электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.732.056

Анализ угроз безопасности компонентам технологии облачных вычислений

Маликов А. Ю., студент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра ИУ-10 «Защита информации»

Научный руководитель: Богомолова Н. Е., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
bauman@bmstu.ru

Технология облачных вычислений (cloud computing) - это модель реализации повсеместного доступа по запросу к вычислительным ресурсам с настраиваемой конфигурацией, которые могут быстро предоставляться и высвобождаться с минимальными затратами на управление и эксплуатацию. Это могут быть сети передачи данных, серверы, хранилища данных, приложения и сервисы [1].

Национальный институт стандартов и технологий США (NIST) определяет несколько основных характеристики облачных технологий.

- *Обслуживание по запросу* (*on-demand self-service*), при котором клиент сам решает, в каких вычислительных ресурсах он нуждается: серверное время, скорость выполнения операций доступа и вычислений, размер хранилища данных. При этом потребитель может не взаимодействовать с поставщиком услуги.
- *Общий доступ к ресурсам сети* (*broad network access*), при котором клиент получает доступ к ресурсам облака через сеть используя любое устройство (компьютер, смартфон, планшетный компьютер).
- *Интегрирация ресурсов* (*resource pooling*), когда провайдер объединяет вычислительные ресурсы в общий пул, что позволяет обслуживать большее количество потребителей и динамически перераспределять ресурсы. При этом клиентам необходимо контролировать наиболее общие характеристики услуги (например, объём данных, скорость доступа), но, фактически, предоставляемые ресурсы распределяет провайдер услуги.

- *Эластичность услуг (rapid elasticity)*, при реализации которой объем предоставляемых услуг может быть расширен или сужен, при этом нет необходимости взаимодействовать с поставщиком.
- *Измерение объема услуг (measured service)*, когда провайдер в автоматическом режиме вычисляет количество используемых клиентом ресурсов (объем размещенных данных, число клиентов, количество совершенных операций) и по этим данным определяет объём услуг, предоставленных клиентам.

Технологии облачных вычислений классифицируют по виду модели обслуживания и по виду модели размещения [1]. Выделяют три модели обслуживания.

Предоставления программного обеспечения - SaaS (Software-as-a-Service). В этой модели клиент может пользоваться прикладным программным обеспечением поставщика, которое работает внутри облака и отображается на терминальных устройствах при помощи тонкого клиента из браузера (web-почта) или при помощи интерфейса программы. При этом управление инфраструктурой облака и, частично, клиентским приложением реализуется поставщиком услуг.

Предоставления платформы - PaaS (Platform-as-a-Service). Данная модель позволяет клиенту воспользоваться технологией облачных вычислений для размещения в облаке программного обеспечения, которое позволит загрузить новые или существующие приложения. Такая платформа имеет различные возможности для разработки и тестирования различного рода программных комплексов — систем управления базами данных, промежуточного программного обеспечения, сред разработки.

Предоставления инфраструктуры - IaaS (Infrastructure-as-a-Service). Эта модель делает возможным использовать инфраструктуру облака, чтобы самостоятельно управлять ресурсами облака (обработкой, хранением данных). В частности, клиент может установить и запустить программное обеспечение. При этом клиент контролирует операционные системы, системы хранения данных и приложения, которые были установлены, а также некоторые доступные сервисы (например, связанные с безопасностью). При этом контроль и управление инфраструктурой облака, в частности, серверов, систем управления и мониторинга, запущенных виртуальных машин остается за поставщиком услуг.

Имеется четыре модели размещения технологии облачных вычислений: частное облако, общедоступное облако, гибридное облако и коллективное облако.

Частное облако (private cloud) - облако, используемое одним учреждением, включающим несколько отделов организации, или клиентами этой фирмы. Такое облако может эксплуатироваться, как самим учреждением, так и третьей стороной, а центр обработки данных, в котором физически размещается облако может принадлежать как владельцу облака, так и фирме-провайдеру.

Общедоступное (public cloud) — облако, позволяющее любым пользователям осуществлять свободный доступ. Оно может эксплуатироваться правительственными, научными и коммерческими учреждениями (или их сочетаниями). Физически оно размещается в юрисдикции провайдера.

Коллективное облако (community cloud) — модель, реализующая распределение вычислительных ресурсов среди конкретного сообщества клиентов, имеющих схожие цели и задачи. Общественное облако может принадлежать и эксплуатироваться одной или нескольким организациям этого сообщества. При этом физически такое облако может находиться как внутри, так и вне юрисдикции собственника.

Гибридное облако (hybrid cloud) — это сочетание нескольких типов инфраструктур (частные, общедоступные или коллективные), которые являются отдельными объектами, но взаимодействуют друг с другом при помощи технологий передачи данных (например, задействование вычислительных ресурсов общедоступных облаков распределения нагрузки).

Рассмотрим подробнее структуру облака [2]. Оборудование включает в себя оснащение центра обработки данных, а также подсистему хранения, сеть передачи и вычислительную инфраструктуру. На каждом сервере реализуется разделение ресурсов благодаря большому количеству запущенных виртуальных машин (virtual machine). Виртуализация увеличивает производительность и снижает стоимость услуг. Так же она позволяет перемещать виртуальные машины с одного физического сервера на другой с целью выравниванию нагрузки. Виртуализация реализуется при помощи программного компонента, называемого гипервизором, или монитором виртуальных машин (virtual machine monitor), как показано на рисунке 1. Наличие гипервизора позволяет одновременно работать множеству операционных систем (и установленным на них приложений) на одном физическом сервере. Виртуальные машины, работающие под управлением гипервизора, инкапсулируют в себе операционную систему, запущенные в ней приложения и ее конфигурацию. Для динамической виртуализации (перемещение виртуальных машин на другие физические сервера) разрабатываются новые системы управления и мониторинга. При этом управление

необходимо реализовывать на различных уровнях, то есть, управлять необходимо как самим сервером и его конфигурацией так и всей инфраструктурой облака, включая все его подсистемы.

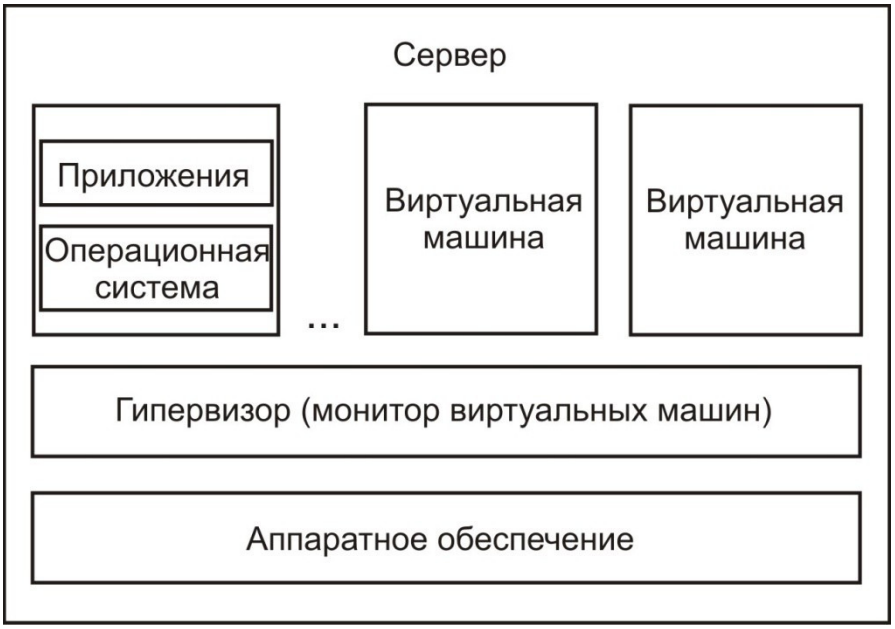

Рис. 1. Сервер виртуализации

Если взять серверы из рисунка 1 и организовать их в единую сеть с общим доступом к системе хранения данных, настроить систему управления, а затем реализовать систему балансировки трафика от клиентов, то мы получим виртуальную инфраструктуру, которая и является облаком.

Одной из важнейших проблема обеспечения безопасности является контроль и управление инфраструктурой облака [3]. Система управления должна отслеживать нарушения в равномерности распределения ресурсов, неконтролируемые виртуальные машины, лишние процессы в системе и изменения конфигурации элементов облака. Учитывая, что все облака имеют разную инфраструктуру, необходимо проектировать систему защиты индивидуально для каждого облака. Облачная архитектура имеет значительно большее число компонентов, чем классическая клиент-серверная, поэтому в ней можно выделить большее количество угроз. Если угрозы операционной системе и запущенным в ней приложениям можно отнести к традиционным (и для них разработаны способы защиты), то угрозы работе виртуальной машины, гипервизора, аппаратных средств и

системе управления облаком являются новыми (см рис. 2) и для некоторых низ них необходимы новые средства защиты.

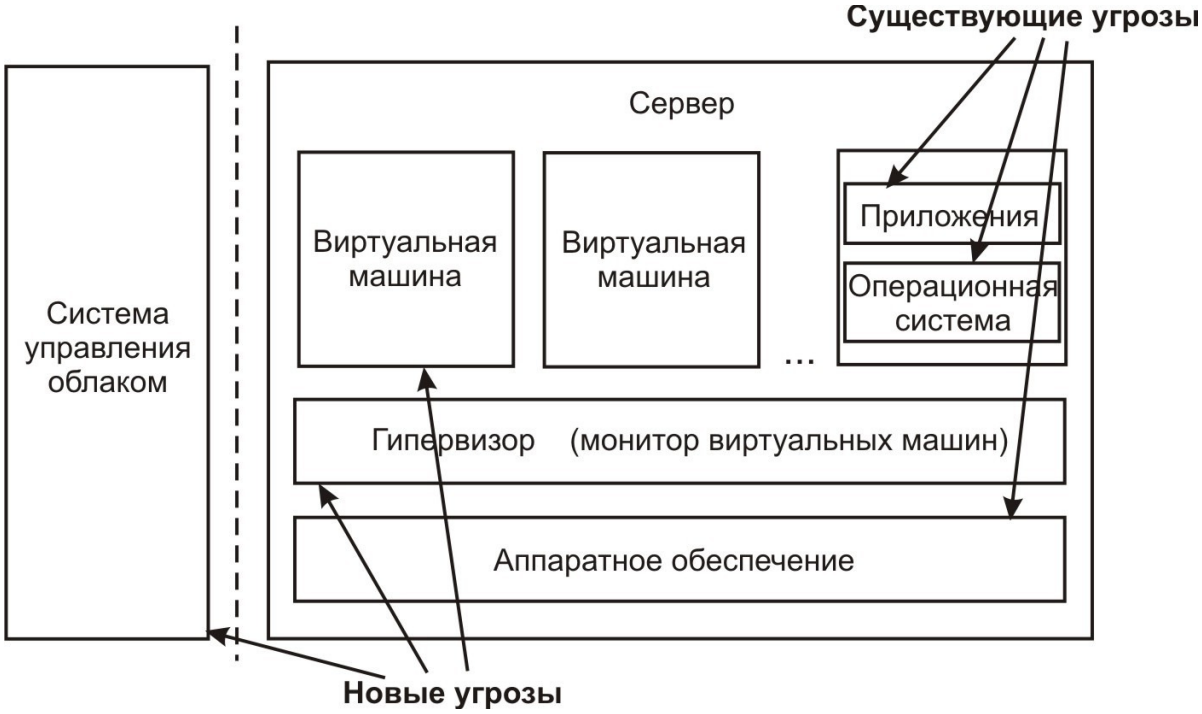

Рис. 2. Существующие и новые угрозы компонентам облака

Предлагается выделить следующие виды атак.

Традиционные атаки на программное обеспечение: использование уязвимостей операционных систем, приложений, сетевых протоколов и др. Для защиты от такого рода угроз необходимо применять межсетевые экраны, антивирусные программы, системы обнаружения вторжений и другие программные и аппаратные средства, обеспечивающие защиту. Однако, необходимо, чтобы данные компоненты защиты могли работать с виртуализацией.

Атаки на потребителя: клиент чаще всего получает доступ к ресурсам облака через браузер. Поэтому становятся возможными такие атаки, как межсайтовый скриптинг (Cross Site Scripting), перехваты паролей и web-сессий, атаки вида man-in-the-middle и многие другие. Для защиты от такого рода атак необходимо использовать аутентификацию и защищенное соединение (SSL) с взаимной аутентификацией. Однако, такие средства защиты, как правило, являются неудобными и дорогими для владельцев облака. В этой сфере информационной безопасности есть еще множество актуальных задач.

Атака виртуальной машины другой виртуальной машиной: обычные межсетевые экраны не применимы для защиты от таких атак, так как трафик между различными виртуальными машинами может находиться внутри сервера виртуализации. Для защиты необходимо использовать специальные виртуальные межсетевые экраны.

Атаки на гипервизор: гипервизор - один из важнейших элементов системы виртуализации. Его основная функция заключается в разделении ресурсов между запущенными виртуальными машинами. Вследствие такой атаки может возникнуть ситуация, когда неконтролируемая виртуальная машина получает доступ к ресурсам и области памяти другой машины. Неконтролируемая виртуальная машина в состоянии перехватывать сетевой трафик, отнимать вычислительные ресурсы и даже вытеснить другие виртуальные машину с физического сервера. Для защиты от таких атак следует применять специальное программное обеспечение, использовать политики периодического изменения паролей, а также использовать встроенный межсетевой экран сервера виртуализации. Также рекомендуется отключать неиспользуемые сервисы (например, web-доступ к серверу).

Атаки на системы управления: систем управления инфраструктурой облака, должны в реальном масштабе времени управлять процессами создания, переноса и удаления виртуальных машин. Вследствие изменения конфигурации системы управления могут появиться виртуальные машины — невидимки, блокирующие работающие виртуальные машины.

В дальнейшем должны быть разработаны конкретные модели угроз для технологии облачных вычислений, учитывающие все вышеперечисленные факторы.

Список литературы

1. NIST SP 500-292. NIST Cloud Computing Standards Roadmap // National Institute of Standards and Technology. 2010. Available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505, accessed 20.08.2014.
2. Джонс Т. Анатомия облака с открытым кодом // IBM: Разумные вычисления. Режим доступа: http://www.ibm.com/developerworks/ru/library/os-cloud-anatomy/ (дата обращния 20.08.2014).
3. Krutz R.L., Vines R.D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis: Wiley Publishing, Inc., 2010. 358 p.