# 8 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

**УДК 004.9**

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

**М.Я. Беккер, Ю.А. Гатчин, Н.С. Кармановский, А.О. Терентьев, Д.Ю. Федоров**

Рассмотрена обобщенная модель облачных вычислений и виды услуг облачных вычислений. Предложена классификация облаков. Показаны основные достоинства и основные риски информационной безопасности при использовании облачных вычислений.

**Ключевые слова:** облачные вычисления, безопасность облачных вычислений, IaaS, PaaS, SaaS, cloud computing, IT security.

### Введение

В общем объеме производимых вычислений неуклонно растет доля той совокупности современных технологий, которая получила броское наименование «облачные вычисления» [1]. Если раньше через Интернет были доступны, по большей части, лишь приложения, ответственные за обмен электронными сообщениями и публикацию web-страниц, то сегодня глобальная сеть все чаще используется для работы со многими другими программными приложениями и базами данных.

Для дальнейшего развития распределенных сетевых приложений и концентрации вычислительных ресурсов все более важной становится проблема обеспечения информационной безопасности. Целью данной работы является анализ проблем обеспечения информационной безопасности при переходе к облачным вычислениям.

### Основные понятия и классификация

Облачные вычисления – относительно новый термин, на сегодняшний день уже прочно вошедший в общепринятую практику как за рубежом, так и в России. Он используется для обозначения совокупности современных технологий, применяемых для распределенной обработки данных, при которой ресурсы вычислительных систем, программное обеспечение и информация предоставляются пользователю по запросу через сеть [2].

Под облаком принято понимать единый с точки зрения клиента виртуальный сетевой узел, реализующий вычислительные службы (один или несколько серверов), который физически может представлять собой географически распределенную совокупность взаимосвязанных аппаратных узлов компьютерной сети. В дальнейшем под поставщиком подразумевается организация, поставляющая услуги облачных вычислений, под потребителем – организация или физическое лицо, приобретающее такие услуги, а под пользователем – физическое лицо (сотрудник, партнер, гипотетический субъект – аппаратный или программный модуль), непосредственно использующее услуги, предоставленные поставщиком потребителю. При этом регулирование организации безопасности облачных вычислений и данных осуществляется на основании договора о предоставлении услуг (SLA – Service Line Agreement), заключаемого между поставщиком и потребителем. В зависимости от вида предоставляемых услуг варьируется и распределение ответственности поставщика и потребителя в вопросах обеспечения безопасности вычислений.

Обобщенная модель системы облачных вычислений представлена на рисунке.

Предполагается, что средства разных уровней приведенной обобщенной модели облачных вычислений (инфраструктуры, платформы, приложений) могут быть предоставлены одним поставщиком потребителю в качестве услуги (as a service), в то время как другие средства потребитель может получать у иного поставщика или контролировать и администрировать самостоятельно.

Рассмотрим три основных вида услуг облачных вычислений [3].

1. IaaS (Infrastructure-as-a-Service) – инфраструктура как сервис.

Поставщик предоставляет потребителю готовую IT-инфраструктуру для развертывания своих приложений. Такая инфраструктура включает в себя, как минимум, средства коммуникации и бесперебойное электропитание. Также могут быть предоставлены средства для исполнения приложений в виде выделенных или виртуальных серверов.

Потребитель получает непосредственный и (или) удаленный доступ для развертывания, настройки и сопровождения требуемых базовых программных продуктов (операционная система, система управления базой данных, система универсальной коммуникации и пр.), специальных программных продуктов (связанных с конкретной проблемной областью, например, система бухгалтер-

ского учета) и индивидуальных программных разработок (как правило, собственных или заказных программных продуктов), а также удаленный доступ для пользователей.

2. PaaS (Platform-as-a-Service) – платформа как сервис.

Поставщик предоставляет потребителю интегрированную платформу для развертывания и выполнения приложений. Также могут быть предоставлены соответствующие средства разработки, отладки, поддержки.

Потребитель получает удаленный доступ для развертывания, настройки и сопровождения требуемых специальных программных продуктов (связанных с конкретной проблемной областью, например, система бухгалтерского учета) и индивидуальных программных разработок (как правило, собственных или заказных программных продуктов), а также удаленный доступ для пользователей.

Базовые программные продукты (операционная система, система управления базой данных и пр.) предоставляются и сопровождаются поставщиком услуг.

3. SaaS (Software-as-a-Service) – программное обеспечение как сервис.

Поставщик предоставляет потребителю готовое для удаленного использования приложение, обеспечивающее решение тех или иных прикладных задач. Потребитель получает удаленный доступ только для пользователей заказанного программного продукта без привилегий администрирования информационной системы.


Рисунок. Обобщенная модель системы облачных вычислений

Перечисленные три модели вычислений касаются непосредственно организации вычислений внутри облака. При этом вовсе не подразумевается, что каждая последующая модель более высокого уровня включает в себя предыдущую, иначе говоря, PaaS <> (Infrastructure + Platfrom) as a Service, SaaS <> (Infrastructure + Platform + Software) as a Service. Однако на рынке наиболее распространены именно такие включающие предложения для конечного потребителя, вплоть до предоставления готовых пользовательских рабочих мест в качестве услуги. В то же время ничто не мешает сочетать перечисленные виды услуг произвольным образом, используя инфраструктуру, платформы и приложения от разных поставщиков услуг.

При каждом из указанных видов услуг поставщик несет ответственность за организацию безопасности вычислений на соответствующих уровнях – инфраструктуры, базовых программных продуктов (платформы), специальных прикладных программ (приложения). В случаях, если поставщик обеспечива-

ет для потребителя услуги всех указанных уровней, ответственность потребителя за организацию безопасности вычислений минимальна.

Вычисления могут быть организованы так, что средства всех перечисленных уровней не приобретаются как услуги, а полностью управляются и контролируются IT-специалистами компании, использующей облачные вычисления. Можно представить, что такая компания является и поставщиком, и потребителем услуг облачных вычислений одновременно. Это позволяет получить некоторые преимущества облачных вычислений, избежав при этом рисков, связанных с приобретением инфраструктуры, платформы или приложений как услуг. Такой подход обычно называют частным облаком, что создает путаницу в терминологии вследствие конфликта с другим, тоже весьма распространенным значением этого термина, о котором будет сказано ниже.

По пользовательской аудитории (области видимости) [2, 4] можно выделить пять классов облаков:

1. Private cloud (for internal users) – частное облако. Пользователями такого облака является ограниченный круг лиц, как правило, сотрудники и контрагенты соответствующей компании-потребителя. Такое облако может быть доступно только внутри локальной сети предприятия и/или посредством VPN-соединений;
2. Community cloud – облако для сообщества. Пользователями такого облака являются участники того или иного сообщества, связанного с потребителем определенными регламентными соглашениями;
3. Public cloud (for external users) – публичное облако. Пользователем такого облака может стать любое лицо, имеющее возможность сетевого доступа к службам облака, при выполнении им определенных условий (наличие электронной почты и т.д.) или без всяких условий (по запросу);
4. Hybrid cloud – гибридное облако. С дальнейшим развитием облачных вычислений перечисленные основные классы облаков и виды услуг образуют более сложные сочетания, которые называют гибридными облаками. Каждое такое облако может сочетать инфраструктуру, платформу и приложения от разных поставщиков услуг, а также предоставлять сервисы, некоторые из которых доступны для ограниченного круга пользователей, некоторые – для сообщества, а некоторые – публично;
5. Intercloud – Интерклауд. В ходе развития облачных вычислений возник новый термин – Интерклауд [4], подразумевающий глобальное «облако облаков» как совокупность групп взаимосвязанных серверов – узлов сети, взаимодействующих посредством «сети сетей» Интернет.

Каждый класс облака предусматривает индивидуальный подход к обеспечению защиты информации, отражающий специфику сетевой топологии и политику авторизации пользователей.

### Стандартизация облачных вычислений

Поскольку технологии облачных вычислений только начинают свой путь к массовому потребителю, одной из основных проблем обеспечения безопасности является отсутствие общепринятых стандартов предоставления облачных услуг. Следовательно, и в вопросах обеспечения безопасности при облачных вычислениях не существует общепринятых стандартов. Проблема стандартизации в обеспечении информационной безопасности находится в процессе решения по трем основным направлениям.

Во-первых, игроки на рынке облачных вычислений создают собственные корпоративные стандарты, которые вовсе не обязательно становятся достоянием общественности. Основное, на что вынужден полагаться потребитель в таком случае, – это имя и репутация компаний, активно продвигающих свои облачные услуги. Среди таких компаний сегодня выступают, например, Microsoft, Google, Adobe, Amazon, IBM, Force.com, VMWare и др. Не исключено, что выработанные поставщиками услуг собственные стандарты будут опубликованы и станут общепринятыми.

Во-вторых, компании-поставщики услуг адаптируют свои предложения согласно уже существующим, устоявшимся стандартам информационной безопасности (сертификация НАТО и GIAC [5], BSI [6], и т.д.), проходят соответствующую сертификацию, получая в результате свидетельство о соответствии предоставляемых информационных услуг определенным регламентирующим документам. Эта работа на сегодняшний день особенно актуальна в аспекте получения заказов от государственных и общественных организаций как долгосрочных потребителей услуг облачных вычислений.

И, в-третьих, различные общественные, правительственные и коммерческие организации предпринимают усилия по выработке регламентирующих требований к созданию безопасных облачных служб обработки информации. Так, Европейское агентство сетевой и информационной безопасности (ENISA), созданное в 2004 г. для совершенствования сетевой и информационной безопасности в Евросоюзе, выпустило документ [7]. Группа компаний, включающая таких крупнейших игроков, как AMD, IBM, CISCO и SUN, подписали так называемый «Манифест открытого облака» (Open Cloud Manifesto), направленный на создание и сохранение как можно большей открытости облачных систем, что, безусловно, в интересах потребителей [8]. Ряд известных компаний сформировали группу «Альянс облачной безопасности». Группа выпустила обширный документ, подробное руководство по безопасности облач-

ных вычислений [9]. Группа специалистов на форуме Jericho Forum консорциума Open Group выработала ряд рекомендаций по безопасному использованию облачных вычислений, предложив подход к выбору архитектуры системы облачных вычислений для безопасной работы [10].

Известные специалисты по информационной безопасности уже представляют общественности свои наработки в области облачных вычислений. Так, например, в одном из самых уважаемых издательств академической литературы John Wiley & Sons вышла заслуживающая серьезного внимания работа [11]. Издательство уже выпустило и планирует выпустить ряд изданий, посвященных использованию и безопасности облачных вычислений.

### Специфика обеспечения информационной безопасности при облачных вычислениях

Рассмотрим основные достоинства облачных вычислений с точки зрения обеспечения информационной безопасности.

– Снижение затрат.

  При росте масштабов вычислительных систем любые меры по обеспечению безопасности обходятся дешевле в расчете на одного пользователя. Концентрация ресурсов позволяет снизить как начальные, так и текущие расходы на защиту информации (например, на приобретение аппаратных средств защиты, использование усиленной аутентификации, резервное копирование, привлечение специалистов по информационной безопасности, на разработку и сопровождение концепции защиты информации, дизайн и стабилизацию производственных процессов и пр.).

– Оптимизация структуры инвестиций.

  Облачные вычисления позволяют оптимизировать два ключевых показателя экономической эффективности информационной инфраструктуры. Возврат инвестиций в инфраструктуру (return of investments, ROI) легко планируется и начинается с момента использования облачных служб. Начальные инвестиции снижаются, потребители платят только за действительно необходимые и заказанные используемые ресурсы, службы и функции. Дополнительные и внеплановые инвестиции со стороны потребителя исключены, поскольку, в случае возникновения сбоев служб, ответственность несет поставщик.

  Совокупная стоимость потребления (total cost of ownership, TCO) во многих случаях существенно ниже, чем при организации собственных центров обработки данных. Затраты на содержание, сопровождение, минимизацию рисков, сервисное обслуживание и масштабирование, обслуживающий персонал и сопутствующие расходы (электроэнергия, производственные площади, страхование, противопожарная защита) включены в абонентскую плату.

  Наибольший эффект от оптимизации структуры инвестиций могут получить предприятия малого и среднего бизнеса. Компании, для которых эксплуатация IT-инфраструктуры не связана с основным направлением деятельности, могут избежать вложений в непрофильные активы.

– Повышение защищенности данных и перенос ответственности.

  Предоставление услуг облачных вычислений подразумевает высоконадежное хранение и резервирование данных, функции быстрого восстановления в случае отказа, сертифицированное шифрование данных при хранении и при пересылке между поставщиком и пользователями. При надлежащем обеспечении всех перечисленных условий поставщиком хранение данных в облаке, можно сравнить с арендой банковского сейфа. Ответственность за обеспечение информационной безопасности на соответствующих уровнях переносится с потребителя на поставщика.

При предоставлении системных ресурсов от поставщика потребителю в виде услуги возникает ряд организационных рисков, которые необходимо учитывать при использовании облачных вычислений.

Рассмотрим основные виды таких рисков.

– Зависимость от поставщика услуг.

  Отсутствие общепринятых стандартов может поставить потребителя в зависимость от поставщика услуг. Необходимым условием минимизации этого риска является разработка, верификация и сопровождение концепции миграции данных и приложений к альтернативному поставщику.

– Невозможность соблюдения вновь возникающих требований.

  Развитие бизнеса потребителя услуг может породить новые требования к системе вычислений, которые не могут быть соблюдены при работе с имеющимся поставщиком. Для минимизации этого риска потребителю необходимо заблаговременно разработать и внедрить производственные процессы отслеживания, оценки и планирования реализации новых свойств и функций вычислительных процессов (release management).

– Ограничение контроля над используемыми службами.

  Используя услуги облачных вычислений, потребитель обладает не только ограниченной ответственностью за информационную безопасность, но и ограниченным контролем над эксплуати-

руемыми службами. Степень ограничений определяется выбранной моделью облачной инфраструктуры и положениями договора (SLA) между поставщиками и потребителем.

Концентрация и совместное использование вычислительных ресурсов также порождает ряд технических рисков, специфичных для облачных вычислений.

Рассмотрим эти риски.

– Нарушение изоляции данных.

  Облачные вычисления в силу коллективного использования системных ресурсов требуют надежной изоляции пользовательских данных друг от друга. Потребителю следует обратить внимание на то, на каких уровнях обобщенной модели обработки данных имеет место участие других пользователей в вычислительном процессе – на уровне инфраструктуры (например, виртуальные серверы, совместно используемые аппаратные ресурсы и пр.), на уровне платформы (например, используемая система виртуализации и пр.), на уровне приложения (например, системы управления базами данных, web-приложения и службы и пр.).

  Наибольшую опасность в этом плане представляют системы, не поддерживающие разделение мандатов и (или) партиционирование, в которых один аппаратный модуль (например, центральный процессор), фрагмент кода базового программного обеспечения (например, платформы виртуализации) или экземпляр прикладного приложения (процесс) используется несколькими различными пользователями от разных потребителей параллельно.

– Использование уязвимостей системы облачных вычислений.

  Передаваемые и хранимые в системе облачных вычислений данные могут быть скомпрометированы или фальсифицированы в обход правил и процессов обеспечения безопасности в результате эксплуатации возможных уязвимостей на различных уровнях системы облачных вычислений. Информация о таких уязвимостях может оказаться общедоступной до того, как проблема будет решена поставщиком.

  Для минимизации этого риска необходимо использовать шифрование передаваемых и хранимых данных. При этом отдельного внимания заслуживает организация управления ключами шифрования и сертификатами, используемыми для шифрования данных в организации – потребителе услуг облачных вычислений.

– Истощение ресурсов и отказ в обслуживании.

  Превышение уровня запросов к службам над максимальной допустимой нагрузкой, в том числе вследствие DoS-атак (Denial of Service – отказ в обслуживании), может привести к недоступности системы облачных вычислений для пользователей. В этой связи особое внимание следует уделить гарантированным параметрам доступности вычислительных систем и восстановления в случае сбоев, которые предусмотрены договором (SLA) между поставщиком и потребителем.

– Несовместимость разработок.

  К сбоям в системе безопасности могут привести проблемы аппаратной или программной совместимости (например, разработок для конкретной платформы с программным интерфейсом платформы). Для минимизации таких рисков следует обратить внимание на сертификацию аппаратной и программной части вычислительных систем и служб, предоставляемых поставщиком, ознакомиться с организацией поддержки в процессе эксплуатации (сервисное обслуживание, обновление и т.д.), выбрать модель организации инфраструктуры вычислений, предусматривающую минимальные требования к компетентности пользователей.

## Заключение

Использование облачных вычислений влечет за собой не только значительные экономические преимущества, такие как снижение затрат, оптимизация структуры инвестиций, повышение защищенности данных и перенос ответственности за обеспечение безопасности на поставщика услуг, но и значительные риски с точки зрения обеспечения информационной безопасности.

Рассмотренные виды услуг облачных вычислений и основных рисков, возникающих при их использовании, среди которых можно выделить организационные (такие как зависимость от поставщика услуг, невозможность соблюдения новых требований, ограничение контроля над используемыми службами) и технические (такие как нарушение изоляции данных, эксплуатация уязвимостей системы облачных вычислений, истощение ресурсов и отказ в обслуживании, несовместимость используемых разработок), лежат в основе рекомендаций для перехода на облачные технологии.

Фундаментальный и многосторонний анализ рисков для информационной безопасности является неотъемлемой предпосылкой разработки и сопровождения успешных и эффективных мер по защите информации в условиях облачных вычислений.

Несмотря на все достоинства облачных вычислений, на сегодняшний день потребителям необходимо взвешенно подходить к их внедрению, органично сочетать традиционные (локальные) и облачные инфраструктуры в организации вычислительного процесса.

Авторы планируют продолжить обсуждение ключевых вопросов предложенной тематики, обеспечивающей защиту информации, в дальнейших публикациях.

**Литература**


1. XaaS Check 2010 – Status Quo und Trends im Cloud Computing. XaaS Check [Электронный ресурс]. – Режим доступа: http://www.xaas-check.eu/download.php?cat=00_Willkommen&file=2010-XaaS-Check-Report.pdf, свободный. Яз. нем. (дата обращения 04.12.2010).
2. Cloud Computing. Wikipedia, the free encyclopedia [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/Cloud_computing, свободный. Яз. англ. (дата обращения 04.12.2010).
3. Сычев А.В. Теория и практика разработки современных клиентских веб-приложений. Интернет-Университет Информационных Технологий [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/internet/thpdevweba/24/thpdevweba_24.html, свободный. Яз. рус. (дата обращения 04.12.2010).
4. Bernstein David, Ludvigson Erik, Sankar Krishna, Diamond Steve, Morrow Monique. Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability// IEEE Computer Society. – 2009.
5. GIAC Mission Statement. Global Information Assurance Certification [Электронный ресурс]. – Режим доступа: http://www.giac.org/overview/statement.php, свободный. Яз. англ. (дата обращения 04.12.2010).
6. BSI Functions. Federal Office for Information Security [Электронный ресурс]. – Режим доступа: https://www.bsi.bund.de/cln_174/EN/TheBSI/Functions/functions_node.html, свободный. Яз. англ. (дата обращения 04.12.2010).
7. Cloud computing: Benefits, risks and recommendations for information security. The official web site of The European Union [Электронный ресурс]. – Режим доступа: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, свободный. Яз. англ. (дата обращения 05.11.2010).
8. Open Cloud Manifesto. Opencloudmanifesto.org. [Электронный ресурс]. – Режим доступа: http://www.opencloudmanifesto.org/opencloudmanifesto1.htm, свободный. Яз. англ. (дата обращения 04.12.2010).
9. Security Guidance for Areas of Focus in Cloud Computing V.2. 1. Cloud Security Alliance [Электронный ресурс]. – Режим доступа: http://www.cloudsecurityalliance.org/csaguide.pdf, свободный. Яз. англ. (дата обращения 04.12.2010).
10. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration. Open group [Электронный ресурс]. – Режим доступа: http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf, свободный. Яз. англ. (дата обращения 04.12.2010).
11. Ronald L. Krutz, Russell Dean Vines. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. – John Wiley & Sons, Inc., 2010.



***Беккер Михаил Яковлевич*** – Microsoft Deutschland GmbH, ведущий консультант, mbecker@microsoft.com

***Гатчин Юрий Арменакович*** – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, доктор технических наук, профессор, зав. кафедрой, gatchin@mail.ifmo.ru

***Кармановский Николай Сергеевич*** – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, кандидат технических наук, доцент, karmanov50@mail.ru

***Терентьев Андрей Олегович*** – Законодательное собрание Санкт-Петербурга, главный помощник депутата, 9444828@mail.ru

***Федоров Дмитрий Юрьевич*** – Санкт-Петербургский государственный инженерно-экономический университет, ассистент, dmitry.yuryevich.fyodorov@gmail.com