ПОСТРОЕНИЕ ГИБРИДНОЙ ЗАЩИЩЕННОЙ ОБЛАЧНОЙ СРЕДЫ КАК ОДИН ИЗ ПОДХОДОВ К ПОВЫШЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СЕРВИСОВ В БАНКАХ*

Качко А.К.,
Финансовый университет при Правительстве Российской Федерации
akkachko@gmail.com

Аннотация. *Вопрос защиты информации финансовой системы Российской Федерации необходимо рассматривать в контексте современных ИТ-технологий, которые позволяют, с одной стороны, сократить издержки и использовать современные подходы к организации ИТ-инфраструктуры, с другой, вносят новые задачи по обеспечению конфиденциальности обрабатываемых данных. В связи с этим подход к построению ИТ-инфраструктуры на основе облачных вычислений с целью повышения уровня безопасности является актуальной задачей, требующей применения стоимостной методики расчета в совокупности с методом оценки риска информационной безопасности (ИБ).*

Ключевые слова: *модели безопасности компьютерных систем, облачные вычисления, публичное облако, частное облако, гибридное облако, требования безопасности, конфиденциальность данных.*

CONSTRUCTION OF HYBRID CLOUD ENVIRONMENTS PROTECTED AS ONE OF THE WAYS TO IMPROVE INFORMATION SECURITY USING CLOUD SERVICES IN BANKS

Kachko A.K.
Financial University under the Government of the Russian Federation

Abstract. *Information security of the financial system of the Russian Federation should be viewed in the context of modern information technologies. They allow you to reduce costs and to use new approaches in creating the IT infrastructure, but they also create new challenges in data security and confidentiality. In this regard, it is necessary to create an approach to build a secure IT infrastructure based on cloud computing, taking into account the cost calculation method and the risk assessment method.*

Keywords: *security model, cloud computing, public cloud, private cloud, hybrid cloud, security requirements, data confidentiality.*

Введение

Российские банки, которые традиционно считаются одними из самых требовательных заказчиков, при выборе и внедрении новых технологий прежде всего обращают внимание на степень проработанности аспектов информационной безопасности. Несмотря на высокую динамику распространения и использования технологии облачных вычислений в бизнес среде, ряд вопросов в области ИБ остается открытым, что подтверждает необходимость исследования и разработки методики построения гибридной защищенной облачной среды (ГЗОС), позволяющей использовать преимущества общедоступной облачной среды (ООС) с возможностью обработки критически важных данных в пределах демилитаризованной зоны, роль которой может выполнять частная облачная среда (ЧОС).*

* I Международный конгресс по информационной безопасности национальных экономик в условиях глобализации «InfoSecurityFinance». Под научной редакцией: **Царегородцева А.В.**

При построении облачной ИТ-инфраструктуры в первую очередь необходимо учитывать главный фактор риска, который заключается в потере контроля со стороны банка над обрабатываемыми данными.

Существует точка зрения, что технология облачных вычислений является эволюционным этапом развития ИТ-индустрии, постепенно сменяющим традиционные модели построения ИТ-инфраструктуры. При этом необходимо отметить, что информационная безопасность, как объект исследования должна рассматриваться в новом контексте, так как часть контролей и управления будет реализована не внутренними силами облачного клиента (банка), а внешней организацией – облачным провайдером.

Аналитика, предоставляемая крупными зарубежными агентствами показывает, что общедоступные (публичные) облачные сервисы становятся все более востребованными и траты организаций на них растут в несколько раз быстрее, чем траты в других сегментах ИТ. По данным IDC, в 2012-2016 гг. темпы роста облачных расходов составят 26,4%, что в 5 раз больше показателей ИТ-индустрии в целом. Gartner в этом году прогнозирует рост рынка публичных облаков на 20%, аналитики Forresterна 60,6%. Исследования InformationWeek[1]показывают, что западные банки используют облачные сервисы в следующих областях:

- 25% используют внешние центры обработки данных (ЦОДы),
- 28% адаптировали бизнес приложения и услуги в облачную среду,
- 21% обеспечивают хранение данных и непрерывность бизнеса,
- 41% проводят тестирование программного обеспечения (ПО).

Основным сдерживающим фактором повсеместного распространения облачных сервисов является опасение потери контроля за критически важными данными. Для понимания российских реалий использования облачных вычислений приведем информацию о проектах в банках (таблица 1), где внедрение позволило сократить часть издержек, связанных с поддержкой ИТ-инфраструктуры и к другим положительным измеримым эффектам[1].

Приведенные проекты прежде всего показывают, что если банки и решаются на использование облачных сервисов, то единственным приемлемым для них вариантом является построение дорогостоящего частного облака с последующим его использованием для своей филиальной и территориальной организационной структуры. Но стоит отметить, что существенным ограничением является то, что частное облако может быть построено только крупными банками, обладающими необходимыми финансовыми возможностями, средние и небольшие финансовые организации должны использовать методику, которая позволит им сочетать преимущества двух типов развертывания облачных сервисов: частного и общедоступного.

К стимулирующим факторам использования общедоступных облачных сервисов относятся:

1) сокращение издержек на поддержку инфраструктуры,

2) повышение гибкости инфраструктуры,

3) перераспределение людских и финансовых ресурсов с поддержки на развитие АБС,

4) истории успеха в крупных западных финансовых организациях.

Как видно, использование облака может предоставить организации большой набор преимуществ, но изменения всегда сопровождаются новыми и часто неожиданными рисками в области информационной безопасности. Самой серьезной проблемой является невозможность со стороны клиента определить где располагаются его данные. Риск потери контроля заставляет организации искать альтернативные варианты использования публичных облачных сервисов с предоставлением возможности управления качеством управления данными в рамках своей инфраструктуры. Это позволит клиенту самостоятельно проводить техническое обслуживание, планировать необходимые исправления, включать дополнительные механизмы защиты данных.

Таблица 1

Проекты внедрения облачных сервисов в банках

Банк	Подрядчик	Проект	Преимущества
Сбербанк	«Сбербанк Технологии»	Крупнейший в Европе ЦОД	Единая централизованная платформа
Центральный Банк	«Инфосистемы Джет»	Развертывание частного IaaSоблака	Рост скорости обработки запросов пользователей. Уменьшение нагрузки на администраторов.
Ситибанк	Нет информации	Облачный ЦОД во Франкфурте	Единая централизованная платформа Предоставление мощностей в аренду
Газпромбанк	Нет информации	Построение частного облака	Эффективное предоставление вычислительных мощностей
Ак Барс банк	«ICL-КПО»		
Райффайзенбанк	Нет информации		
Банк «Интеза»	КРОК	Использование IaaS облака в качестве резервного дата центра	Экономия ресурсов Построение облачной ИТ инфраструктуры
МФК	Группа компаний ЦФТ	Внешняя ИТ-инфраструктуру для АБС как сервис	Сократить затраты на оборудование и его обслуживание Построение инфраструктуры безопасности, контроля доступа, аутентификации, средства обеспечения отказоустойчивости

Также к ключевым проблемам безопасности относят следующие моменты:

1. Отсутствие нормативно-правовой базы. На данный момент в РФ отсутствуют рекомендации надзорных органов по организации работы с облачным провайдером. Сертификация провайдеров, как надежных поставщиков услуг, рассматривается только, как направление будущей работы. По факту организация при миграции данных в облако должна самостоятельно на основе SLA (сервисного соглашения об уровне обслуживания) принимать решение о компетентности провайдера в вопросах управления и организации защиты данных.

2. Отсутствие контроля над данным. При выборе со стороны клиента модели предоставления облачных сервисов уровень его осведомленности меняется от самого минимального в случае выбора SaaS до максимального IaaS. Но даже при использовании инфраструктуры как услуги, клиент не отвечает за аппаратную поддержку, физическую безопасность, системное администрирование.

3. Техническое обслуживание, резервное копирование, аварийное восстановление, управление конфигурацией и обновлениями выполняется на стороне облачного провайдера. Корректность проведения этих работ клиент проверить не может, что усиливает фактор риска увеличения поверхности атаки.

4. Отсутствие информации о физическом местонахождении. Данные одного клиента могут быть распределены по облачным дата центрам, находящимся в разных географических регионах. Соответственно изъятие физических серверов в одном из дата центров может привести к полной потере данных.

5. Низкая пропускная способность. Организация при использовании облачных сервисов должна обеспечивать доступ к ШПД всем территориальным подразделениям, что в ряде регионов РФ становится достаточно сложной задачей.

Указанные проблемы можно решить, применяя разработанный подход для построения гибридной облачной среды [2], что позволит расширить и усилить внутреннюю инфраструктуру безопасности организа-

ции, внедрить более надежные и в то же время гибкие средства управления, сократить риск и стоимость развертывания облачной ИТ-инфраструктуры.

Применение ГЗОС востребовано при решении следующих практических задач.

1. ГЗОС в качестве партнера. При этом критически важные приложения и данные обрабатываются в частной облачной среде (ЧОС), а остальные располагаются в общедоступной облачной среде (ООС).

2. ГЗОС в качестве полигона, когда речь идет о необходимости использования временного рабочего пространства.

3. ГЗОС в качестве дополнительной емкости, когда ООС используется при возникновении внезапных пиковых нагрузок.

Таким образом, гибридное облако – это сочетание компонентов ЧОС и одной облачной инфраструктуры общедоступного пользования, которая обеспечивает прозрачный доступ к ЧОС и может динамически масштабироваться для управления неравномерной нагрузкой. Особо отметим, что при такой организации происходит усиление внутреннего контроля над критически важными приложениями (процессами), которые предприятие не хочет выводить за пределы демилитаризованной зоны, но в то же время остается возможность при необходимости использовать ключевые преимущества облачных вычислений.

Политика ИБ при использовании ГЗОС должна включать в себя решение следующих ключевых задач.

1. Определение ролей доступа к информационным активам организации. Установление контроля над запросами, которые оперируют с данными, построение маршрутов распределения обработки данных для выбора наиболее оптимального варианта развертывания облачной среды.

2. Описание контролируемых показателей для принятия решений. Организация должна провести анализ и оценку производительности критически важных бизнес приложений, сформировать показатели эффективности использования дополнительных мощностей, определить исключения и ограничения при выделении ресурсов в ООС.

3. Соглашения об уровне обслуживания (SLA). Ключевым этапом является необходимость установления уровней надежности как для приложений, так и для всей облачной инфраструктуры, ряд договоренностей с провайдером должно в явном виде быть описано с возможностью проведения внутреннего аудита со стороны клиента с целью проверки заявленных характеристик с реальным уровнем оказания услуг.

4. Гарантированное качество обслуживания. Определение критериев качества предоставляемых услуг, конечно, должно регулироваться лучшими практиками и рекомендациями со стороны ведущих институтов в области стандартизации.

Таким образом, для эффективного управления гибридным облаком необходимо создать всеобъемлющую инфраструктуру в соответствие со следующей разработанной концепцией (таблица 2). Формализованная модель безопасности процесса обработки данных в условиях среды облачных вычислений рассмотрена в [2].

При практической реализации ГЗОС необходимо принять во внимание следующие задачи [3].

1. Адаптация функциональных возможностей локальных приложений для использования в облачной среде, определение способа развертывания данных.
2. Настройка механизма аутентификации пользователей и авторизация рабочих процессов.
3. Проработка механизма передачи данных из ООС в ЧОС.
4. Настройка логики и маршрутизации потоков данных.
5. Проведение синхронизации данных.
6. Поддержка требуемого уровня масштабируемости, производительности и доступности с возможностью выделения дополнительных экземпляров облачных компонентов приложения с целью выполнения различной нагрузки и обеспечения защиты от кратковременных проблем с сетью.

Заключение

Как показало исследование, гибридный тип развертывания облачной среды является одним из наиболее экономичных и эффективных подходов для достижения организацией целей минимизации издержек на ИТ-инфраструктуру с возможностью самостоятельного управления над обработкой критически важных данных.

Таблица 2

Концепция построения ГЗОС

№	Описание этапа	Предпосылки	Основные шаги
I	**Идентификация и оценка информационных активов**	Принято решение о миграции данных в облачную инфраструктуру	Проведение идентификации активов, составления полного перечня информационных ресурсов
		Активы идентифицированы	Проведение оценки стоимости активов
		Оценка проведена	Выделениекритически важных данных и процессов бизнес приложений
II	**Идентификация требований ИБ и определение последовательности обработки данных в ГЗОС**	Критически важные данные и процессы определены	Построение последовательности обработки данных
		Последовательность определена	Идентификация и оценка требования безопасности
		Сформированы условия безопасного функционирования рабочего процесса	Выбор варианта гибридной защищенной облачной среды (ГЗОС)
		Составлена карта присвоения облачных сервисов и данных. Определены основные компоненты ГЗОС и их структура.	Составление вариантов распределения процессов в ГЗОС
III	**Идентификация угроз и построение риск модели ГЗОС**	Варианты распределения в ГЗОС получены	Идентификация угроз и уязвимостей ГЗОС
		Риск модель ГЗОС построена, угрозы и уязвимости определены	Определение приемлемого риска
		Приемлемый риск определен	Применение методики количественной оценки риска для ГЗОС
		Величина риска превышает приемлемый уровень	Принятие решения о включении ЧОС в ГЗОС
IV	**Применение стоимостной методики и построение архитектуры ГЗОС**	Величина риска не превышает приемлемый уровень	Применение стоимостной методики для ГЗОС
		Стоимость ГЗОС не удовлетворительна	Пересмотр приемлемого уровня риска
		Стоимость ГЗОС удовлетворительна	Выбор архитектуры ГЗОС на основе практических рекомендаций

Список литературы

1. ИТ в банках и страховых компаниях 2012. [Электронный ресурс]. — Режим доступа: URL: http://www.cnews.ru/reviews/free/banks2012/ (дата обращения: 13.05.13).
2. Качко, А.К. Формализованная модель безопасности процесса обработки данных в условиях среды облачных вычислений / А. К. Качко // Проблемы информационной безопасности. Компьютерные системы. 2012. №2. С. 14-20.
3. Connecting to the cloud, Part 2: Realize the hybrid cloud model. Mark O'Neill, CTO, Vordel.[Электронный ресурс]. — Режим доступа:URL: http://www.cnews.ru/reviews/free/banks2012/ (дата обращения: 13.05.13).