ОДИН ИЗ ПОДХОДОВ К ПОСТРОЕНИЮ РИСК-МОДЕЛИ БЕЗОПАСНОСТИ ДАННЫХ В КОРПОРАТИВНЫХ СЕТЯХ, ФУНКЦИОНИРУЮЩИХ НА ОСНОВЕ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Царегородцев А.В.,
заведующий кафедрой «Информационная безопасность»
Финансового университета при Правительстве Российской Федерации,
доктор технических наук, профессор
AVTsaregorodtsev@fa.ru

Аннотация. *Широкое распространение и применение облачных вычислений диктует необходимость адаптации и доработки существующих моделей безопасности компьютерных систем. Эта статья в первую очередь направлена на освещение основных вопросов безопасности, имеющих место в облачных средах. И предложен подход к анализу рисков, используемый при принятии решения о миграции критичных данных в облачную инфраструктуру организации.*

Ключевые слова: *угрозы информационной безопасности, анализ информационных рисков, методы управления информационной безопасностью.*

THE APPROACH TO THE DEVELOPMENT OF DATA SECURITY RISK-MODEL IN ENTERPRISE CLOUD COMPUTING NETWORKS

Tsaregorodtsev A.
Head of "Information Security" Department,
Financial University under the Government of the Russian Federation,
Doctor of Sciences (Engineering), Professor

Abstract*. Use of cloud computing applications and services requires review and adaptation of existing formal models for computer security. This article is primarily intended to cover the main safety issues that occur in cloud environments. And the approach to risk analysis used in making decisions about the migration of critical data in the cloud infrastructure of the organization are proposed.*

Keywords*: threats to information security, information risk analysis, methods of information security control.*

Введение

Широкое распространение и применение облачных вычислений может создать революцию в компьютерной индустрии, результатом которой станет предоставление доступа различным организациям к самой современной вычислительной инфраструктуре, платформе и услугам на основе модели, построенной по принципу «оплата по мере пользования». Существует несколько причин, по которым организации будут рассматривать облачные вычисления, как альтернативный способ использования традиционных моделей предоставления ИТ-услуг [1].

- Облачные вычисления являются недорогим решением и доступны для большинства организаций.
- Облачные вычисления обладают гибкостью и возможностью динамической настройки под конкретные требования клиента.
- Облачные вычисления позволяют определить расходы на основании реального потребления ресурсов.
- Увеличивается влияние бизнес пользователей в принятии решений о выборе ИТ-технологий.
- Граница между пользовательскими и корпоративными приложениями постепенно стирается.

Эти причины в ближайшем будущем могут коренным образом изменить традиционные модели предоставления ИТ-сервисов с поддерживающими их организационными структурами.

Необходимо отметить, что самыми критичными вопросами при построении инфраструктуры, основанной на среде облачных вычислений, являются аспекты обеспечения информационной безопасности. Достижение целей информационной безопасности организации, является ключевым фактором для принятия решений об услугах аутсорсинга информационных технологий и, в частности, для принятия решения о миграции информационных активов организации на различные модели предоставления облачных сервисов.

Предварительные оценки экономии на облачных решениях свидетельствуют о возможности сокращения посредством «облаков» затрат на эксплуатацию ИТ в среднем на 60-70%. Подобная экономия открывает возможность переключения высвобождаемых заметных финансовых и кадровых ресурсов на решение новых задач и соответствующую модернизацию экономик.

Однако и аутсорсинг, и, в особенности, облачные технологии, с очевидностью требуют оценки дополнительных рисков в сфере информационной безопасности.

1. Модели предоставления облачных сервисов и развертывания облачных сред

В настоящее время существующую совокупность «облачных сервисов» принято разделять на три основные категории, которые в свою очередь, могут подразделяться на более мелкие группы [2]:

- инфраструктура как сервис (Infrastructure as a Service, IaaS);
- платформа как сервис (Platform as a Service, PaaS);
- программное обеспечение как сервис (Software as a service, SaaS).

Инфраструктура как сервис, по сути, означает аренду вычислительных мощностей, но не физически, а виртуально. Пользователю предоставляется виртуальный сервер с уникальным IP-адресом (или набором адресов), структура для хранения данных и возможность управления этим комплексом.

Платформа как сервис (PaaS) состоит из одного или нескольких виртуальных серверов с установленными операционными системами и специализированными приложениями, которые выбираются исходя из интересов пользователя.

Программное обеспечение как сервис (SaaS) дает возможность пользоваться программным обеспечением провайдера, осуществляющего «облачные» вычисления удаленно через Интернет. Такой сервис позволяет не покупать программное обеспечение, а пользоваться им при возникновении необходимости с помощью различных клиентских устройств. В то же время контроль и управление физической и виртуальной инфраструктурой облака в том числе сети, серверов, операционных систем, хранения, осуществляется «облачным» провайдером.

Национальный институт стандартов и технологий США выделяет следующие обязательные характеристики облачных вычислений:

- самообслуживание по требованию (англ. self service on demand), при котором потребитель самостоятельно определяет и изменяет вычислительные потребности, такие как серверное время, скорости доступа и обработки данных, объем хранимых данных без взаимодействия с представителем поставщика услуг;
- универсальный доступ по сети, услуги доступны потребителям по сети передачи данных вне зависимости от используемого терминального устройства;
- объединение ресурсов (англ. resource pooling), при котором поставщик услуг объединяет ресурсы для обслуживания большого числа потребителей в единый пул для динамичного перераспределения мощностей между потребителями в условиях постоянного изменения спроса на мощности; при этом потребители контролируют только основные параметры услуги (например, объем данных, скорость доступа), но фактическое распределение ресурсов, предоставляемых потребителю, осуществляет поставщик;

- эластичность, означающая, что услуги могут быть предоставлены, расширены, сужены в любой момент времени, без дополнительных издержек на взаимодействие с поставщиком, как правило, в автоматическом режиме;
- учет потребления и объема предоставленных потребителям услуг.

Как видим, все более широкое использование облачных технологий определяется их привлекательностью для пользователя, предоставляющих ему явные выгоды и преимущества. Так, снижаются финансовые издержки, поскольку оплата услуг «облачного» провайдера и покупка собственной техники несопоставимы по уровню расходов. Кроме того, пользователь получает и оплачивает услугу, только когда она ему необходима, и только в том объеме, который он использует. Таким образом, облачные технологии позволяют сократить расходы как на приобретение и модернизацию собственного оборудования, так и на приобретение, поддержку и модернизацию собственного программного обеспечения.

Привлекательность «облачных» вычислений связана как с организационными, так и экономическими моментами. Для малого и среднего бизнеса, безусловно, принципиально, что им предоставляется возможность не создавать собственные структуры, обеспечивающие необходимые вычисления, а использовать «облачные» технологии. Они, как потребители информационных технологий, могут существенно снизить капитальные расходы на создание центров обработки данных, закупку серверного и сетевого оборудования, аппаратных и программных решений.

Что касается крупных компаний, то они, сохраняя за собой собственные структуры, могут передавать «облачному» провайдеру выполнение отдельных функций (например, хранение архивов, фильтрация спама).

Еще одна популярная услуга – электронная почта. «Облачные» технологии позволяют передать ее сервис-провайдеру, который обеспечивает ее своими силами. Не меньший интерес представляет резервное копирование и хранение архивов, которые сервис-провайдер также может взять на себя. Передавая сервис-провайдеру определенные функции, потребитель освобождает себя и от необходимости выполнения ряда сопутствующих им процедур (например, обновления программного обеспечения). Если при стандартных отношениях провайдер получает фиксированное вознаграждение за использование (или возможность использования) его вычислительных ресурсов за определенный промежуток времени независимо от реально использованного объема и времени, то в «облачных» технологиях применяется плата за фактическое использование, когда пользователь оплачивает только тот объем, который им действительно был использован за определенный промежуток времени.

Одним из основных факторов, сдерживающих внедрение технологий облачных вычислений, является гарантированная безопасность обрабатываемых данных. Решением, создающим предпосылки для повышения безопасности облачных вычислений, является разделение их на «публичные» и «частные облака».

Целью такого разделения вычислений является обеспечение защиты конфиденциальных данных с возможностью «смешивания» и сочетания публичных и частных облачных вычислений в зависимости от потребности организации.

Существуют следующие базовые варианты развертывания облачных сред.

Во-первых, частное (закрытое) «облако», используемое для сервисов внутри кредитно-финансовой организации, являющейся и заказчиком, и поставщиком услуг. Компания или банк создает «облако» для себя в рамках своей организации, например, для снижения затрат, улучшения логистики и т.д. «Частные облака» представляют собой вычислительные ресурсы, функционирующие в доверенной зоне корпоративной сети за межсетевым экраном.

Во-вторых, публичное (общедоступное) «облако», используемое облачным провайдером для предоставления внешним заказчикам сервисов облачной структуры. Поставщик услуг обеспечивает предоставление сервисов в соответствии с соглашением об уровне предоставления услуг (SLA), которое не всегда обеспечивает требуемый финансовыми институтами

уровень безопасности вычислений и конфиденциальности данных.

В Gartner выявили четыре основных фактора риска облачных решений, которые необходимо учитывать при заключении договора с провайдером. Основные факторы риска, согласно оценке Gartner, следующие.

Во-первых, при анализе договора о предоставлении облачного сервиса необходимо обратить внимание на то, как составлен контракт: нацелен ли он на защиту прав потребителя или же на то, чтобы в большей мере защитить права провайдера. Gartner советует обратить особое внимание на политику и процедуры обработки данных, дополнительные процедуры резервного копирования, а также на плату за доступ к информации после расторжения контракта. Все эти факторы могут привести к возникновению дополнительных затрат.

Во-вторых, в Gartner рекомендуют: чтобы провайдер оправдал ожидания заказчика, следует обратить внимание на четкое перечисление и «роспись» в договоре услуг, которые обязуется предоставить провайдер.

В-третьих, провайдер может менять условия договора в одностороннем порядке. Поэтому в Gartner советуют получить гарантию провайдера, что контракт не будет изменен в течение определенного срока и что заказчик будет поставлен в известность обо всех изменениях в договоре.

Наконец, существует риск размытых обязательств провайдеров. Перед тем как вложить средства в облачный сервис, необходимо просчитать, что придется предпринять, если провайдер не справится, каковы риски отказа сети между организацией и провайдером, включая риски «последней мили».

И третий вариант развертывания – гибридное «облако», использующее совместно два вышеперечисленных варианта развертывания.

Для определения пропорций использования «публичных» и «частных» облаков в интересах кредитно-финансовых организаций необходимы соответствующие стандарты и методологические решения. В настоящее время над этой проблемой работает коллектив консорциума Enterprise Cloud Leadership Council. Участниками данного консорциума являются Bank of America, Credit Suisse, Deutsche Bank и другие финансовые организации. Разработкой, стандартизацией и продвижением решений для обеспечения различных аспектов безопасности облачных вычислений для банковского сообщества занимается и другая организация - Cloud Security Alliance.

2. Оценка безопасности виртуализированных сред

Полная и частичная виртуализация: Существуют два вида виртуализации в парадигме облачных вычислений. В полной виртуализации, вся аппаратура архитектуры системы реплицируется виртуально. А при частичной виртуализации операционная система модифицирована таким образом, что она может быть запущена одновременно с другими операционными системами. VMM (монитор виртуальных машин), представляет собой программный слой, который позволяет абстрагироваться от физических ресурсов, используемых несколькими виртуальными машинами. VMM предусматривает виртуальный процессор и другие виртуальные системы, такие как устройства ввода/вывода, хранения, памяти и т.д.

При оценке безопасности виртуализированных сред были обнаружены уязвимости во всех виртуализациях программного обеспечения, которые могут быть использованы злоумышленниками для прохождения некоторых ограничений безопасности и/или с целью повысить свои привилегии.

Рассмотрим основных поставщиков облачных сервисов, предоставляющих своим услуги по всем основным направлениям облачных вычислений:SaaS, PaaS и IaaS (табл. 1). Следует отметить, что представлен не полный перечень провайдеров, а лишь самые основные игроки данного сегмента рынка информационно-телекоммуникационных услуг.

Таблица 1

Крупнейшие поставщики облачных услуг

Услуга	Фирма-провайдер
IaaS	Amazon EC2, Amazon S3, GoGrid
PaaS	Google App Engine, Microsoft Azure Services, Amazon, Elastic Map Reduce
SaaS	Salesforce, Google Docs

В таблице 2 приводятся результаты оценки текущего состояния механизмов безопасности, реализованные крупнейшими поставщики облачных услуг. Представленная в таблице 2 данные, основаны на информации доступной в открытых источниках на официальных сайтах этих поставщиков.

Таблица 2

Механизмы безопасности, реализованные крупнейшими поставщики облачных услуг

Механизм безопасности	Результат
Восстановление пароля	90% используют стандартные методы для большинства предоставляемых услуг, в то время только 10% используют сложные методы и механизмы
Механизм шифрования	40% используют стандартное шифрование SSL, при этом 20% используют механизмы шифрования за дополнительную плату. 40% также используют методы реализованные по принципу протокола HTTPS.
Расположение данных	70% определили местонахождение своих ЦОДов в некоторых страна, в то время как 10% имеют единственное местоположение. 20% относят данный вид информации к конфиденциальной
Доступность истории	В 40% присутствует заявленное время простоя, наряду с результатом в потере данных, в то время как в 60%-ых случаях доступность данных высока.
Частная собственность / Открытость	Только 10% провайдеров имеют открытые механизмы
Мониторинг сервисов	70% оказывают данные услуг за дополнительную плату, в то время как 10% используют автоматические методы. 20% не предоставляют данную информацию.

3. Оценка риска в облачных вычислениях

Современная технология обеспечения безопасности дает возможность создания определенного уровня доверия в области облачных технологий. Например, SSL (протокол Secure Socket Layer), цифровые подписи и аутентификация протоколов для доказательства методов аутентификации и контроля доступа для управления авторизацией. Однако сами методы не могут дать методику определения достоверности. SSL, например, не может сам по себе доказать, что сообщение между сервером и несколькими хостами является безопасным. Кроме того, есть вероятность нескольких точек отказов в облачной среде.

Современные технологии безопасности не обладают эффективными инструментами для определения достоверности информации. Анализ отечественных и зарубежных публикаций показал, что большинство авторов определяют доверие следующим образом. «Доверие является определенным уровнем субъективного представления о вероятности, с которой агент будет выполнить определенное действие, в то время как мы можем контролировать такие действия, и в контексте, в котором он касается наших собственных действий». Исходя из этого определения, можно сказать, что доверие является субъективной оценкой и зависит от тех действий, которые мы не можем контролировать.

Можно выделить три вида моделей доверия в распределенных системах:

- прямое (полное) доверие;
- доверительные отношения;
- допустимое доверие.

В облачных технологиях, в которых данные и программы, по сути, являются трансграничными, доверительные отношения может иметь решающее значение для определенного типа приложений. Модель прямого доверия существует в облаке, когда есть общая сущность доверия, когда выполняются все заявленные аутентификации и генерации учетных данных, которые связаны с конкретными лицами.

Ключевая разница с другими моделями в том, что прямая модель доверия не позволяет делегировать заявленные аутентификации. И каждая проверяющая сторона должна использовать эту структуру. Примером такого типа доверия является использование PKI (Инфраструктура Публичного Ключа), где проверка подлинности на основе ключевых центров сертификации (ЦС) дает все виды доверительных отношений. Ответственность безопасной передачи данных лежит в руках сертифицирующих органов (удостоверяющих центров).

Очень сложно найти подходящую единицу измерения для определения доверия, но есть несколько производных переменных (например, данные о затратах), которые могут быть использованы для его описания. На основании значимых факторов безопасности строится матрица доверия и проводится анализ рисков безопасности данных. Для построения матрицы доверия, некоторые эвристики могут быть использованы для выбора параметров безопасности.

В облачной среде, стоимость данных, как правило, зависит от оценки пользователей, основанной на критичности данных. Существует большое многообразие факторов, влияющих на критичность данных. Так, например, конфиденциальная коммерческая информация может быть важной, и поэтому ей назначается более высокая стоимость по сравнению с менее критическими данными.

Кроме того, история провайдера может являться допустимым параметром для оценки риска. История включает в себя профиль провайдера, его заслуги в прошлом. Если пользователи не удовлетворены качеством конкретного сервиса, предоставляемого провайдером, это существенно повлияет на фактор доверия. Если поставщик услуг не обладает хорошей историей безопасности данных (например, есть последняя запись является записью о нарушении безопасности), то она может также уменьшить фактор доверия. При этом и другие переменные также могут быть использованы для создания матрицы доверия, например, поддержка шифрования, стоимость услуги, поддержка мониторинга и т.д.

Наряду с матрицей доверия, существуют ряд параметров также используемых для измерения доверия, позволяющие точно настроить доверительные переменные. Параметры, которые мы выбираем в этой категории – это расположение данных, соблюдение установленных норм.

Как правило, вышеперечисленные параметры используются, как механизм поддержки в матрице доверия. Они используется в качестве проверки факторов, которые обеспечивает поддержку принятия решения при анализе рисков.

Используя матрицу доверия, где оси отражают используемые переменные, свяжем их по значению друг с другом. Рисунок 1, дает графическую интерпретацию матрицы доверия для анализа риска, где низкий риск – зона высокого доверия (high trust zone), а высокий риск – зона низкого доверия (low trust zone):

Здесь по оси X представлены данные по стоимости (data cost); по оси Y – историю услуг провайдера (provider's history) и по оси Z – информация о местоположении данных (data location).

Теперь очевидно, что высокая стоимость данных наряду с плохой историей поставщика услуг и в сочетании с очень критичными местами размещения данных приведет к более высокому риску – меньшему доверию.

Зона высокого доверия может указать риск безопасности для текущих операций, а также для будущих сделок с этим сервисом провайдера. Такой превентивный подход к оценке риска рассматривается как часть профилактической или реактивной меры. Например, добавленный уровень аутентификации и/или проверки пользователя может быть использован для процессов, которые связаны с зоной низкого доверия. Этот метод может быть использован для измерения доверия и для осуществления последующих операций с данными. На основе этого метода можно определить доверительные действия для всех будущих сделок с поставщиком услуг.

Согласно данным, приведенным IDC (International Data Corporation), пока еще для обеспечения целостности и непротиворечивости данных, хранимых в облаках, используются только криптографические

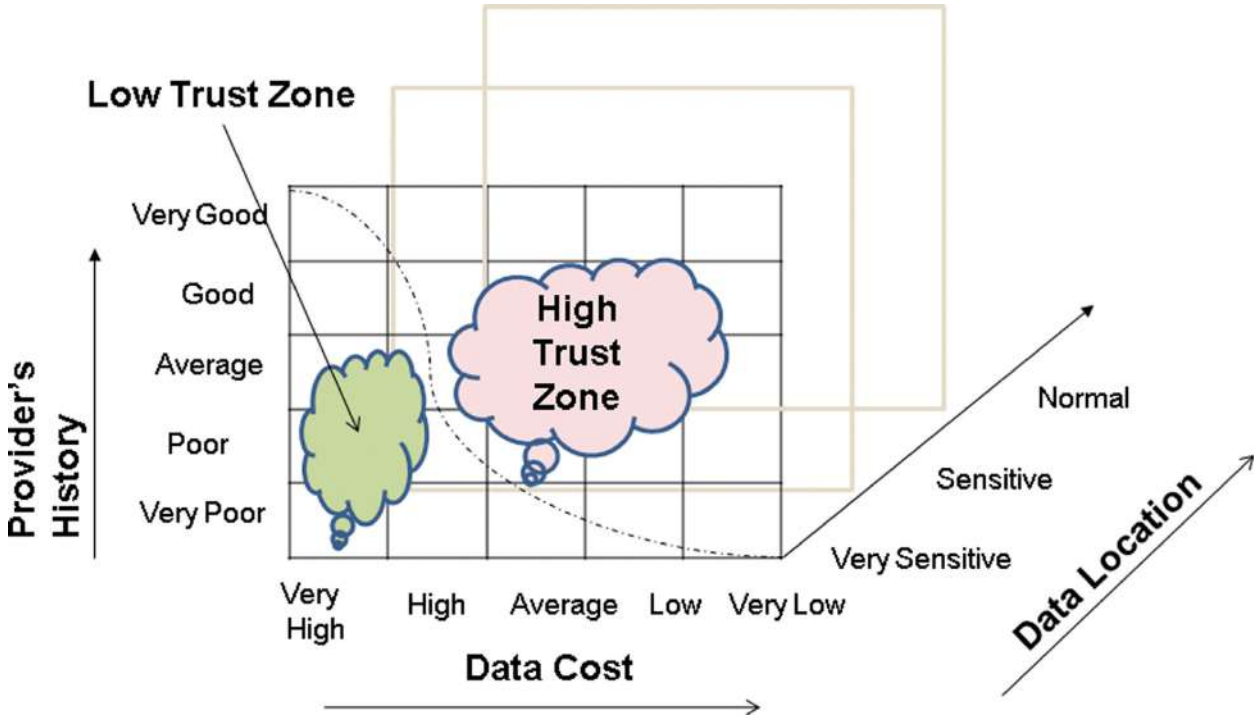

Рис. 1. Матрица доверия для анализа степени риска

средства защиты. В техническом описании на AWS (Amazon Web Services) рассматривается физическая безопасность, резервное копирование и использование соответствующих сертификатов [3]. Аналогичным образом, другие поставщики, такие как Google, Microsoft и т.д. рассматривают альтернативные механизмы обеспечения безопасности в облаке.

В работе [4] показаны семь значимых рисков, которые клиент должен оценить, чтобы использовать инфраструктуру облачных вычислений. В дополнение к этим семи рискам, мы также определили ряд других определяющих факторов, которые должны учитываться при выборе провайдера облачных сервисов. Эти вопросы включают хранение данных, безопасность сервера, привилегированный доступ пользователей, виртуализацию и переносимость данных. Для принятия риска безопасности данных предлагается определить ключевой набор переменных доверия, в результате чего, возможно построения доверительной матрицы, основанной на безопасности данных в облачных вычислениях.

Заключение

Достижение целей информационной безопасности (ИБ) организации становится одним из ключевых факторов для принятия решений об услугах аутсорсинга информационных технологий и, в частности, для принятия решения о миграции организационных данных, приложений и других ресурсов на инфраструктуру, основанную на среде облачных вычислений.

В настоящее время отсутствует системный подход к анализу рисков в средах облачных вычислений. В данной статье представлен один из подходов к анализу рисков безопасности данных. Предложенный подход легко адаптируется для автоматизации процесса анализа рисков в корпоративных сетях организаций, функционирующих на основе технологии облачных вычислений.

Список литературы

1. Царегородцев А.В., Качко А.К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность. – М.: Изд-во “НБ Медиа”, 2011. - №5. – С. 25-34.
2. Царегородцев А.В., Качко А.К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // Национальная безопасность. – М.: Изд-во “НБ Медиа”, 2012. - №1(18). – С. 46-59.
3. Overview of Security Processes (2011).
4. Brodkin, J. Seven Cloud Computing Security Risks (2008), http://www.gartner.com/DisplayDocument?id=685308.