ГУРИЕВ Марат Аликович -
доктор технических наук, профессор,
директор государственных программ IBM
в России и странах СНГ
Адрес: 123317, г. Москва, Пресненская наб., 10
e-mail: marat_guriev@ru.ibm.com

КОССАКОВСКИЙ Владимир Викторович -
руководитель направления по развитию
программного обеспечения мэйнфреймов IBM
в России и странах СНГ
Адрес: 123317, г. Москва, Пресненская наб., 10
e-mail: vladimir_kossakovsky@ru.ibm.com

ОБЛАЧНАЯ ПРОБЛЕМАТИКА В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И СИСТЕМАХ

1. Основная причина развития облачных технологий

Важнейшим направлением повышения продуктивности информационных технологий (далее ИТ) в последние годы является растущий уровень автоматизации процессов комплексных поставок информационных технологий потребителям в рамках разнообразных сервисных процедур.

Происходящий в мире переход к сервисной модели доставки ИТ-функционала к потребителю является прямым следствием изменения роли информационных технологий, которые за последнее десятилетие превратились из рядовой инфраструктурной компоненты современного общества в основной источник роста производительности труда в большинстве отраслей экономики и необходимое условие продуктивной модернизации цивилизации в целом.

При этом суммарная потребительская нагрузка на ИТ быстро растет, и для соответствия требованиям потребителей информационные технологии должны демонстрировать растущую результативность и рекордные темпы собственного усовершенствования.

Облачные технологии, получившие свое название от значка и термина «облако», отражающего сервисную модель с использованием сети Интернет, призваны обеспечить индустриальный - то есть высоко автоматизированный - подход к организации информационно-вычислительных работ и, тем самым, снять остроту проблемы обработки быстро растущих потребительских нагрузок.

2. Описание сложившейся ситуации

Первой практической реализацией современной сервисной модели поставок ИТ можно считать виртуализацию серверов, происшедшую в некотором естественном темпе внутреннего технологического развития ИТ-отрасли и поэтому практически не замеченную национальными элитами за пределами профессиональных ИТ-сообществ.

Виртуализация отличается возможностью оперативного и гибкого перераспределения ИТ-ресурсов между потребителями и очевидной экономией на масштабе, что и определило неизбежность доминирования этого сервиса в корпоративных решениях. Последующее развитие ИТ показало, что логическими следствиями виртуализации являются аутсорсинг ИТ-сервисов и облачные вычисления, которые выступают как потенциальные мультипликаторы эффективности, достигнутой благодаря сервисам виртуализации. 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, которые, по всей видимости, в недалеком будущем будут компенсированы включением дополнительных механизмов мониторинга, контроля и восстановления устойчивости функционирования облачных технологий.

Но перед тем как это произойдет, глобальный и локальные рынки ИТ должны будут преодолеть период неопределенности и нестабильности, порожденный возникшей отчетливой дихотомией между естественным стремлением специалистов по безопасности к абсолютной информационной безопасности и не менее естественным стремлением предпринимателей к максимальной прибыльности ИТ-бизнеса.

Вследствие сложного характера возникшей проблемы дальнейшего эффективного развития ИТ элиты большинства стран вынуждены будут в той или иной мере погрузиться в существо проблемы, поскольку любое из возможных решений потребует корректировки законодательства и обеспечения большей информированности граждан о преимуществах и рисках дальнейшего развития сети Интернет и облачных вычислений.

В ряде стран - лидеров развития ИТ - в настоящее время развернуты работы по формированию научных и методологических основ практического освоения облачных технологий, выпущены соответствующие релизы национальных стратегий информационной безопасности, дополненных в отдельных случаях специальными стратегиями развития облачных технологий, а также основополагающих концепций расчета рисков при дальнейшем развитии ИТ [1,2,3]. К ключевым вопросам, требующим решения, в указанных документах отнесены:

- вопросы формирования и сопровождения глоссариев облачных вычислений на государственном языке, в том числе для целей возможного изменения законодательства;
- вопросы разработки современных стратегий информационной безопасности, ориентированных на реализацию в условиях зарождения будущих технологических переделов информационных технологий;
- вопросы формирования национальных структур, обеспечивающих планирование и мониторинг устойчивости ИТ-развития с комплексированием задач безопасности и ускорения развития новых технологий;
- вопросы организации поддержки инициатив со стороны предпринимательства, академического сообщества и университетов в части разработки стандартов, способствующих эффективному и скоординированному развитию облачных вычислений;
- вопросы выпуска практических рекомендаций и регламентов по организации облачных технологий;
- вопросы разработки программ подготовки и переподготовки кадров пользователей и провайдеров облачных технологий.

Для развития информационных технологий в России до уровня, позволяющего обеспечить модернизацию российской экономики, а также преодолеть отставание в развитии передовых технологических укладов в сфере ИТ[1] представляется необходимым комплексное рассмотрение всего приведенного перечня ключевых вопросов развития облачных технологий.

3. Предложения по мерам поддержки облачных технологий

В связи с набирающими темп работами по формированию в России инфраструктуры информационного общества актуальность использования облачных технологий как важной подосновы этой инфраструктуры становится очевидной. При этом пока не получила развития государственная и общественная регуляторика в этой области. Ниже приводятся предложения по мерам поддержки облачных технологий, которые, как представляется, полностью или частично будут реализованы в ближайшие месяцы:

1. Разработать и утвердить программу развития облачных технологий в Российской Федерации, предусматривающую:

- формирование и систематическое сопровождение русскоязычного глоссария облачных вычислений, в том числе для целей возможного изменения законодательства;
- организацию поддержки инициатив со стороны предпринимательства, академического сообщества и специалистов по стандартизации и техническому регулированию в части разработки стандартов и технических регламентов, способствующих развитию облачных технологий;
- разработку методических рекомендаций и регламентов для органов государственной власти и управления по организации облачных технологий, предусматривающую оперативный переход к практике так называемых корпоративных облачных моделей (Private clouds) и затем тщательно подготовленный с участием специалистов по информационной безопасности переход к общественным и гибридным облачным моделям (Public and Shared clouds);
- разработку программ подготовки и переподготовки кадров пользователей и провайдеров облачных технологий;
- формирование перспективного плана внесения изменений в законодательство, необходимых для ускорения развития облачных технологий.

2. Внести в Правительство Российской Федерации предложения о целесообразности разработки и утверждения программы развития работ по информационной безопасности в условиях развития сервисных моделей доставки информационных технологий, включающей в себя:

- разработку современной стратегии информационной безопасности, нацеленной на ликвидацию отставания в развитии и применении новейших информационных технологий и сервисов;
- усовершенствование существующей организационной структуры и распределения ответственности органов государственной власти и управления в сфере информационной безопасности с целью обеспечения реального содействия ускорению развития и применения новейших информационных технологий и сервисов.

4. Пример реализации подхода к облачным сервисам на основе технологий IBM

Почти полвека назад задача функциональности мейнфрейма была сформулирована как предоставление пользователю необходимых ИТ-ресурсов, практически в режиме on-line, сразу после формирования запроса. Основой для быстрого предоставления вычислительных ресурсов стала виртуализация всей ИТ-среды.

4.1 История виртуализации в IBM [4]

Впервые в промышленной системе виртуализация была реализована IBM в середине 70-х годов прошлого века, была создана операционная система VM/370 (Virtual Machine/370). Идея виртуализации ресурсов мейнфрейма возникла из-за крайне низкой утилизации дорогостоящего оборудования группами разработчиков программного обеспечения - реальное использование компьютер-

[1] *«47. Источниками угроз национальной безопасности могут стать такие факторы, как кризисы мировой и региональных финансово-банковских систем, усиление конкуренции в борьбе за дефицитные сырьевые, энергетические, водные и продовольственные ресурсы,* ***отставание в развитии передовых технологических укладов, повышающие стратегические риски зависимости от факторов изменения внешних».*** *(Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента РФ от 12 мая 2009 г. № 537 // Российская газета. - №4912. - 19 мая 2009.)*

ных мощностей в разы меньше времени написания кода программ. ОС VM/370 обеспечивала каждому пользователю личный мейнфрейм со всеми компонентами - процессором, памятью, дисками, лентами, принтерами, перфораторами. Все эти устройства эмулировались CP (Control Program). CP полностью отделила пользователя от реальных, физических устройств - все привилегированные команды операционной системы (команды управления физическими устройствами, компонентами) перехватывались CP и транслировались на реальные ресурсы. Таким образом, множество пользователей разделяло ограниченное количество ресурсов.

Виртуальная машина полностью эмулировала реальную, гостевые операционные системы устойчиво работали на виртуальной машине.

Подобный принцип виртуализации позже был реализован в построении логических разделов (LPAR) мейнфреймов, затем он был перенесен на другие платформы.

Облачная среда основана на виртуализации всех вычислительных ресурсов.

4.2 Построение облака

Построение облака требует кропотливой подготовки всех возможных для данной среды (корпорации) виртуальных машин. Облачная среда IBM поддерживает виртуальные среды:

- VMware 3.5 / 4.0 (ESX, vCenter, vShpere);
- Xen на IBM System x (семейство серверов IBM, поддерживающих архитектуру Intel);
- KVM переключатель на System x;
- IBM System p PowerVM (программная функция для виртуализации, названная IBM **PowerVM** Active Memory Sharing), которая позволяет оперативной памяти автоматически «перетекать» от одного виртуального сервера (или логического раздела) к другому;
- z/VM на System z.

Администратор должен предусмотреть и дать возможность пользоваться операционными системами, СУБД, языками программирования, компиляторами, приложениями и т.п.

После настройки облака выделение и предоставление ресурсов по запросу пользователя превращается в рутинную процедуру. Продукты IBM Tivoli, управляющие выделением ресурсов, обеспечивают «самообслуживание» пользователя, т.е. он сам формирует запрос на необходимые ресурсы.

4.3 Потенциальные пользователи облака

Виртуализация ресурсов значительно сокращает затраты и повышает утилизацию физического оборудования. Типичными пользователями Cloud могут быть структуры, вынужденные предоставлять вычислительные ресурсы группам пользователей:

- учебные учреждения (выделение студентам или группам вычислительных ресурсов для обучения, выполнения практических, лабораторных и дипломных работ);
- корпорации/предприятия (выделение ресурсов группам пользователей корпоративных приложений);
- государственные учреждения (выделение ресурсов типовым территориальным подразделениям с типизированными одинаковыми функциями);
- предприятия, предоставляющие аутсорсинговые услуги (выделение ресурсов и эксплуатация приложения для сторонних заказчиков: наглядный пример - популярная система 1С).

4.4 Референсная архитектура

Описание референсной архитектуры содержит большое количество технических аббревиатур, однако все они относятся к устоявшейся классике виртуализации и легко открываются в Википедии. Поэтому ссылки на литературу даются только к некоторым из них. Основное назначение приводимой архитектуры - показать, что технологические возможности для построения облака уже сегодня обеспечиваются надежными продуктами, выпускаемыми достаточно давно.

Наиболее универсальной можно считать облачную архитектуру, базирующуюся на современных серверах семейства z и в дополнение на нескольких серверах HP и Sun (Oracle):

- управляющая машина IBM z196 [5] (несколько CPU для поддержки z/OS и множество IFL (Integrated Facility for Linux) для поддержки z/VM и zLinux;
- обязательно использовать zBX (стойки лезвий P и X серверов), управляемые из z196 (поддерживают операционные системы AIX, Linux, Windows);
- HP & SUN (для поддержки HP-UX и Solaris);
- диски, библиотеки, принтеры;
- СУБД - DB2 (все платформы), Oracle (все платформы), MS-SQL, Sybase и другие системы управления базами данных;
- при этом весь комплекс создается и управляется семейством программных продуктов IBM Tivoli [6].

5. Проблемы информационной безопасности в контексте облачных технологий

Несмотря на наличие необходимых наборов решений в части информационно-вычислительной электроники и в части программного обеспечения, реальный прогресс в распространении облачных технологий невелик и ограничивается, как правило, сферой отладки программного обеспечения, а также образовательными и маркетинговыми проектами.

Даже в США, где руководством предприняты решительные меры по переходу к облачным технологиям, выделено целевое финансирование и назначены сроки перехода для большинства министерств и ведомств [3], пока еще только предстоит погрузить в облака такие сравнительно несложные и хорошо защищенные приложения, как ведомственную электронную почту. Критические приложения и различные системы управления в реальном времени пока еще ждут своего часа.

Ключевым препятствием является недостаточное обеспечение информационной безопасности на рассматриваемом этапе очередного усложнения ИТ (потому что при всех очевидных перспективах и преимуществах облачных технологий они, безусловно, являются новым усложнением).

В этом аспекте важно отметить, что в последнем годовом отчете X-Force (специальной команды IBM по информационной безопасности) сообщается, что вследствие широкого распространения технологий виртуализации за период с 2001 года выявлено 316 новых видов уязвимости информационных систем, связанных с виртуализацией. Не приходится сомневаться, что сопоставимый, если не больший, набор уязвимостей ждет нас вследствие развития облачных технологий в начавшемся десятилетии.

Логическим шагом навстречу подступающим проблемам выглядит объявленный международным Альянсом облачной безопасности CSA (Cloud Security Alliance [7]) проект дополнительного базового сервиса в составе облачных технологий, именуемый «Безопасность как сервис» - SecAAS (Security as a service).

Следует отметить, что постепенно растущий опыт практического применения облачных технологий при-

носит свои прагматические рекомендации. Последний пример таких рекомендаций распространен журналом Infoworld в рамках специального отчета Cloud security, Deep Dive series, August 2011 под названием «Новая модель безопасности для новой эры» [8]. Авторы отчета настаивают на коренном пересмотре подхода к информационной безопасности при переходе к облачной среде. Начиная новые требования с обоснования потребности значительного расширения процедур аутентификации, для которых необходимо усовершенствовать систему электронной цифровой подписи, продолжая с требованием понимания новых вызовов, связанных с территориальной неопределенностью места хранения данных в облаках, а также с требованием по-новому посмотреть на уязвимости, связанные с виртуализацией в облаках, авторы завершают анализ предложением новой классификации безопасности для облачных сервисов, приводимой ниже.

КЛАССИФИКАЦИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ С ПОДТЕМАМИ

- ***Инфраструктура безопасности***

Физическая безопасность, контроль окружения, обеспечение непрерывности бизнеса / аварийного восстановления, сетевая инфраструктура, сетевые экраны и прокси-серверы, маршрутизаторы, списки управления доступом, штатное расписание / проверки анкетных данных сотрудников, обеспечение доступа (производительность и противодействие DoS-атакам), политики безопасности (в том числе ресурсы, доступные клиентам), удаленного доступа, мобильный доступ и платформы, идентичность / аутентификации / федерации, биллинговые системы, проблемы виртуализации, высокая доступность.

- ***Ресурсное обеспечение***

Предоставление ресурсов, модификации, собственность и контроль, доступ, отмена доступа, повторное использование / переназначение: пользователей, вычислительных ресурсов, системы ЭВМ или IP-адресов, услуги доменного имени; каталог услуг, управления конфигурацией самообслуживания.

- ***Хранение и безопасность данных***

Безопасность / управление конфиденциальностью, теги данных, зонирование хранения данных, правила хранения данных, поддержание / удаление данных, шифрование (хранимых, передаваемых, управление ключами, Федеральные стандарты обработки информации / Федеральный акт по управлению информационной безопасностью), цифровая подпись / аттестация целостности, вопросы множественной аренды, архивирование, резервное копирование, восстановление данных, классификация данных, локальные требования, профилактика вредоносной агрегации данных.

- ***Безопасность приложений (если применимо)***

Дизайн жизненного цикла безопасности, идентификация / аутентификации / федерация, управление сессиями, верификация ввода данных, обработка ошибок, тестирование уязвимости, установка патчей, проверки подлинности, интеграция данных / обмена, API, прокси-серверы, «песочница» для приложений[2], контроль версий, устранение / поиск ошибок.

- ***Аудит / соответствие (compliance)***

Ведение журнала, мониторинг, аудит, соответствие, аккредитация, правовые вопросы, правила, локальные требования, обнаружение попыток взлома, судебная экспертиза, соглашения об уровне сервисов, планы государственных телекоммуникаций, обнаружение мошенничества.

- ***Общая безопасность***

Средства поиска вредоносных программ, Анти-спам, установка патчей, реагирование на инциденты, предотвращение утечки данных.

Приведенный обширный перечень классифицируемых компонент безопасности облачных сервисов свидетельствует о большом объеме работы, который предстоит выполнить отрасли информационных технологий для практического перехода от действующего «дооблачного» порядка вещей к облачным сервисам. Такой переход можно по объему работ сравнить с переходом в машиностроении от нероботизированного производства к роботизированному, единственное отличие в том, что с дополнительной ролью новых роботов справятся прежние сервера и прежнее программное обеспечение при определенной модификации и настройке.

[2] ***Песо́чница*** *(англ. sandbox) - в компьютерной безопасности механизм для безопасного исполнения программ. Песочница обычно предоставляет собой жестко контролируемый набор ресурсов для исполнения гостевой программы.*

Литература:

1. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

2. http://www.enisa.europa.eu/act/rm/emerging-and-future

3. http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

4. www.cap-lore.com - Norman Hardy's Short history of IBM's virtual machines

5. http://www-03.ibm.com/systems/z/hardware/zenterprise/

6. http://www-01.ibm.com/software/tivoli/products/asset-discovery-zos/index.html

7. http://www.cloudsecurityalliance.org/

8. http://www.infoworld.com/d/cloud-computing/download-the-cloud-security-deep-dive-660?idglg=ifwsite_en.wikipedia.org_General_Deep%20Dive_na_na_na_na_wpl

Юбилей

Журналу «Информационные ресурсы России» исполняется 20 лет. Для профессионального издания такой возраст - это результат востребованности и признания в среде специалистов и экспертного сообщества.

Редколлегии под руководством главного редактора О.В. Кедровского и его заместителя М.В. Изотова удалось создать журнал, который отличается профессиональной подачей материала и компетентностью, постоянно обновляется и в то же время сохраняет традиции.

Поздравляя журнал с юбилеем, мы хотим пожелать творческому коллективу издания всегда сохранять высокий профессиональный уровень, а самому изданию оставаться таким же интересным и информационно насыщенным!