ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ: СОВРЕМЕННЫЕ МОДЕЛИ ПРЕДОСТАВЛЕНИЯ УСЛУГ И ВОЗМОЖНЫЕ РИСКИ

Саклаков В. М.
Научный руководитель – к. т. н. Иванов М. А.
кафедра ОСУ, Томский политехнический университет
romanov_ky@mail.ru

С развитием глобальной сети и ростом количества данных, которые необходимо хранить, обрабатывать и передавать возникла необходимость выполнения уже существующих задач – бизнеса, науки и других – на новом уровне. Основным проблемой стал разрыв возможностей отдельной организации или физического лица самостоятельно содержать и масштабировать информационную и (или) вычислительную инфраструктуру и соответствующих потребностей. По этой причине происходит эволюция традиционной клиент-серверной модели – появляются *облачные вычисления*. По сути они не являются новой технологией, а только методом предоставления необходимых вычислительных ресурсов. Тем не менее они позволили в значительной степени снизить транзакционные, а в некоторых случаях и трансформационные издержки существующих на различном уровне экономических процессов [1]. При этом использование облачных вычислений не лишено недостатков, которые нужно учитывать.

Целью настоящей работы является анализ существующих моделей предоставления услуг с использованием облачных вычислений, а также анализ связанных с этих рисков.

Выделим и опишем модели облачных служб по уровням (см. рисунок 1):

1. **Инфраструктура как сервис** (Infrastructure as a Service – IaaS). На данном уровне находятся непосредственно аппаратный комплекс, основа облака – диски, сетевые устройства, сервера и т. д. Инфраструктура предоставляет пользователю возможность управлять ресурсами хранения и обработки данных, сетями и другими вычислительными ресурсами. Взаимодействие с IaaS не предполагает управления базовой инфраструктурой. Примером инфраструктуры может служить IBM Cloud.

2. **Платформа как сервис** (Platform as a Service – PaaS). Данный уровень является промежуточным, здесь находится инфраструктура приложений. С помощью PaaS можно развернуть в облаке непосредственно их самих, используя поддерживаемые поставщиком инструментальные средства, а также языки программирования. На данном уровне нет возможности управления инфраструктурой, а лишь развернутыми приложениями, а также, в определенных пределах конфигурациями среды хостинга приложений. Примером платформы может служить Amazon Elastic Compute Cloud (EC2).

3. **Программное обеспечение как услуга** (Software as a Service – SaaS). Данный уровень является верхним. Выполняющиеся в нем приложения предоставляются по требованию пользователя. Он может получить доступ к необходимым приложениям посредством различных устройств. Управление физической инфраструктурой облака осуществляется провайдером. Примерами SaaS могут служить почтовый сервис mail.ru, и другие.

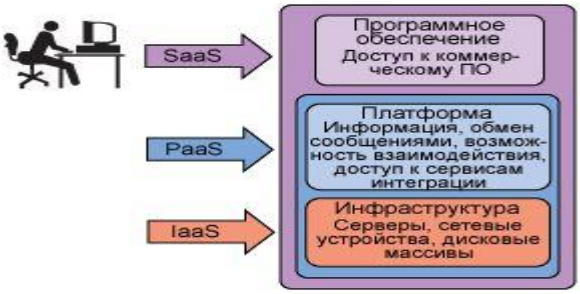

Рисунок 1 - Уровни облачных вычислений [2]

Так же стоит упомянуть следующие сервисы:

- Коммуникации как услуга (Com-aaS);
- Облачное хранилище данных;
- Рабочее место как услуга (WaaS);
- Антивирусное облако;
- Распознавание (когнетивность) как сервис – Cognition-as-a-Service (CaaS) [3].

Рассмотрим последний более подробно. Данный сервис становится популярным в интеллектуальных системах (ИС), архитектура которых включает в себя базу знаний. Для создания ИС не в полной мере подходят ранее описанные технологии облачных вычислений. Причиной является то, что средства создания ИС, зачастую, сами являются таковыми. Следовательно, их использование должно поддерживаться средой. CaaS делает каждое приложение «умным», машинный код становится доступным для пользователя. Они – приложения – смогут взаимодействовать с пользователем как виртуальные ассистенты.

Использование облачных вычислений несет в себе не только преимущества, но и риски. Обеспечение конфиденциальности и безопасности данных является важнейшей задачей поставщика услуг. Убытки или иной ущерб от использования организацией облачных сред оценивается как величина информационного риска в системе облачных вычислений [4]. Рассмотрим подробнее возможные угрозы безопасности и целостности данных в облаке:

1. **Риски, связанные с перемещением традиционных серверов в облачную среду**. Облачные вычисления, помимо имеющихся требований к безопасности, присутствовавших в центрах обработки данных (ЦОД), имеют и свою специфику. Новым типом угрозы стал доступ через глобальную сеть к управлению вычислительными мощностями. Прозрачность внесения изменений в данные и разграничение контроля доступа на уровне системы считается одним из важнейших критериев защиты.

2. **Динамичность виртуальных машин**. Клонирование и миграция между физическими серверами виртуальных машин (ВМ), их остановка или перезапуск осуществляется за короткое время. Данное свойство негативно сказывается на разработку целостной системы безопасности. Последняя не должна зависеть от местоположения или состояния ВМ.

3. **Внутренняя уязвимость виртуальной среды**. Локальные и облачные серверы используют идентичные приложения и операционные системы. Высок риск удаленного взлома или заражения вирусным программным обеспечением. «Атакуемая поверхность» увеличивается за счет использования параллельных ВМ. Задачей системы безопасности является обнаружение вредоносной активности на уровне как ВМ, так и гипервизора.

4. **Обеспечение защиты бездействующих виртуальных машин**. Даже не функционирующая (выключенная) ВМ имеет риск заражения. У вредоносного программного обеспечения есть достаточное количество возможностей получения доступа к хранилищу образов ВМ через сеть. При этом запуск защитных механизмов на выключенной машине невозможен как таковой. Данная угроза снимается путем реализации системы безопасности не только внутри каждой ВМ, но и на уровне гипервизора.

5. **Разграничение сети и защита периметра**. При использовании облачных вычислений происходит размытие периметра сети или вовсе ее исчезновение. Таким образом, общий уровень защищенности сети определяется ее наименее защищенной частью. ВМ должны сами обеспечивать себя защитой в процессе разграничения сегментов с различными уровнями доверия в облачной среде. Благодаря этому сетевой периметр смещается к самой виртуальной машине. При этом стоит помнить, что корпоративный фаерволл не имеет возможностей влияния на серверы, расположенные в облаке.

Некоторые авторы предлагают матрицу оценки уязвимости внешних границ облака по пятибалльной шкале: от низкой, когда внешние угрозы отсутствуют (нет удаленных пользователей), до очень высокой, когда к информационным ресурсам облака имеются каналы для внешнего администрирования [5]. Такая матрица может быть очень полезной при проведении технологического аудита.

Отметим, что при использовании какого-либо облачного сервиса пользователю необходимо убедиться, что поставщик использует технологию, соответствующую международным стандартам, например [6]. Так же необходимо помнить о (а) возможностях пропускной способности канала от пользователя к облаку и обратно; (б) издержках: несмотря на общее снижение расходов от использования облачных вычислений все же необходимо учитывать стоимость обслуживания оборудования, администрирования и другие.

Заключение

Описанные выше меры по обеспечению безопасности облачных вычислений успешно применялись системными интеграторами в процессе создания и функционирования частных облаков. В результате снизилось количество нежелательных инцидентов. Однако сохраняется проблемное поле, связанное с защитой виртуализации. Оно требует принятия проработанного решения на основе системного подхода.

Литература

1. Давыдов Д.С., Кашевник А.М., Косицын Д.П., Шабаев А.И. Шабалина И.М. Разработка платформы планирования производства с использованием технологий «облачных вычислений» // Труды СПИРИАН. №4 (23). 2012. с. 416-430

2. Грейс Уокер. Основы облачных вычислений. Новый способ предоставления вычислительных ресурсов. [Электронный ресурс]: официальный сайт IBM developerWorks. URL: http://www.ibm.com/developerworks/ru/library/cl-cloudintro/index.html (дата обращения 24.10.2015)

3. Кузовлев А. Г. Применение технологии облачных вычислений в интеллектуальных информационных системах // Информатика и прикладная математика: межвузовский сборник научных трудов. №20. 2014. с. 50-52

4. Сенцова А. Ю., Машкина И. В. Анализ информационных рисков в среде облачных вычислений на основе интеллектуальных технологий // Безопасность информационных технологий. №1. 2013. с. 120-121

5. Кораблев А. В. Технология анализа и оценки системы управления информационными рисками облачных вычислений. // Проблемы совершенствования организации производства и управления промышленными предприятием: межвузовский сборник научных трудов. №1. 2014. с. 75-83

6. Information security. Managing Information Security. Risk Organization, Mission, and Information System View [Электронный ресурс]: NIST Special Publication 800-39. 2011. URL: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (дата обращения 24.10.2015)