КонсалтИнфоМенеджмент

ООО «КиМ», www.km-ltd.ru, info@km-ltd.com
197375, г. Санкт-Петербург, ул. Вербная, д. 27, оф. 817
Тел. (812) 309-36-64

ИТ-аутсорсинг в банках. Заметки на полях

Ограниченность аутсорсинга в банках - дело не в "зрелости" банков

Причиной ограниченности аутсорсинга в банках является то, что финансовые организации обязаны обеспечивать выполнение требований законодательства и регуляторов к защите информации. В ряде случаев представители сторонней организации получают доступ к информации, которая является коммерческой, банковской тайной, либо персональными данными клиентов. При этом необходимо помнить, что банк ответствен за принятие необходимых мер по обеспечению конфиденциальности и сохранности такой информации. Данные требования в большинстве случаев являются для банков сдерживающим фактором при выборе ИТ-процессов для аутсорсинга.

В то же время банки заключают контракты с субподрядчиками на выполнение проектных работ, которые также могут затрагивать конфиденциальную информацию. В таких случаях заключаются специальные соглашения о неразглашении конфиденциальной информации (Non Disclosure Agreement, NDA), в которых описываются все требования банка к обеспечению субподрядчиком необходимых мер по защите информации и определяется уровень его ответственности за их несоблюдение. Передача ИТ-процессов на аутсорс также должна осуществляться с соблюдением требований по защите информации, наличием механизмов контроля качества их выполнения и возможности повлиять на сами реализуемые процессы. В ходе формирования требований должны учитываться как ущерб, причиненный вследствие утечки информации, так и упущенная выгода.

Мнение Центрального Банка относительно аутсорсинга банковских ИТ-сервисов выразил Артём Сычёв, заместителя начальника ГУБиЗИ Банка России, участник Комитета банковского надзора Банка России на V форуме «Информационная безопасность банков» 16 февраля 2013 года. По его словам — «Сегодня такая практика не только вступает в конфликт с федеральными законами «О банках и банковской деятельности» и «О коммерческой тайне», но и чревата серьёзными рисками. У регулятора неминуемо возникнут претензии к кредитным организациям, применяющим подобную практику».

Обеспечение качества аутсорсинга

Важнейшим аспектом при передаче ИТ-процесса на аутсорсинг является обеспечение необходимого качества результатов предоставляемых поставщиком услуг. Зачастую именно повышение качества является одним из мотивов использования аутсорсинга. Если до передачи процесса отдел информационных технологий сам отвечал за его качество и контролировал процесс, то теперь качество результатов должен обеспечивать провайдер услуг аутсорсинга. В этом случае наличие у поставщика услуг системы менеджмента качества по стандартам серии ISO 9000 является крайне важным условием. Процесс взаимодействия и контроль результатов будут намного прозрачнее и эффективнее, если и в банке также внедрена система контроля качества. При организации такой системы необходимо учитывать важность переданного процесса, риски и последствия для банка в случае несоблюдения необходимого качества выполнения. Банк должен непрерывно управлять процессом взаимодействия с провайдером услуг аутсорсинга и контролировать результаты их выполнения.

Методы контроля должны быть зафиксированы в соглашении с провайдером услуг аутсорсинга об уровне обслуживания (Service Level Agreement, SLA). SLA является основным документом, описывающим обязательства поставщика по обеспечению необходимого качества услуг с указанием его ответственности, цен, уровней обслуживания, методов и параметров контроля результатов, порядка взаимодействия сторон, требований к квалификации специалистов, реакции на непредвиденные обстоятельства и т. д. Более того, необходимо предусмотреть порядок пересмотра указанных в SLA условий с целью их актуализации с учетом изменений в технологиях и бизнесе банка. **Выделять в аутсорсинг нужно только те процессы в ИТ, о которых имеется исчерпывающее представление и которыми могут эффективно управлять как банк, так и провайдер услуг аутсорсинга. Любая попытка реализовать на стороне неясные банку ИТ процессы, либо переложить на провайдера проблемы, пути решения которых неизвестны банку, приведет к тому, что банк не получит ожидаемого результата. Банк просто не сможет адекватно контролировать результаты работы, осуществляемой провайдером услуг.**

Сергей Таран, генеральный директор компании «Онланта»

http://www.youtube.com/watch?v=_X07adH84jA&t=5m15s

Провайдер услуг аутсорсинга не работает с конфиденциальной информацией. В работе используются четкие метрики.

А.Ильина, Управляющий директор Optima services (Группа Optima)

ИТ-обеспечение практически всех операций сегодня является необходимой составляющей банковской деятельности. Причем **значительная часть этих операций относится к числу критических для бизнеса финансовой организации. Передача бизнес-критических функций в аутсорсинг до сих пор (и зачастую обоснованно) представляется неприемлемой для руководства финансовых компаний.**

Законодательство в части защиты персональных данных, коммерческой и прочей информации, а также страховая практика не только не учитывает специфику ИТ-аутсорсинга, но также не защищает интересы ни заказчика, ни сервис-провайдера. Для обеспечения передачи функций (полностью или частично) от внутреннего подразделения заказчика к исполнителю необходимо проделать большую подготовительную работу по выявлению и предупреждению возможных рисков сторон, разграничению зон ответственности, определить размер данной ответственности и условия ее наступления, а также создать сложную схему взаимодействия.

А. Санников, председатель правления СИББИЗНЕСБАНКа

Процесс организации взаимодействия между банком и поставщиком аутсорсинговых услуг был весьма непрост. **Согласование и подписание договоров на оказание соответствующих услуг и сопутствующих этому условий заняло примерно четыре месяца**. При этом банк и поставщик имели опыт предыдущей совместной работы, все основания доверять друг другу и взаимную заинтересованность в проекте.

Я. Алексеев, вице-президент Пробизнесбанка

На аутсорсинг целесообразно отдавать те процессы, которые **могут быть формализованы**, то есть результат и параметры процесса (например, время, цена, качество) могут быть описаны в договоре или соглашении об уровне услуг (так называемые Service Level Agreements).

ООО «КиМ», www.km-ltd.ru, info@km-ltd.com
197375, г. Санкт-Петербург, ул. Вербная, д. 27, оф. 817
Тел. (812) 309-36-64

Система администрирования автоматизированных информационных систем в условиях ИТ-аутсорсинга **противоречит** статье 857 Гражданского кодекса (Банковская тайна) [1], статье 26 ФЗ №395-1 "О банках и банковской деятельности" (Банковская тайна) [2], а также отдельным разделам Положения Банка России №382-П [3]:

- Раздел 2.4 - требования к обеспечению защиты информации при назначении и прав и обязанностей лиц, связанных с осуществлением переводов денежных средств;
- Раздел 2.5 - требования к обеспечению защиты информации на стадиях создания, эксплуатации, модернизации, снятия с эксплуатации объектов информационной инфраструктуры;
- Раздел 2.6 - требования к обеспечению защиты информации при осуществлении доступа к объектам информационной инфраструктуры;
- Раздел 2.9 - требования к обеспечению защиты информации при использовании средств криптографической защиты информации.

В соответствии с методикой оценки соответствия организации защиты информации при переводе денежных средств Банка России, при нарушении требований, определённых в указанных выше разделах обобщённое суждение об организации работ по ИБ **не превысит уровня «сомнительно»**[4].

Процессы и информационные системы, не связанные с основной банковской деятельностью, допускается передавать на обслуживание внешним организациям. При этом взаимодействие с провайдерами услуг аутсорсинга рекомендуется организовывать в соответствии с рекомендациями «Стандарта качества организации деятельности по аутсорсингу информационных технологий в банках», разработанного рабочей группой Ассоциации Российских Банков, не ниже чем по 4-му уровню зрелости процессов аутсорсинга («Управляемый»)[5]

При передаче ИТ-процессов на аутсорс также необходимо учесть возросшие риски — **при аутсорсинге непрерывность бизнеса банка будет зависеть не только от него, но и от провайдера услуг**, что повлечет за собой необходимость контроля мер по обеспечению непрерывности бизнеса самих провайдеров. Финансовая организация должна принять соответствующие шаги, чтобы выявить и оценить возможные последствия проблем и форс-мажорных обстоятельств, возникающих у провайдера услуг, сформировать планы по обеспечению непрерывности бизнеса, в том числе по поиску альтернативного провайдера услуг или возврата деятельности внутрь организации.

Отдельно следует отметить, что предоставление услуг по проведению работ в области защиты информации (в частности администрирования средств защиты информации и средств криптографической защиты информации) **является лицензируемыми видами деятельности** в соответствии с Постановлениями Правительства РФ 79[6] и 313[7] и может осуществляться исключительно лицензиатами ФСТЭК и ФСБ.

ВЫВОДЫ И ЗАКЛЮЧЕНИЯ

- Подавляющее большинство Банков пользуется услугами аутсорсинга (не только ИТ).
- На аутсорсинг передаются **некритичные** сервисы (call-центр, обслуживание АРМ пользователей, периферийных устройства, СКУД).
- Нормативное обеспечение и государственное регулирование накладывает **ограничение на применение в банковской сфере отдельных информационных технологий и решений**, обеспечивающих некоторые эффективные сервисы в других сегментах рынка.
- На практике Банки обращаются к разработчику конкретного сервиса, а **администрирование внедренных систем осуществляют сами.**
- При проработке вопроса о передаче сервиса на аутсорсинг **Банк должен оценить свои риски.**
- Сторонами должно **быть разработано соглашение об уровне обслуживания (SLA)**, определяющее метрики сервисов, ответственность провайдера услуг аутсорсинга перед Банком, требования по информационной безопасности.
- Все процессы, реализуемые провайдером услуг аутсорсинга, **должны быть документированы, согласованы и понятны Банку**. Со стороны Банка должен быть определен куратор по вопросам ИБ и ИТ, согласующий мероприятия, реализуемые в рамках ИТ-аутсорсинга и проекты, предлагаемые Банку.
- В процессе передачи ИТ-процессов на аутсорс должны учитываться не только эффективность и современность с точки зрения ИТ, **но и отраслевые требования**.
- Провайдер услуг должен обладать необходимыми лицензиями, системой менеджмента качеством услуг, являться не только дилером/реселлером, но и иметь подготовленную команду из сертифицированных специалистов по направлению **оказываемых услуг, обладающих достаточным опытом и квалификацией.**

При разработке настоящего документа использовались материалы журналов "Банковские технологии", "BIS Journal" и информационного портала «Bankir.ru» (2012-2013 гг.)

[1] Гражданский кодекс. Статья 857. Банковская тайна

1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.
2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом.
3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

[2] Федеральный закон №395-1 "О банках и банковской деятельности". Статья 26. Банковская тайна.

Кредитная организация ... гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов.
Все служащие кредитной организации обязаны хранить тайну об операциях, о счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

[3] Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств. (утв. Банком России 09.06.2012 N 382-П)

[4] Методика оценки соответствия организации защиты информации при переводе денежных средств требованиям Банка России предполагает 4 уровня соответствия -«неудовлетворительно», «сомнительно», «удовлетворительно», «хорошо». (раздел 7 приложения 1 к Положению Банка России от 9 июня 2012 года N 382-П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств").

[5] Стандарт качества организации деятельности по аутсорсингу информационных технологий в банках от 02.06.2006. http://arb.ru/b2b/docs/411439/

[6] Постановление Правительства РФ №79 от 3 февраля 2012 г «О лицензировании деятельности по технической защите конфиденциальной информации».

[7] Постановление Правительства РФ от 16.04.2012 №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».