Кияев В.И., Газуль С.М.

«Облачные» вычисления: задачи и реалии информационной безопасности

(СПбГУ, СПбГУЭФ, Санкт-Петербург)

«Облака», «облачные технологии», «облачные вычисления...» За последние несколько лет, эти термины появлялись на слуху все чаще и чаще. Сегодня многие эксперты говорят о новой парадигме предоставления IT-услуг, которая позволит обеспечить колоссальную гибкость IT-сервисов, их круглосуточную работоспособность и поддержку, большую отдачу и эффективность для бизнеса. Не нужно накапливать большие количества быстро устаревающей вычислительной техники – достаточно найти подходящую «облачную» структуру с необходимыми мощностями и задействовать её только на то время, которое необходимо для решения конкретной бизнес-задачи!

По данным Capgemini World Quality Report Survey, в 2010–2011 гг. основными причинами использования «облачных технологий» в компаниях являются: следование тенденциям быстрого развития технологий, сокращение времени выхода продукта на рынок, повышение гибкости производства, сокращение затрат и т.д. (рис. 1).

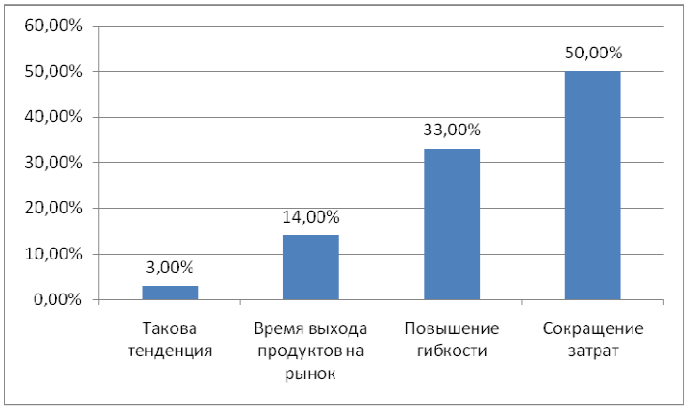

Рис. 1. Распределение по значимости причин использования «облаков»

Действительно, облачные вычисления представляют очень интересные перспективы для бизнеса и позволяют компаниям экономить на IT-затратах: можно платить лишь за те сервисы, которыми компания пользуется, причем именно в том количестве, в котором она нуждается. При этом если компании в какой-то момент потребуется гораздо больший объем вычислительных или коммуникационных услуг, то проблема разрешается простым увеличением

оплаты их стоимости, например, за месяц. Это свойство и называется «гибкостью» облачных решений. Именно оно делает облака привлекательными для многих компаний. Чтобы это понять, достаточно представить какие капитальные расходы ждут компанию, если при небольшой штатной инфраструктуре ей срочно понадобится большее количество мощностей для реализации каких-либо новых проектов, реинжиниринга бизнес-процессов или освоения новой сферы деятельности.

Всё это делает облачные вычисления очень привлекательной парадигмой оказания IT-услуг и предполагает их широкое применение. Отметим, однако, что в настоящее время внимание активных пользователей облачных технологий всё больше и больше фокусируются на вопросах информационной безопасности.

Попробуем сформулировать эти вопросы. Насколько уникальна задача обеспечения информационной безопасности (ИБ) «облачных» вычислений? Глобальная ИТ-индустрия активно рекламирует «облака» как экономически выгодное решение. Однако каковы риски, связанные с переходом к этой модели предоставления услуг, и какие элементы инфраструктуры нуждаются в особой, дополнительной защите, вызванной спецификой «облачных» вычислений? Основной вопрос, который сейчас волнует очень многих, звучит так: «Насколько надёжно хранить свои данные, в том числи и конфиденциальные, в облаке?» (http://www.computerra.ru/vision/485315/).

Рассмотрим историческое развитие IT и колебания уровня информационной безопасности (рис. 2). Каждый раз, с появлением новых технологий, до формирования решений по их защите, уровень информационной безопасности серьёзно падал. По нашему мнению, в настоящее время произойдет очередное колебание, связанное с тем, что стандартных решений по защите информации в облаке и стандартов в области информационной безопасности для облачных технологий пока в достаточной степени не существует!

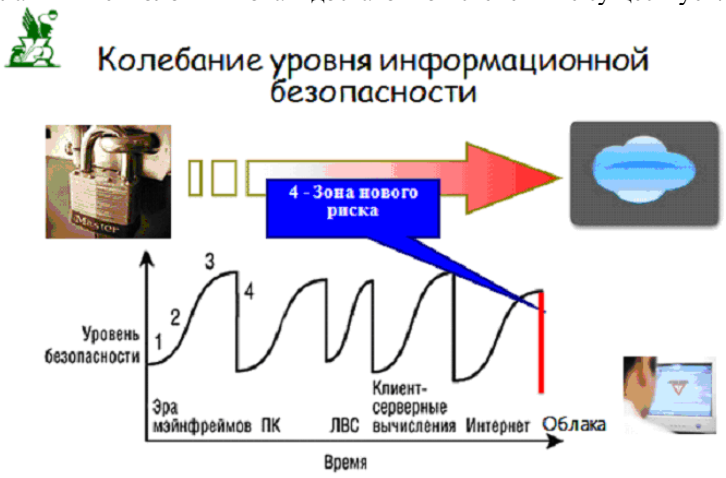

Рис. 2. Развитие вычислительных технологий и колебание уровней риска

По замыслу, облачные вычисления тем и хороши, что данные хранятся на внешнем по отношению к пользователю носителе (на облачных серверах) в распределённом виде и периодически архивируются. Однако никто не застрахован от сбоев. Подобные прецеденты уже были, например, с ресурсом Gmail. Тогда удалось восстановить информацию большинства аккаунтов, но часть данных всё-таки пропала навсегда. Одно дело – частная переписка, совсем другое – бизнес-информация. В первом случае можно немножко подосадовать и забыть, а вот второй может грозить, как минимум, вынужденным простоем, потерей критически важных данных, репутации и, как следствие, прибыли. Неслучайно многие бизнес-пользователи предпочитают хранить всю важную информацию на дополнительных (собственных) серверах с настроенной системой бэкапов. В конце концов, даже если произойдёт сбой «своих» устройств и накопители повредятся, то их всегда можно попробовать восстановить. А если такое произойдёт где-то в облаке, то всё будет зависеть уже от возможностей cloud-провайдера. Особенно «приятно» видеть в лицензии EULA практически всех провайдеров пресловутый «отказ от ответственности» за сохранность обрабатываемых данных! Выходом пока может стать только поддержание актуальной копии всех данных вне «облака», но это, как было отмечено выше, приводит к значительным дополнительным расходам.

Мы указали лишь на один аспект информационной безопасности, а именно − безопасное хранение данных. Есть и другая серьезная проблема. Например, мы регулярно проводим backup базы данных, все данные надежно сохранены, но во время работы с «облачной» базой, происходит хакерская атака, «перехват» данных и, таким образом, конфиденциальные сведения могут стать доступными злоумышленникам.

Некоторые «продвинутые» участники индустрии ИБ уже выводят на рынок решения по реализации «облачной» безопасности. Попробуем разобраться, какие именно участки «облачных» информационных систем нуждаются, по мнению поставщиков, в специфических средствах обеспечения безопасности.

Обзор соответствующих новостей по информационной безопасности, что при организации «облачных» информационных систем в 80% используются вполне традиционные средства − серверы, сети, СУБД и средства виртуализации [3–9]. Таким образом, решение вопросов безопасности в «облаках», как минимум, не приходится начинать с нуля. Многие решения уже созданы и оказываются вполне пригодными. Другое дело, что средств виртуализации, сумевших получить признание специалистов и обладающих промышленным уровнем надежности, сегодня не так уж и много.

Согласимся с авторами статей, что для формирования защиты «облаков» на начальном этапе не нужно изобретать велосипед. Решение задач обеспечения ИБ включает в себя традиционные и широко известные решения, хотя и содержит ряд специфических моментов, которые в процессе выполнения традиционных задач должны быть оптимизированы для экономии производительности виртуальной среды любого рода с обеспечением её безопасности. Причем делать это нужно, не уменьшая общей производительности программных приложений.

По сути, вопрос заключается в том, какую долю вычислительных ресурсов следует резервировать для обеспечения работы защитных систем. И не приведет ли достижение максимально возможного уровня безопасности к чрезмерной нагрузке, препятствующей эффективной работе бизнес-приложений, ради которых, собственно, и затеваются «облачные» проекты?

Компании, активно продвигающие на рынке разработки для защиты сетей, серверов и виртуальных сред, полагают: «облачные» коммуникации достаточно эффективно может защитить высокопроизводительный межсетевой экран, дополненный системой защиты от вторжений. Что же касается обеспечения безопасности работы серверов (ресурсы которых всегда должны быть доступны для выполнения клиентских задач), то очевидно: критически важные приложения обязаны при любых системах защиты работать быстро и надежно. В этом случае, следует быть предельно аккуратными с добавочной нагрузкой на серверы, обеспечивающей безопасность.

Подобной «аккуратности» могут, в частности, содействовать «динамические белые списки» приложений. Подобные системы безопасности (например, McAfee Application Control или другие близкие по функционалу решения) просто не дают разрешения на запуск в «облаке» неизвестного (а часто и вредоносного) исполняемого кода. Если же действительно требуется обеспечить работу на «облачных» серверах новых приложений, администратор легко сделает это: современные системы безопасности позволяют гибко настраивать исключения и обновлять серверы согласно действующим ИБ-политикам.

Не менее важным элементом «облачной» безопасности оказывается защита виртуальной среды. Внимание, которое ИТ-специалисты уделяют этой проблеме, вполне объяснимо. Достаточно оценить ресурсы, необходимые для обеспечения работы традиционного антивирусного решения и умножить полученные цифры на все виртуальные рабочие станции или серверы. Понятно, что «линейное» масштабирование оказывается слишком дорогим выходом из положения. В таком случае антивирус сам превращается в своеобразный «вирус», поглощающий существенные объемы вычислительных ресурсов.

Одним из наиболее популярных ныне решений является перенос нагрузки по сканированию на выделенное ядро антивирусной системы, что позволяет, по разным оценкам, экономить до 30% всей вычислительной мощности, на которую мог бы претендовать «обычный» антивирусный пакет, установленный на каждую виртуальную систему. Экономия практически трети ресурсов − серьезный аргумент! Но из этого следует, что предприятиям, запускающим собственные частные «облака», при проектировании таких систем следует уделять особое внимание принципам организации антивирусной защиты. Разумеется, та же задача актуальна и для поставщиков «облачных» сервисов. Однако в первом случае речь идет о расходах, которые несет сам пользователь.

Технический директор компании Artezio Д. Романовский рекомендует всем участникам «облачных» проектов не забывать о ключевой триаде информационной безопасности: конфиденциальности, доступности и целостности информации. При этом конфиденциальность должна обеспечиваться по всей цепочке, включая поставщика «облачного» решения, потребителя и связывающих их коммуникаций. Задача поставщика облачных услуг − обеспечить как физическую, так и программную неприкосновенность данных от внутренних и внешних посягательств. Не случайно «облачные» дата-центры, как правило, проектируются с опорой на самые современные международные стандарты безопасности (включая вопросы шифрования, а также упомянутые средства антивирусной защиты и защиты от хакерских атак).

В свою очередь потребитель должен ввести в действие «на своей территории» соответствующие политики и процедуры, исключающие передачу прав доступа к информации третьим лицам. В этом смысле объективные преимущества «облаков» не следует смешивать с избавлением заказчика облачных услуг от каких бы то ни было усилий по обеспечению безопасности собственного информационного периметра.

«Облака» не отменяют и необходимости поддержания в адекватном состоянии соответствующей инфраструктуры и программных средств, призванных гарантировать защиту пользовательских рабочих мест, включая обеспечение достоверности и конфиденциальности соединения с «облачным» ресурсом, надежно «прикрытое» от атак третьих лиц. «В целом, − советует Д. Романовский, − должны быть определены минимальные корпоративные стандарты и политики ИБ, соответствие которым будет означать достаточный, объективно определенный уровень безопасности».

Поскольку в «доставке облачных услуг» может участвовать не один, а несколько провайдеров, то, добавим, анализ и согласование политик безопасности следует тщательно производить по всей цепочке «пользователь облачного ресурса – провайдер$_1$ – провайдер$_2$ – ….. – провайдер$_N$ – владелец облачного ресурса».

Доступность «облачных» услуг − новая задача для ИТ-служб в организации информационной безопасности предприятий. Ведь гарантированное предоставление сервиса − результат усилий, предпринимаемых не только поставщиком облачных услуг, но в большой степени и самим предприятием-пользователем.

Отметим, что серьезные сбои в работе оборудования даже у крупных поставщиков «облачных» услуг уже происходят. В мировой практике «облачных» вычислений известны случаи, когда потребитель в течение длительного времени не мог получить доступ к заказанным приложениям. А банальное «отключение Интернета» по вине провайдера или магистрального оператора во время сеансов использования облачных ресурсов может сделать работу с ними невозможной в принципе. Материальные и моральные потери пользователя очевидны!

Таким образом, перед началом проектов, связанных с выносом тех или иных ИТ-сервисов в «облака», заказчикам следует оценить подобные риски,

провести тщательную инвентаризацию приложений (зафиксировав список критически важных для бизнеса), и только затем принимать решения о том, как выстраивать свое «облачное» ИТ-будущее.

Рис. 3. Рекомендации по решению проблем обеспечения информационной безопасности при использовании облачных технологий

И здесь снова многое зависит от пользователя. Мы считаем, что следует в обязательном порядке разрабатывать «плановые пути отхода». Это может быть альтернативный интернет-провайдер, находящийся в «горячем резерве», альтернативный поставщик «облачного» решения, прозрачное управление поддержанием архивных копий данных, страхование, жесткие условия ответственности в соглашениях с поставщиками – всё это обязательные элементы безопасности в «облаках». На рис. 3 показаны рекомендации, которые, с нашей точки зрения, позволят в целом эффективно решать задачи обеспечения информационной безопасности при использовании облачных вычислений.

Многие крупные провайдеры гарантируют сохранность данных, однако, никто не может гарантировать невозможность перехвата данных, потерь информации, в случае природных катаклизмов в тех регионах, где будут находиться региональные дата-центры. Поэтому в области информационной безопасности облачных решений компаниям, находящимся на этом рынке, предстоит большая работа.

Стандарт	Предназначение
ISO 27000	Основные положения и термины
ISO 27001:2005	Требования к системам управления информационной безопасностью
ISO 27002:2007	Практические правила управления информационной безопасностью
ISO 27003	Руководство по внедрению системы управления информационной безопасностью
ISO 27004	Измерение эффективности управления информационной безопасностью
ISO 27005	Руководство по управлению рисками информационной безопасности
ISO 27006:2007	Требования для органов, выполняющих аудит и сертификацию систем управления информационной безопасностью
ISO 27007	Руководство по аудиту систем управления информационной безопасностью
ISO 27031	Руководство по обеспечению непрерывности бизнеса
ISO 27032	Руководство по обеспечению компьютерной безопасности
ISO 27033	Руководство по обеспечению безопасности сетевых технологий
ISO 27034	Руководство по обеспечению безопасности программных приложений

Рис. 4. Совокупность международных стандартов
в сфере информационной безопасности

И последнее, на что мы хотели обратить внимание. В настоящее время существует развитый профиль международных стандартов в сфере информационной безопасности (рис. 4). Однако эти стандарты нацелены, в основном, на формирование системы ИБ внутри компании для защиты внутренних и частично внешних, распределенных ресурсов. Стандартов, сфокусированных на сфере предоставления облачных услуг, пока нет. Отсюда следует, что при активном и постоянном использовании облачных ресурсов особое внимание следует уделить разработке корпоративных стандартов, связанных с безопасностью в «облаках» по всей цепочке предоставления облачной услуги − решения поставщиков на базе этих стандартов станут безопаснее, доступнее и качественнее. Потребителям же нужно будет, как и сегодня, обеспечивать безопасность своей инфраструктуры, чтобы доступ к выбранному «облаку» (который, часто осуществляется через Интернет по протоколу SSL) был безопасным изнутри компании.

Выводы

1. «Облака» формируются из стандартных вычислительных и сетевых блоков, методы защиты которых по отдельности достаточно хорошо отработаны ИТ-индустрией. Однако агрегированные облачные конструкции требуют новых подходов в сфере информационной безопасности.

2. «Облака» − вовсе не «волшебная палочка», избавляющая заказчика облачных услуг от решения вопросов информационной безопасности. Напротив, новый инструментарий требует тщательного аудита свое системы ИБ, трезвой оценки рисков и применения новых средств «облачной защиты».

3. Отраслевые стандарты в сфере обеспечения ИБ в «облаках» только формируются. А значит, к решению вопросов обеспечения целостности данных, а также доступности «облачных» сервисов пока следует подходить индивидуально.

4. Нужно понимать, что никакое «облачное» решение никогда не обеспечит полной гарантии доступности, конфиденциальности и целостности данных и информации. Однако и традиционные решения точно так же уязвимы, поскольку их работа неизбежно связана с проблемами в сфере коммуникаций, риском выхода из строя оборудования и человеческим фактором. Следует четко понимать особенности реализации поддержки бизнес-процессов с помощью «облачных» технологий, оценивая критические риски для каждого конкретного решения. То же самое относится и к попыткам интеграции разных облачных сервисов.

Литература

1. Журнал «Открытые системы» от 06.2010.
2. Электронная энциклопедия Wikipedia [Электронный ресурс]: http://www.wikipedia.org .
3. Безопасность в облаках // Интернет-журнал ibusiness [Электронный ресурс]: http://www.ibusiness.ru/15656 .
4. Проблемы облачных вычислений // Интернет-журнал Computerra [Электронный ресурс]: http://www.computerra.ru/vision/485315/ .
5. Журнал «Хакер».
6. http://technet.microsoft.com/ru-ru/magazine/gg607453.aspx .
7. http://winsecurity.ru/articles/microsoft-azure-security-cloud.html .
8. http://habrahabr.ru/blogs/cloud_computing/112961/ .
9. http://www.ci.ru // Статьи Игоря Козлова.

Нестерук Л.Г., Нестерук Ф.Г.

Об организации распределенных средств интеллектуальной защиты информации

(СПбГУЭФ, Санкт-Петербург)

Актуальность обсуждаемой тематики заключается в том, что перспективные разработки средств защиты информации (СЗИ) должны быть сориентированы на аналогию с механизмами защиты (МЗ) биосистем. При этом МЗ должны соответствовать адаптационным свойствам биологических систем, подтвердивших свою жизнеспособность в течение длительного процесса эволюции [1–5]. Известно, что в зависимости от реализуемых механизмов обеспечения безопасности как реакцию биосистемы на внешние воздействия можно выделить два интеллектуальных уровня: иммунной системы и нервной системы [5–7], аналоги которых целесообразно реализовать в рамках информационно-коммуникационных сетей (ИКС) в условиях высокой динамики угроз, изменения тактики и стратегии проведения компьютерных атак [8].

Анализ текущей обстановки в области моделирования средств иммунной защиты.

Имунная система способна эффективно обрабатывать значительные объемы данных путем высокопараллельных распределенных вычислений [14].