутатами Госдумы РФ внесения поправок в закон "Об информации, информационных технологиях и о защите информации", обязывающих регуляторов рынка защищать не только поставщиков программных продуктов, но и их потребителей.

Всё это происходит на фоне усиления контроля со стороны государственных органов за деятельностью банковских учреждений, свидетельством чему стали сообщения ЦБ РФ об отзыве лицензий у некоторых банков.

Таким образом, можно констатировать, что в настоящее время российские финансовые учреждения оказались под воздействием ряда негативных факторов. При этом банковские структуры составляют кровеносную систему экономики, а используемые ими информационные технологии и решения являются важнейшим элементом жизнеобеспечения самих этих структур.

Какие проблемы в ИТ-обеспечении финансовых учреждений выходят сегодня на первый план? Как меняется ландшафт ИТ- и ИБ-угроз в данной сфере? Какое решение этих проблем может предложить сегодня ИТ-индустрия? Как в перспективе могут измениться подходы к ИТ-обеспечению банковской деятельности? Эти и другие важные вопросы мы постараемся обсудить в нашем тематическом обзоре.

Стабильная работа в нестабильное время

Информационные технологии в финансовой сфере уже давно стали одним из главных инструментов повышения оборота и увеличения рыночной доли, поэтому расходы на них растут. Так, в глобальном масштабе аналитическая компания Ovum прогнозирует увеличение ИТ-инвестиций розничных банков со 118,6 млрд. долл. в 2013 г. до 152,5 млрд. в 2018-м.

Аналогичная тенденция наблюдается и в России. По прогнозу IDC, с 2013-го по 2017-й расходы на ИТ в нашей стране ежегодно будут расти в среднем на 6%, а для объединенной вертикали, охватывающей банки, страховые компании и поставщиков иных финансовых услуг, этот показатель составит 8,2%.

Вместе с тем в связи с общей экономической нестабильностью и возросшими политическими рисками в ИТ-обеспечении финансовых учреждений на первый план сегодня выходят новые проблемы и задачи. Относительно новым фактором риска стала потенциальная возможность использования западными странами зависимости России от иностранного ПО, оборудования и организационной инфраструктуры в качестве рычага давления и инструмента подрыва социально-политической стабильности страны. "На фоне усилившегося противостояния России и западных стран растет риск атак, нацеленных уже не просто на кражу денег и информации, а на разрушение информационной инфраструктуры", — подчеркнула Наталья Храмцовская, ведущий эксперт компании ЭОС по управлению документацией.

В силу этого, по словам Константина Усаковского, руководителя дирекции "АйТи" по работе со стратегическими рынками, банки вынуждены смотреть на обычные задачи обеспечения непрерывности своей деятельности с учетом новых рисков. Как отмечает г-жа Храмцовская, сейчас нужно, с одной стороны, искать возможности для снижения зависимости ИТ-инфраструктуры финансовой отрасли от зарубежных стран, а с другой — заранее продумывать меры на случай чрезвычайных ситуаций.

Некоторые банки уже действуют в данном направлении. Константин Усаковский отмечает, что с каждым днем увеличивается внимание к разработкам российских компаний и к системам на открытых платформах, особенно со стороны госбанков. Однако зависимость российской финансовой отрасли от зарубежных продуктов настолько велика, что быстро перейти на отечественные вряд ли удастся, даже если будет на что переходить.

Нельзя сбрасывать со счетов и другие растущие риски, не связанные с внешними факторами. На одну из важных проблем, с которой сталкиваются сегодня финансовые структуры, указал Константин Соловьев, заместитель председателя правления международной платежной системы "Лидер": "В последнее время на первый план выходит проблема энергетической безопасности. Непредсказуемость действий наших электроснабжающих компаний, их полная безнаказанность ставят перед нами еще и такие задачи, как обеспечение многоуровневых систем защиты от энергетических сбоев".

Судя по мнению экспертов, банки, по крайней мере ведущие, уделяют немало внимания вопросам стабильности и надежности функционирования. Так, в компании "АйТи" отмечают повышение у крупных банков интереса к обеспечению непрерывности критических бизнес-процессов, к поиску отказо- и катастрофоустойчивых решений, к системам мониторинга работоспособности бизнес-сервисов. Важным трендом является интерес к системам управления планами реагирования на нештатные ситуации, к системам принятия решений о выборе сценариев восстановления после сбоев, отслеживания действий сотрудников в нештатных ситуациях.

В фокусе небольших банков по-прежнему стоят задачи сбора и очистки данных, необходимых для формирования обязательной отчетности. Эти задачи особенно актуальны для тех банков, в чьи стратегии заложена региональная экспансия за счет более слабых игроков, а также для тех, которые активно запускают новые банковские продукты или меняют автоматизированную банковскую систему. Основной проблемой для них оказывается не столько создание хранилища и технологии сбора информации из разнородных источников, сколько контроль за качеством данных первичного учета, используемых при формировании отчетности для Банка России.

Алексей Катрич, старший управляющий консультант IBM в России и СНГ по развитию рынка/сектора финансовых услуг, один из путей обеспечения стабильности и надежности существующего ИТ-ландшафта финансовых учреждений видит в том, чтобы максимально передать функции развития ИТ бизнес-заказчикам, то есть людям, занятым основной деятельностью организации, но при этом обязательно сохранить в ИТ-блоке централизованную службу по архитектуре бизнес-процессов и приложений. По его мнению, такой подход, а также разделение ответственности за принятие финансовых решений по вопросам ИТ позволит повысить надежность и оптимизировать затраты на ИТ.

На глобальном рынке, считает он, уже определилась система координат развития ИТ на следующие пять лет: это облачные технологии и предоставление всех ИТ-решений как сервисов, анализ данных и управление ими как новым ресурсом каждой компании, мобильность и социальные сети в качестве способа организации взаимоотношений с клиентами. Поэтому финансовым организациям следует выстраивать свои стратегии в соответствии с данной системой координат.

Собственно, движение в сторону облаков, как отмечает Сергей Котов, эксперт по информационной безопасности из компании "Аладдин Р.Д.", уже наблюдается, причем обретает все более осмысленные формы: "Сначала была буря восторгов под лозунгом "всё перенесем в облака", потом пришло понимание, что здесь есть проблемы и торопиться не надо, затем возникли опасения относительно безопасности публичных облаков, и наконец начался переход к спокойному внедрению частных облаков и переносу в публичные только некритичных данных".

Что касается политических рисков и экономических санкций, то, по словам экспертов, финансовый сектор пока занимает выжидательную позицию. "В целом каких-то глобальных изменений в ранее принятых информационных стратегиях мы не видим. Возможно, они появятся в последующем, когда будут очерчены, например, контуры отечественной платежной системы или каким-то образом изменятся принципы функционирования и договоры с международными агентами," — сказал Константин Усаковский.

Наш ответ на санкции

Возвращаясь к актуальной проблеме угрозы для банков и других организаций финансового сектора в связи с возможными санкциями, нельзя не остановиться на потенциальных проблемах с поддержкой и лицензированием технических систем и ПО, приобретенных у зарубежных компаний и используемых учреждениями для поддержания внутренних бизнес-процессов и операционной деятельности в целом.

Судя по появившимся в конце апреля сообщениям российских СМИ, эта угроза уже стала реальностью. Так, по информации от анонимных источников из двух российских банков, ряд ведущих американских компаний присоединились к санкциям в отношении этих банков. Правда, никаких официальных сообщений на данную тему не последовало. Но тем не менее эта новость взволновала компьютерную общественность, которая начала обсуждать вопрос о том, что может предложить в качестве ответа наше государство и отечественная ИТ-индустрия.

Наши эксперты

АЛЕКСЕЙ КАТРИЧ, *старший управляющий консультант по развитию рынка/сектора финансовых услуг, IBM в России и СНГ*

СЕРГЕЙ КОТОВ, *эксперт по информационной безопасности, "Аладдин Р.Д."*

КОНСТАНТИН СОЛОВЬЕВ, *заместитель председателя правления, международная платежная система "Лидер"*

КОНСТАНТИН УСАКОВСКИЙ, *руководитель дирекции по работе со стратегическими рынками, "АйТи"*

НАТАЛЬЯ ХРАМЦОВСКАЯ, *ведущий эксперт по управлению документацией, ЭОС*

Мнения экспертов разделились. Одни полагают, что Россия способна достаточно быстро продублировать у себя практически любые технологии при условии жесткого централизованного контроля над ходом соответствующих программ. По словам Натальи Храмцовской, нужно продумать серьезные ответные меры против попыток подрыва национальной экономики, вплоть до полного прекращения защиты прав интеллектуальной собственности зарубежных компаний на территории РФ, как это имело место во времена холодной войны: "Для начала следует, как это и делает правительство России, попытаться договориться с зарубежными партнерами по-хорошему, но при этом готовиться к худшему и всерьез вместе с партнерами из дружественных стран взяться за разработку альтернативных технологий".

Такие технологии уже давно разрабатываются, например в рамках свободного ПО. В нашей стране, например, развивается немало отечественных дистрибутивов Linux. В том числе, как отмечает Сергей Котов, есть сертифицированные ФСБ России, ФСТЭК России и МО России и содержащие интегрированные в защищенную среду средства общего назначения (СУБД, офисные программы и т. п.), а также продукты, включающие наряду с механизмами защиты возможность подключения средств электронной подписи.

Но не все программные уровни закрываются такими разработками. Константин Усаковский отметил, что корпоративное программное обеспечение строится по иерархическому принципу: системное ПО, инфраструктурное ПО, бизнес-приложения и т. п. При этом чем ниже уровень, тем больше зависимость от производителя, и наоборот, чем выше уровень, тем зависимость от производителя меньше, а от конечного внедренца — больше.

Поэтому к вопросу импортозамещения следует подходить дифференцированно. "На рынке банковских систем есть несколько сильных российских игроков, которые занимают львиную долю рынка

АБС, поэтому в некоторых функциональных ИТ-сегментах проблем быть не должно, — сказал Константин Усаковский. — Но с другой стороны, базы данных вряд ли получится в близлежащей перспективе перевести на другую платформу, если возникнет такая необходимость".

В целом, считает он, вопрос поддержки и развития инфраструктуры необходимо в каждом конкретном случае решать отдельно, так как есть заключенные соглашения и договоры между производителями, их партнерами и заказчиками, которые никто не отменял, есть приобретенные лицензии, есть сроки действия обязательств по поддержке и т. д.

Алексей Катрич видит выход в переходе банков от использования собственных ИТ-департаментов, занятых разработкой и сопровождением ИТ-систем, к передаче не связанных с бизнесом функций на внешнее обслуживание. Он отметил, что банкам такой подход пригодится, так как в каждом из них установлены на 80% одинаковые программы, а различия состоят в их исторической специфике и в настройках бизнес-процессов. Это означает, что в банках мало универсального ПО и очень много нишевых решений, соединенных интеграционным слоем. По словам Алексея Катрича, некоторые поставщики уже предоставляют программные решения как заказные сервисы.

По идее, такой подход в некоторой степени позволит снизить зависимость банков от западного ПО, даже если поставщики услуг будут и дальше его использовать. Но переход этот непрост и может занять много времени.

Аналогично обстоят дела с СПО. "Правительство озаботилось этими проблемами уже давно, постановление по СПО было принято еще в 2010 г., а план по переходу для госорганов рассчитан до 2015-го, — напомнил Сергей Котов. — Депозитарий создан, но зайдя в банк, много ли мы увидим ПО из этого депозитария?"

Эта и другие проблемы развития СПО в России недавно обсуждались на форуме Russian Open Source Summit 2014, участники которого отметили, что пробуксовки в реализации плана перевода госорганов на СПО начались весной 2012-го, после смены правительства РФ.

Тернистый путь к национальной платежной системе

Инцидент с временным прекращением обслуживания банковских операций отдельных кредитных учреждений международными платежными системами Visa и MasterCard привел к активизации действий, направленных на создание в России национальной платежной системы (НПС).

Судя по сообщениям в прессе, государство уже всерьез озаботилось этим вопросом. По плану в ближайшее время будет выбран оператор НПС, а первую российскую карту должны выпустить в середине 2015-го. Предполагается, что национальная платежная система будет строиться не с нуля, а на основе технической инфраструктуры одной из действующих платежных систем. Основными кандидатами являются системы ПРО100 и "Золотая Корона". Но встает вопрос, готова ли отечественная ИТ-отрасль к решению столь амбициозной задачи.

Мнения экспертов разошлись. Так, Наталья Храмцовская не считает эту задачу амбициозной: "С ней уже справились Белоруссия, Япония и Китай. Здесь нет ничего непознанного, никаких сверхъестественных сложностей — просто нужно проделать масштабную и объемную работу, на которую потребуется несколько лет. Но поскольку данная задача имеет стратегическое значение для страны, те, кто участвует в подобных программах, должны сознавать и свою личную ответственность". Это мнение разделяет Константин Усаковский, который указал на то, что создание НПС — это лишь вопрос времени и финансирования.

Однако другие эксперты считают, что на пути к НПС есть немало подводных камней. По словам Константина Соловьева, хотя российская ИТ-отрасль готова и имеет все необходимые ресурсы для решения этой технически несложной задачи, создать систему, которая была бы признана на международном уровне, — задача уже иного уровня. Пока таких систем всего четыре, а реально из них работают только две.

С ним согласен Алексей Катрич, который отметил, что развитие международных платежных систем как в России, так и за рубежом имеет долгую историю. Некоторые отечественные продукты обладают рядом требуемой функциональности на территории России. Но создание национальной платежной системы — задача комплексная и многоэтапная, и решать её нужно совместно с международными.

Действительно, системам Visa и MasterCard потребовались многие годы на создание надежной и работоспособной инфраструктуры: первая была запущена еще в 1958-м, а вторая — в 1966-м.

Есть и другие проблемы. Сергей Котов, например, видит одну из них в том, как совместить нашу защиту (криптографию) с необходимостью превращения платежной системы в международную, так как иначе она вряд ли когда-нибудь окупится.

Важно разобраться также, с какой целью создается НПС. В компании "АйТи" полагают, что возможны два полярных сценария. По первому из них цель состоит в минимизации рисков, связанных с осуществлением расчетов по картам международных платежных систем в России и за рубежом. Но эти риски уже сейчас можно закрыть в рамках существующей договорной базы с платежными системами и иностранными банками и путем создания центра расчетов на территории РФ. Такие планы уже есть: представители Visa и MasterCard недавно объявили о намерении в течение одного-полутора лет открыть российскую компанию, которая будет работать по правилам национальной платежной системы.

В соответствии со вторым сценарием целью может являться полная автономия расчетов по пластиковым картам внутри страны. Эта технически вполне решаемая задача заключается в использовании локальных платежных систем, таких как "Сберкарта", NCC/Union Card, "Золотая Корона".

Явным минусом такого подхода, правда, не имеющим отношения к технологии, эксперты считают то, что возрождение в сегодняшних реалиях идеи единой локальной платежной системы невозможно без отказа от уже эмитированных карт. Этот процесс будет сопряжен с масштабной эмиссией локальных платежных карт и не только потребует значительных инвестиций в инфраструктуру, но и нанесет дополнительный удар по экономике, поскольку снизится популярность расчетов по пластиковым картам. В результате страна вернется к эпохе наличных расчетов, причем для платежей за границей карты национальной платежной системы долго будут неприменимыми.

Требования регуляторов растут

В последнее время государство уделяет повышенное внимание работе банков. Продолжается чистка банковской системы, начатая летом 2013 г. Только в 2014-м Центробанк отозвал лицензии у 36 банков, а всего лицензий было лишено более полусотни кредитных организаций. Чаще всего причинами такого крайнего шага являются фальсификация отчетности, сомнительные операции и нарушения федерального законодательства по части отмывания денег и противодействия терроризму. Тем не менее возникает вопрос, как ужесточение контроля за деятельностью финансовых учреждений со стороны государственных органов может в перспективе отразиться на подходах к ИТ-обеспечению банковской деятельности.

По словам экспертов, до сих пор еще ни у одного банка не отозвали лицензию по причине ненадлежащей работы ИТ-служб, хотя не исключено, что всё еще впереди. Тем не менее подходы к организации ИТ-инфраструктуры уже меняются. Как отметил Константин Соловьев, на смену довольно туманной формулировке "оптимальное соотношение цены и качества", за которой ИТ-директора традиционно маскировали свои личные пристрастия к тому или иному бренду, приходит четкий показатель "цена — надежность", а это уже измеряемые параметры. Повышаются также требования к защищенности систем, к обеспечению безопасности и т. д., а в с связи, увеличением объема регулярно передаваемой в электронном виде отчетности растут требования к обеспечению сохранности баз данных.

К тому же одним из факторов, влияющих на ИТ-стратегии банков, являются действия регулятора, т. е. издаваемые им указания, регламенты и т. п. Соответственно каждая новая инициатива, как правило, влечет за собой какие-то изменения в информационной инфраструктуре банков, и это процесс постоянный и непрерывный. Так, Центробанк готовит рекомендации по обеспечению информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем, требующие в том числе обеспечения безопасной разработки и тестирования ПО. По мнению Сергея Котова, этот стандарт очень актуален, и если он не заставит себя ждать, то может быть, хотя бы некоторые банки будут закладывать требования по безопасности в контракты на поставку АБС.

Правда, эксперты отметили, что соответствие новым стандартам безопасности потребует от акционеров финансовых структур дополнительных затрат и повлечет за собой увеличение стоимости услуг для конечных потребителей.

Константин Соловьев обратил внимание и на угрозы техногенного характера, которые связаны в первую очередь с проблемами энергоснабжения: "Если бы ответственность за сбои в работе энергообеспечивающих организаций перед финансовыми компаниями была столь же высока, как перед детскими садиками, больницами и т. д., то проблем было бы меньше".

В целом эксперты считают, что финансовая сфера должна готовиться к худшему варианту развития событий — к полной блокаде со стороны США и Западной Европы по иранскому сценарию — и в связи с этим искать альтернативные источники технологий, в том числе серьезно поддерживать разработку и производство отечественных технологий в наиболее ответственных областях.