ОДИН ИЗ ПОДХОДОВ АНАЛИЗА РИСКОВ БЕЗОПАСНОСТИ ДАННЫХ В ОБЛАЧНЫХ СРЕДАХ

Царегородцев А.В.
AVTsaregorodtsev@fa.ru
Савельев И.А.
iasavelyev@fa.ru
Мухин И.Н.
ilyuha1999@mail.ru
Финансовый университет при Правительстве Российской Федерации

Аннотация. *В ответ постоянно растущим потребностям хранения и обработки данных в настоящее время существует тенденция использования облачных вычислительных сред. Наряду с этим принятие парадигмы облачных вычислений может иметь как положительные, так и отрицательные эффекты. Эта статья в первую очередь направлена на освещение основных вопросов безопасности, имеющих место при использовании в облачных средах. Предлагается подход анализа рисков, используемый на этапе выбора перспективных облачных сервисов, прежде чем доверить конфиденциальные данные провайдерам, предлагающим услуги по размещению в среде облачных технологий.*

Ключевые слова: *облачные технологии, анализ рисков, безопасность данных.*

ONE OF THE APPROACHES OF RISK ANALYSIS OF DATA SECURITY IN CLOUD COMPUTING ENVIRONMENTS

Tsaregorodtsev A.V.
Savelev I.A.
Mukhin I.N.
Financial University under the Government of the Russian Federation

Abstract. *There is a growing trend of using cloud environments for ever growing storage and data processing needs. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. This paper primarily aims to highlight the major security issues existing in current cloud computing environments. It's carried out a survey to investigate the security mechanisms that are enforced by major cloud service providers. It's proposed a risk analysis approach that can be used by a prospective cloud service for analyzing the data security risks before putting his confidential data into a cloud computing environment.*

Keywords: *cloud computing environments, risk analysis, data security.*

Введение

В среде облачных вычислений, основная инфраструктура используется по мере необходимости. Например, для обработки запроса пользователя, поставщику услуг требуется привлечь необходимые ресурсы по заявленному требованию, выполнить специализированные работы, а затем отказаться от ненужных ресурсов как правило после того, как работа считается выполненной. В отличие от традиционных вычислений, реализуемых под контролем пользователя, в облаке, данные и приложения осуществляется службой провайдера. Все это приводит к естественному недоверию по поводу безопасности данных, а также возникновению естественных вопросов к защите от внутренних, так и внешних угроз. Несмотря на это, преимущество в использовании таких инфраструктур очевидны: снижение стоимости на техническое обслуживание, гибкое масштабирование и т.д. – убедительные причины для предприятий, при принятии положительного решения об использовании облаков.

Как правило, при использовании облаков, хранение и обработка данных выполняются в едином центре обработки данных. В этих случаях преимущества использования облачных вычислений могут быть связаны с рисками для безопасности. Единственная

точка отказа не приводит к полной потери данных. Как показано на рисунке 1, данные могут быть расположены на нескольких географически распределенных узлах в облаке. Однако, существует вероятность возникновения нескольких точек, где может произойти нарушение безопасности. По сравнению с традиционной в обработкой в локальных сетях, данные нарушения безопасности трудно отслеживать в облачной среде.

В этой статье рассматриваются преимущества и недостатки (в контексте информационной безопасности) использования облачной среды. Проводится анализ основных поставщиков облачных сервисов для оценки важности внедрения определенных дополнительных механизмов, связанных с вопросами безопасности [6].

В данной статье рассматриваются механизмы безопасности, которые используются основными поставщиками услуг. Анализ подтверждает, что в контексте безопасности данных доверие является важнейшим элементом, которое в настоящее время отсутствует в большинстве случаев, как в России, так и за рубежом. Мы считаем, что отсутствие доверительного взаимодействия между поставщиком облачных сервисов и пользователей основано в первую очередь на том, что поставщики услуг используют разнообразные механизмы, чтобы сохранить высокий уровень защиты данных, однако закрытость этой информации и явная несогласованность приводит к определенной доли недоверия (в контексте конфиденциальности данных) среди пользователей облачных сервисов.

Для построения улучшенного доверительного механизма предлагается подход анализа риска, направленного в первую очередь на пользовательскую перспективу использования облака, на начальном этапе, до того как положить их разместить свои конфиденциальные данные в облако. Наш подход основан на идее модели доверия, массово используемой в распределенных информационных системах. Ожидается, что идея доверительного управления и представление его в анализе рисков будет использоваться для обеспечения приемлемого уровня безопасности данных в облачных областях.

Резюмируя материалы, отраженные в данной статье, можно акцентировать внимание на следующих тезисах:

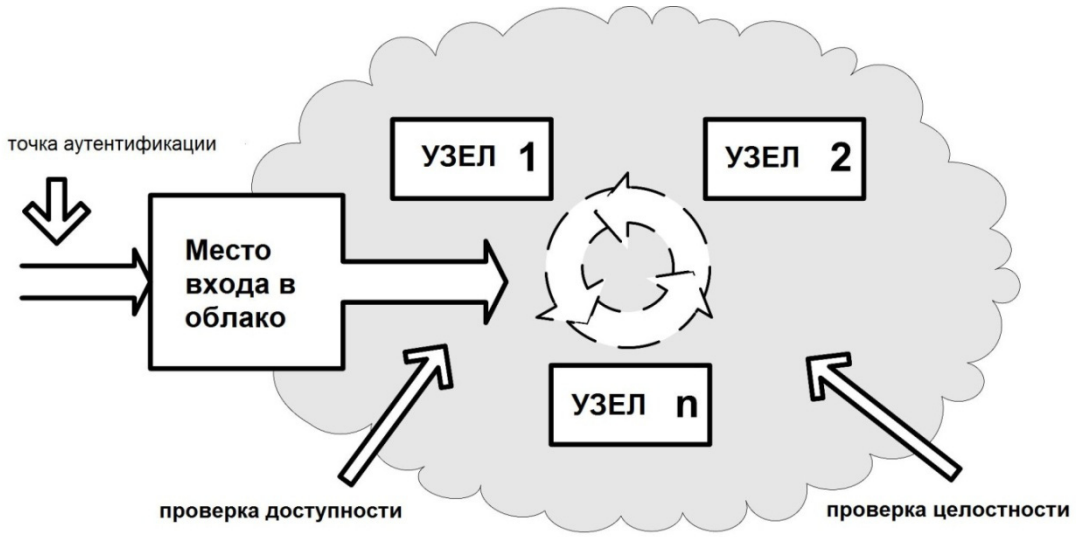

Рис. 1. Типичные контрольно-пропускные пункты защиты информации в облачной среде

1. Исследуются основные вопросы безопасности в парадигме облачных вычислений.
2. Проводится анализ крупных поставщиков облачных сервисов для изучения механизмов безопасности в контексте вопросов информационной безопасности.
3. Кроме того, предлагается подход анализа степени риска, который может использоваться возможным пользователем сервисов облака, чтобы оценить риск защиты информации.

Проблемы и вопросы информационной безопасности в облачных средах.

IaaS (инфраструктура как услуга), PaaS (платформа как услуга) и SaaS (программное обеспечение как услуга) - три основные модели облачных представлений. Каждая из этих модели обладает различным влиянием на безопасность приложений. Тем не менее, в типичных сценариях, при которых приложение размещается в облаке, возникают два глобальных вопроса безопасности:

- Как обеспечивается безопасность Данных?
- Насколько безопасен Код?

В облачных средах принято считать, что качество обслуживания напрямую соответствует стоимости, которую запрашивает провайдер услуги от потребителя. Безопасность, доступность и надежность являются основные проблемами качества пользователей облачного сервиса. Некоторые исследователи предполагают, что безопасность это именно тот аспект среди всех прочих проблем облачных технологий, которому требуется уделять особое значение.

Преимущества безопасности в облачных технологиях

Работа сервисов предоставляемых провайдерами связана с очень большими системам. Они имеют сложные процессы и требуют высококвалифицированный персонал для эксплуатации систем, каждый из которых в отдельности не может иметь полный доступ к информационным ресурсам в целом. В результате, существует множество прямых и косвенных преимуществ информационной безопасности при использовании облачных технологий. Здесь приводятся некоторые ключевые преимущества безопасности данных в облачных средах:

Централизация данных: в облачной среде, сервис-провайдер заботится о вопросах хранения данных, и малому бизнесу нет необходимости тратить много денег на аппаратную составляющую хранения данных. Кроме того, хранение данных в облаке, а следовательно возможность централизованного хранения, может обеспечить обработку данных быстрее и, как правило, дешевле. Это особенно полезно для малого бизнеса, который не имеет возможности тратить дополнительные деньги на специалистов по безопасности и администрированию систем хранения данных.

Реагирование на инциденты: Поставщики IaaS услуги могут поднять выделенный «контрольный сервер», который может использоваться по требованию. Всякий раз, когда зафиксировано нарушение безопасности, сервер может быть поднят в статус онлайн. В некоторых случаях резервная копия сервиса может быть легко сгенерирована и помещена на облако, не затрагивая нормальный ход бизнеса, тем самым не нарушая непрерывности бизнеса.

Контрольное время проверки изображения (FIVT): Некоторые реализации облачных технологий хранения данных подвергаются дополнительным защитам с применением криптографических атрибутов таких как: определение контрольной суммы или вычисление хэш-функции. Например, Amazon S3 вычисляет MD5 (Message-Digest Algorithm 5) автоматически при сохранении объекта. Поэтому в теории, внешние инструменты, требующие много времен на генерирование контрольных сумм MD5, устраняется.

Журналирование: В традиционной модели вычислительных систем, журналирование часто осуществляется задним числом. В общем, недостаточно выделенного места на диске делает его либо не существующим, либо минимальным. Однако, в облаке, потребность хранения в стандартных логах автоматически решена.

Недостатки безопасности в облачных технологиях

Несмотря на все преимущества безопасности, облачные технологии не лишены ряда проблем информационной безопасности:

Расположение данных: Концепция реализации облачных технологий основана на том, что пользователи не знают о точном местонахождении центров обработки данных, а также не имеют никакого контроля над физическим доступом к этим данным. Наиболее известные провайдерам облачных сервисов имеют центры обработки данных по всему миру. Некоторые поставщики услуг также могут воспользоваться своими глобальными центрами обработки данных. Однако, в некоторых случаях, приложения и данные могут храниться в странах, где последние имеют свои судебные интересы. Например, если пользовательские данные хранятся в стране X, то поставщики услуг будут подвергаться требованиям безопасности и правовым обязательствам страны X, что, как правило, затрудняет деятельность пользователя, не знакомого с юридическими издержками данной страны.

Расследование: Расследование незаконной деятельности может быть невозможно в облачной среде. Облачные сервисы особенно трудно расследовать, так как данные для нескольких клиентов могут быть распределены и могут также быть размещены на многих центрах обработки данных. Пользователи имеют мало информации о топологии сети, лежащей в основе среды. Поставщик услуг также может налагать ограничения на сетевую безопасности пользователей услуг.

Данные сегрегации: Данные в облаке, при использовании глобального облака, располагаются вместе с данными других клиентов. Шифрование не может быть единственной возможной панацеей решения проблемы информационной безопасности. Это связано с сегрегацией данными. В некоторых ситуациях, клиенты могут не хотеть зашифровывать свои данные, из-за вероятности повреждения данных при сбои шифрования.

Долгосрочная жизнеспособность: Поставщики услуг должны обеспечить безопасность данных в случаях возможного изменения своего юридического статуса, таких как слияние и поглощение. Клиенты должны обеспечиваться данными в таких ситуациях. Поставщики услуг также должны убедиться, что данные в безопасности при негативных кондициях, таких как длительные отключения и просто и т.д.

Компромитирование серверов: В среде облачных технологий, пользователи не имеют возможности выбора использованием физического инструментария. В ситуации, когда сервер находится под угрозой, они должны выключать сервер, пока они не восстановят предыдущие работоспособные резервные копии данных. Это может являться еще одной причиной наличия проблемы безопасности данных.

Соответствие нормативам: Традиционные поставщики услуг подвергаются проверкам внешних аудиторов и сертификаты безопасности. Если поставщик облачных сервисов не придерживаются этих аудиты, что в настоящее время не запрещено, то это приводит к очевидному снижению доверия со стороны клиентов.

Восстановление: Провайдеры облачных услуг должны обеспечить безопасность данных в случае естественных и техногенных катастроф. Как правило, это достигается репликацией данных на нескольких узлах. Однако в случае любого такого нежелательного события, поставщик должен сделать полное и быстрое восстановление.

Вопросы безопасности в виртуализации

Полная и частичная виртуализация: Существуют два вида виртуализации в парадигме облачных вычислений. В полной виртуализации, вся аппаратура архитектуры реплицируется виртуально. Тем не менее, в области 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 виртуальными системы, такие как устройства ввода/вывода, хранения, памяти и т.д.

Изоляция VMM каждого экземпляра гарантирует, что различные экземпляры, работающие на той же физической среде изолированы друг от друга. Много ошибок уязвмостей было обнаружено во всех популярных VMM, что позволяют обойти VM (Virtual Machine). Уязвимости были обнаружены во всех виртуализациях программного обеспечения, которые могут быть использованы злоумышленниками для прохождения некоторых ограничений безопасности и/или повысить свои привилегии. Ниже приведены несколько примеров:

- Уязвимость в Microsoft Virtual PC и Microsoft Virtual Server дает возможность пользователю операционной системы с правами «гостя» запускать код хозяина или другого гостевого пользователя операционной системы.
- Обнаружена уязвимость в общий папке VMware, что дает пользователей гостевой системы право на чтение и запись к любой части хозяина файловых систем, включая системную папку и другие конфиденциальные файлы.
- Уязвимость в Xen может быть использована гостем для выполнения произвольных команд от имени корневого пользователя домена.

Проведя анализ основных поставщиков облачных сервисов для расследования механизмов безопасности, за основу взяты десять основных поставщиков облачных услуг. Эти провайдеры предоставляют своим услуги по всем основным направлениям облачных вычислений, в том числе SaaS, PaaS и IaaS. Таблица 1 показывает список услуг. Следует отметить, что представлен не полный перечень провайдеров, а лишь самые основные игроки данного сегмента рынка информационно-телекоммуникационных услуг.

В таблице 2 приводятся результаты оценки текущего состояния механизмов безопасности. Информация, представленная в таблице 2, реализована на основе информации доступной в открытых источниках на официальных сайтах этих поставщиков.

Подход оценки рисков

Поставщики облачных технологий используют различные механизмы для обеспечения безопасности. Однако существуют два основных вопроса, связанных с обеспечением информационной безопасности:

- Как оценить риск для безопасности данных, прежде чем приступить к работе в облаке?
- Как убедить клиентов, что их данные и программы в безопасности в помещениях провайдера?

Если пользователь облачного сервиса способен оценить риск безопасности данных, то он может определить уровень доверия с поставщиком услуг. Если есть высокий риск безопасности данных, то это приводит к снижению доверия.

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

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.

Пользователю услуг необходимо иметь четкое представление о методах, принятых поставщиков услуг для обеспечения безопасности. 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 более конкретное понятие достоверности. SSL, например, не может сам по себе доказать, что сообщение между сервером и несколькими хостами является безопасным. Кроме того, как говорилось выше, есть вероятность нескольких точек отказов в облачной среде.

Современные технологии безопасности не обладают дополнительными инструментами для определения эффективной достоверности информации. Анализ отечественных и зарубежных статей 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» [1]. Исходя из этого определения, можно сказать, что доверие является субъективной оценкой и зависит от тех действий, которые мы не можем контролировать.

Три вида моделей доверия были обсуждены в распределенных системах:

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

В облачных технологиях, в которых данные и программы пересекают организационные границы, доверительные отношения и допустимое доверие могут иметь решающее значение для определенного типа приложений. Модель прямого доверия в облаке существует в облаке, когда есть общая сущность

доверия, когда выполняются все заявленные аутентификации и генерации учетных данных, которые связаны 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 корневых центров сертификации (ЦС) дает все виды доверительных отношений. Ответственность безопасной передачи данных лежит в руках сертифицирующих органов (удостоверяющих центров).

Оценка риска. Использование матрицы доверия

Хотя ни одна единица измерения не является адекватной для определения доверия, несколько зависимых переменных (например, данные о затратах), могут быть использованы для его описания. На основании значимых факторов безопасности строится матрица доверия анализ рисков безопасности данных. Для построения матрицы доверия, некоторые эвристики могут быть использованы для выбора параметров безопасности. Тем не менее, простой способ, выбора факторов безопасности является их приоритетность на основе субъективных мнений выбора двух наиболее важных параметров. Например для построения матрицы доверия можно взять две следующие переменные: стоимость данных и история провайдера.

В облачной среде, стоимость данных может варьироваться от оценки пользователем, основанной на критичность данных. Критичность данных должна быть вычислена службой пользователей. Существует большое многообразие факторов, влияющих на критичность данных. Так, например, конфиденциальная коммерческая информация может быть важной, и поэтому мы можем назначить ему более высокую стоимость по сравнению с менее критическими данными.

Кроме того, история провайдера может являться допустимым параметром для оценки риска. История включает в себя профиль провайдера, их заслуги в прошлом. Если пользователи неудовлетворенны качеством конкретной службы (провайдером), они могут выражать свое мнения. 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. Однако другие переменные также могут быть использованы для создания матрицы доверия. Некоторые из этих переменных могут быть: поддержка шифрования, стоимость услуги, поддержка мониторинга и т.д.

Переменные параметры

Наряду с переменными матрицы доверия, существуют несколько параметров, используемых для измерения доверия, примененные, чтобы точно настроить доверительные переменные. Параметры, которые мы выбираем в этой категории: расположение данных, соблюдение установленных норм.

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

Анализ рисков

Можно предположить, что используя матрицу доверия, где оси отражают используемые переменные, переменные следует связать по значению друг с другом. Рисунок 2, представляет собой матрицу доверия для анализа степени риска, представляющей собой низкий риск / зона высокого доверия и, высокий риск / низкая зоны доверия: где: ось X представляет данные стоимости (data cost); ось Y представляет историю услуг (provider's history) и ось Z представляет данные о местоположении (data location).

Теперь очевидно, что высокая стоимость данных с плохой историей поставщика услуг в сочетании с очень чувствительными местами приведет к более высокому риску / меньшему доверию.

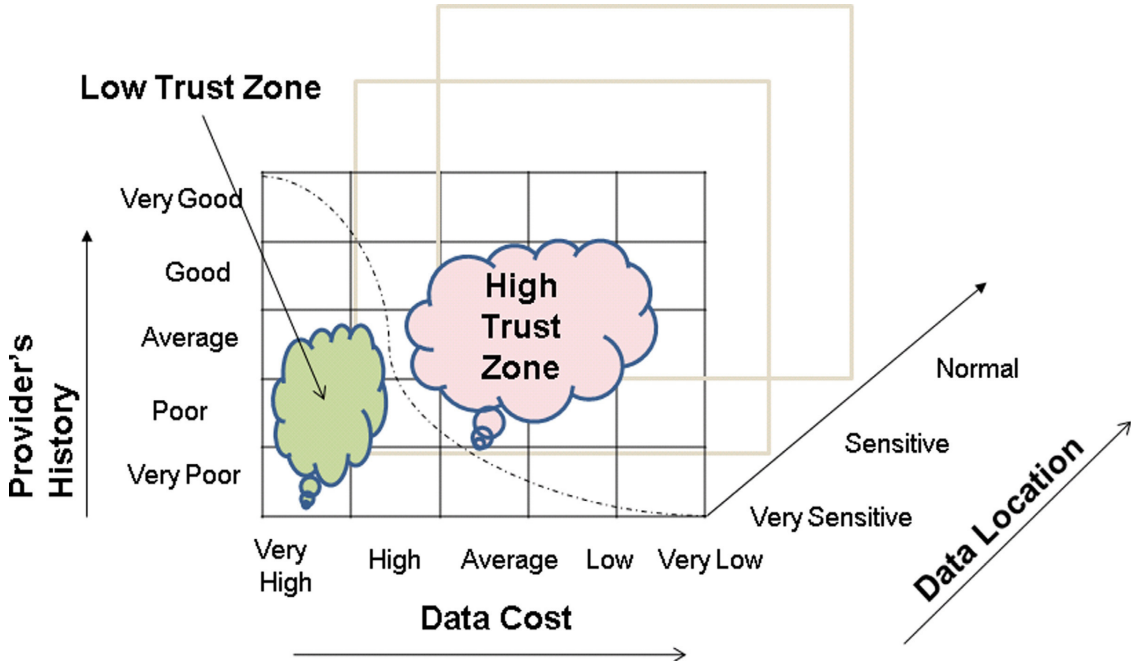

Рис. 2. Матрица доверия для анализа степени риска

Зона высокого доверия может указать риск безопасности для текущих операций, а также для будущих сделок с этой службой провайдера. Как превентивный подход оценка риска рассматривается как часть профилактической или реактивной меры. Например, добавленный уровень аутентификации и/или проверки может быть использован для деятельности, которая связана с зоной низкого доверия. Этот метод может быть использован для измерения доверия и для осуществления всех будущих сделок. На основе этого метода, можно определить доверительные действия, для всех будущих сделок с поставщиком услуг.

Согласно данным, приведенным IDC (International Data Corporation), облачные услуги все еще находятся в ранней стадии развития. Также в ряде исследований дается представление известных криптографических инструментов для обеспечения целостности и непротиворечивости данных, хранимых в облаках. Некоторые программно-аппаратные решения по-прежнему требуют тестирования на некоторых данных в реальном времени, чтобы проверить их пригодность и простоту использования. В техническом описании на AWS (Amazon Web Services) обсуждается физическая безопасность, резервное копирование и сертификаты в их контексте [2]. Аналогичным образом, другие поставщики, такие как Google, Microsoft и т.д. обсудили вопросы безопасности в облаке компьютерами Ing [3, 4].

Хайзер выявил те семь значимых рисков [5], которые клиент должен оценить, чтобы использовать инфраструктуру облачных вычислений. В дополнение к этим семи рискам, мы также определили несколько других крупных факторов, которые должны быть рассмотрены провайдеров облачных сервисов. Эти вопросы включают хранение данных, безопасности сервера, привилегированный доступ пользователей, виртуализацию и переносимость данных. Для принятия некоторых идей моделирования доверия, предлагается определить ключевой набор переменных доверия, в результате чего, возможно построения доверительной матрицы, основанной на вопросах безопасности в области облачных вычислений.

Заключение

С продвижением облачных технологий и увеличения числа облачных пользователей, размеры безопасности данных будет постоянно увеличиваться. В данной статье приведены результаты анализа данных рисков для безопасности и уязвимостей, которые присутствуют в текущих средах облачных вычислений.

Наиболее очевидный вывод заключается в необходимости улучшения доверительного взаимодействия. Подход анализ безопасности и анализа риска поможет провайдерам обеспечивать своих клиентов сервисами, удовлетворяющими критериям безопасности данных. Кроме того, этот подход может быть использован пользователями облачных сервисов для выполнения оценки риска, прежде чем переложить критически важные данные в облака из классической инфраструктуры.

В настоящее время существует недостаток структурированных подходов анализа, который может быть использован для анализа рисков в средах облачных технологий. Данный подход легко адаптируется для автоматизации процесса анализа рисков.

Список литературы

1. Diego, G.: Can we trust Trust? Oxford: Trust Making and Breaking Cooperative Relations (1990).
2. Overview of Security Processes (2011).
3. http://appengine.google.com.
4. http://www.mesh.com.
5. Brodkin, J.: Seven Cloud Computing Security Risks (2008), http://www.gartner.com/DisplayDocument?id=685308.
6. Царегородцев А.В., Савельев И.А., Романовский С.В. Обеспечение безопасности данных в облачных сферах. - Экономика. Налоги. Право. – М., 2013 - №4/2013. С.68-74.