Облачные системы: стратегии развития и безопасность

О.Ю. Пескова

Южный федеральный университет
poy@tgn.sfedu.ru

Аннотация

В статье приведены классификация облачных сервисов, моделей сервиса и моделей развертывания, приведены набор требований к облачным службам и результаты технологических прогнозов по кривой Hype Cycle для облачных вычислений, выделены из них наиболее интересные и критичные с точки зрения обеспечения безопасности облачные технологии. Рассмотрены основные проблемы обеспечения безопасности в облачных сервисах. Предложена классификация проблем информационной безопасности облачных технологий по трем категориям: технологические и организационные проблемы, юридические проблемы, антропогенные проблемы.

1. Требования к облачным сервисам

Облачные сервисы все активнее используются рядовыми (и не очень рядовыми) пользователями для своих личных целей. Например, многие уже не представляют эффективной работы без облачных хранилищ данных (dropbox, google drive, Яндекс диск и многие другие), используя их не только для хранения копий файлов но и для реализации простых, но при этом достаточно эффективных схем совместной работы с документами. Для людей, чья жизнь и работа связаны с обработкой большого объема информации, мощным инструментом стали облачные системы работы с заметками (одним из наиболее функциональных сервисов среди подобных систем можно назвать Evernote). При этом даже для частных лиц вопросы обеспечения безопасности важны и во многом влияют на выбор конкретных поставщиков услуг. В последние годы многие организации тоже задумываются над возможностью перевода (полностью или частично) технологической цепочки обработки информации в облака, и для них вопросы защиты целостности и конфиденциальности данных (а также надежности системы в целом) выходят на первое место.

По ряду опросов, проведенных в западных компаниях, от 35 до 75% организаций используют облачные технологии в том или ином виде, причем до 70% из них используют больше одного облака. По данным прошлогоднего отчета State of the Cloud компании RightScale, 33% опрошенных отметили, что основным предметом беспокойства при принятии решения об использовании облака была безопасность; сейчас этот показатель снизился почти вдвое, до 18% [1].

Тем не менее, до сих пор еще нет четкого и однозначного определения, какие системы относятся к облачным. В 2008 году был опубликован документ IEEE «ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing» [11], в котором дается следующее определение (приведу наиболее распространенный перевод): «Облачная обработка данных — это парадигма, в рамках которой информация постоянно хранится на серверах в интернет и временно кэшируется на клиентской стороне, например, на персональных компьютерах, игровых приставках, ноутбуках, смартфонах и т. д.».

Это определение слишком обобщено, поэтому нуждается в дополнительных уточнениях.

Чаще всего говорят о следующем наборе требований к облачным системам:

1. Сетевой доступ к сервисам обеспечивается с использованием стандартных протоколов – как обычных, так и защищенных (*универсальность доступа*).
2. Объем предоставляемых услуг зависит от потребностей клиента (равно как и от его возможностей – в первую очередь финансовых), при этом объем и перечень предоставленных услуг может быть изменен клиентом самостоятельно, в идеале без специальных обращений к провайдеру услуг (*самообслуживание по требованию и эластичность услуг*).
3. Оборудование, обеспечивающее обработку и хранение данных, не выделяется целиком и полностью под отдельного клиента, а обеспечивает работу пула клиентов, перераспределяя мощности с учетом их текущих потребностей (*объединение ресурсов*).
4. К оборудованию и технологическим процессам обработки данных предъявляются значительно более жесткие требования с точки зрения надежности и отказоустойчивости (*высокий уровень доступности, низкие риски неработоспособности*).

2. Требования к облачным сервисам

Свои рекомендации по организации облачных вычислений предложил National Institute of Standarts and Technology (NIST) [9], [10].

Интернет и современное общество: сборник научных статей XVI Всероссийской объединенной конференции IMS-2013, Санкт-Петербург, 9 - 11 октября 2013 г.

Референтная (эталонная) архитектура облачных вычислений NIST (рис.1, [10]) представляет:

- три модели сервиса (Программное обеспечение как услуга -Software as a Service (SaaS), Платформа как услуга - Platform as a service (PaaS), Инфраструктура как услуга - Infrastructure as a Service (IaaS));
- четыре модели развертывания (частное облако - private cloud, общее облако - community cloud, публичное облако - public cloud, гибридное облако - hybrid cloud);
- пять основных характеристик (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service).

В данной архитектуре представлены 3 типа облачных решений:

1. *IaaS (Infrastructure as a service — Инфраструктура как сервис/услуга)*

Пользователь арендует инфраструктуру в целом, а не конкретный набор услуг, т.е виртуальный сервер с адресом или набором адресов и часть системы хранения данных. Управление службой осуществляется через специальный интерфейс (API). Клиент может устанавливать и запускать любое ПО, от операционных систем до прикладных сервисов. Кроме того, клиент может управлять частью сетевых сервисов (например, межсетевым экраном).

2. *PaaS (Platform as a service — Платформа как сервис/услуга)*

PaaS — это модель, при которой пользователю предоставляется установленная, настроенная и готовая к работе виртуальная платформа из одного или нескольких виртуальных серверов с операционными системами и специализированными приложениями. Клиенты могут устанавливать на этой платформе приложения — как собственные, так и сторонней разработки. Часто в состав платформы входят средства разработки и тестирования ПО.

3. *SaaS (Software as a service — Программное обеспечение как сервис/услуга)*

Облачные решения SaaS позволяет удалённо пользоваться программным обеспечением провайдера с использованием различных клиентов. Поставщик разрабатывает приложение или набор приложений и предоставляет доступ к нему за абонентскую плату (абонентская плата может зависеть от набора клиентов и объема данных, проходящих в через сервис провайдера). Все управление приложениями, в том числе обновление, модернизация и техническая поддержка, обеспечивается провайдером.

Иногда к классической модели добавляют варианты, например DaaS (Data as a service — Данные как сервис/услуга, когда обеспечивается предоставление данных по требованию пользователя), Caas (Communication as a service — Коммуникации как сервис/услуга, когда предоставляются услуги связи, чаще всего IP-телефония) и т.д.

Существует несколько вариантов использования облачных систем: публичное облако, приватное облако, общее облако и гибридное облако, которые отличаются прежде всего тем, кому принадлежат используемые технологии и инфраструктура – пользователю или провайдеру [8]:

1. *Публичное облако* — доступ к технологиям имеет любой пользователь через сетевые каналы передачи данных (обычно Интернет), инфраструктура принадлежит организации, которая это облако создала. Именно в этом варианте вопросы обеспечения безопасности практически полностью возлагаются на провайдера.

Рис. 1. Концептуальная диаграмма референтной архитектуры облачных вычислений

2. *Приватные облака* — облака, создаваемые в основном для нужд конкретной организации. Инфраструктура может быть собственностью компании или арендоваться у провайдера, управление может осуществляться как самой организацией, так и провайдером, который обеспечивает ее обслуживание. Этот подход позволяет организации максимально контролировать всю технологию работы с данными и обеспечить максимальную безопасность (естественно, при разработке и соблюдении соответствующей политики безопасности).
3. *Общее облако* — инфраструктура принадлежит нескольким организациям, которые объединились для достижения какой-либо цели. Инфраструктура может управляться самими организациями или выделенным сервис-провайдером.
4. *Гибридное облако* — используется совокупность двух или более облаков с разными моделями внедрения, объединенные общей технологией или стандартом.

3. Прогнозы развития облачных технологий на основе кривой Hype Cycle

Наиболее полные исследования облачных технологий проводит аналитическая компания Gartner — один из ведущих аналитических центров в мире по прогнозированию перспективности информационных технологий. Для представления прогноза развития технологий используется кривая Hype Cycle (рис. 2) [2], [6].

Данное представление предполагает, что каждая новая технология проходит пять стадий:

1. Technology Trigger (запуск технологии) — объявление технологии или другое событие, которое привлекает к ней интерес общественности.
2. Peak of Inflated Expectations (пик завышенных ожиданий) — стадия, на которой на технологию возлагают слишком большие надежды.
3. Trough of Disillusionment (впадина разочарований) — стадия, на которой выясняется, что возлагаемые на технологию надежды не оправдались, а специалистов, которые смогли бы доказать преимущества технологии, еще нет. На этой стадии пресса обычно перестает писать о технологии, вследствие чего создается впечатление, что она ушла со сцены;
4. Slope of Enlightenment (подъем осведомленности) — по мере того, как люди узнают о способах применения технологии, появляются примеры реального внедрения, наступает осознание ее реальной пользы;
5. Plateau of Productivity (плато продуктивности) — на этой стадии технология становится стабильной, общепризнанной и широко применяемой.

Помимо обозначения места на кривой цикла ажиотажа, Gartner дает каждой технологии оценку степени полезности:

- «слабая» — обеспечивает умеренное улучшение процессов, которое не ведет к значительному увеличению доходов или экономии средств предприятия;
- «умеренная» — вызывает постепенные улучшения в установленных процессах, которые способствуют увеличению экономии и дохода предприятия;
- «высокая» — инициирует новые способы выполнения горизонтальных или вертикальных процессов, приводящие к значительному увеличению доходов или экономии средств предприятия;
- «трансформационная» — создает новые способы ведения бизнеса, что может вызывать серьезные изменения в различных отраслях.

Также дается оценка степени зрелости технологии по ряду показателей:

- «эмбриональная» — технология находится на лабораторной стадии, продуктов нет;
- «начальная» — внедрение пилотных проектов, появляются продукты первого поколения, осуществляется реализация пионерами рынка, высокие цены, требуется большая степень кастомизации;
- «подростковая» — технология взрослеет, появляются продукты второго поколения, требуется меньшая кастомизация;
- «начало повсеместного использования» — технология проверена временем, растет количество вендоров, появляются продукты третьего поколения, отрабатываются методики внедрения;
- «повсеместное использование» — определяется несколько явных лидеров, количество вендоров перестает расти;
- «уходящая из использования» — из-за расходов, связанных с переходом на новые технологии, старая технология еще применяется, но в новых проектах уже отсутствует;
- «вышедшая из употребления» — используется редко, в основном на рынке подержанного оборудования.

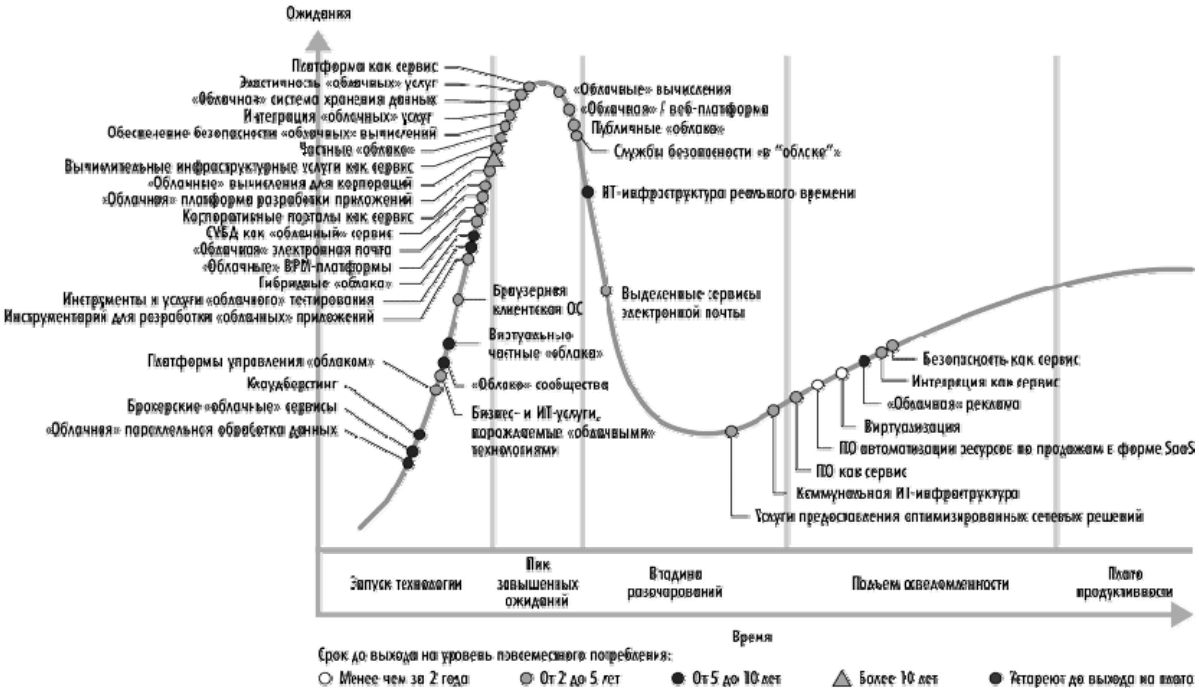

Рис. 2. Цикл ажиотажа Gartner в отношении технологий, связанных с «облачными» вычислениями

Андрей Горелов в своей вполне актуальной (несмотря на возраст) работе [2] рассмотрел широкий спектр облачных технологий, из которых можно выделить ряд наиболее интересных с точки зрения обеспечения безопасности облачные технологии.

На подъеме:

1. Платформы управления облаком — интегрированные продукты, которые обеспечивают управляемость внешнего (публичного) и внутреннего (частного) облака для пользователей.

Gartner отмечает, что хотя спрос на услуги облачных вычислений растет, инструменты для управления приложениями и службами, работающими с этими средами, только появляются.

Степень полезности: высокая.

Проникновение на рынок: менее 1% от целевой аудитории.

Степень зрелости: начальная.

Примеры вендоров: Abiquo, BMC Software, CA Technologies, enStratus, Elastra, HP, IBM Tivoli, Kaavo, Platform Computing, RightScale.

2. Облако сообщества (Community cloud) — это облачная инфраструктура, которая используется совместно несколькими организациями или отдельными лицами, при этом они разделяют общие принципы (например, требования к безопасности, политики, требования к соответствию регламентам и руководящим документам). Такая инфраструктура может управляться самими организациями или третьей стороной и существовать как на стороне клиента, так и на стороне внешнего поставщика услуг. Облако сообщества сочетает в себе достоинства и недостатки публичных и частных облаков и может служить промежуточной стадией между ними.

Степень полезности: трансформационная

Проникновение на рынок: от 1 до 5% от целевой аудитории.

Степень зрелости: начальная.

Примеры вендоров: Terremark Worldwide.

3. Инструментарий для разработки пользовательских приложений используется для создания решений, разворачиваемых на платформе APaaS (Application Platform as a Service — платформа для разворачивания приложений, предоставляемая как сервис), на платформе CEAP (Cloud-Enabled Application Platform — платформа для разворачивания приложений на базе облака) или на базе инфраструктурной облачной системы. Эти приложения могут варьироваться по сложности в зависимости от целевой аудитории и среды исполнения приложения.

Степень полезности: высокая.

Проникновение на рынок: от 1 до 5% от целевой аудитории.

Степень зрелости: «подростковая».

Примеры вендоров: Eclipse Foundation, Google, Microsoft, Qrimp, Rollbase, salesforce.com, Sitemasher, TrackVia.

На пике:

1. Системы управления базами данных (СУБД), применяемые в виде облачных сервисов, — такие СУБД доступны только как облачный сервис и необязательно являются реляционными. Например, Microsoft SQL Azure представляют собой полностью реляционную СУБД, в то время как SimpleDB Amazon и Google BigTable не являются реляционными.

Степень полезности: умеренная.

Проникновение на рынок: менее 1% от целевой аудитории.

Степень зрелости: начальная.

Примеры вендоров: Amazon.com, Google, Microsoft.

2. Частные облака (Private Cloud Computing) — это одна из форм реализации облачных сервисов. В отличие от публичного облака, где доступ к сервису является совершенно открытым, а реализация сервиса полностью скрыта от клиента, в частном облаке доступ к услугам ограничен организацией или некой другой группой лиц, при этом клиент осуществляет контроль над сервисом или сам владеет им и участвует в его реализации.

Существуют внутренние частные облака, в которых клиент имеет контроль над сервисом (или владеет им), а доступ ограничен сотрудниками компании. Есть также вариант Community cloud — облако сообщества — и виртуальные частные облака.

Степень полезности: высокая

Проникновение на рынок: от 1 до 5% от целевой аудитории

Степень зрелости: начальная

Примеры вендоров: Abiquo, Adaptive Computing, BMC, CA, DynamicOps, Elastra, Eucalyptus, HP, IBM, newScale, Novell, Surgient, VMLogix, VMware

3. Облачная веб-платформа — это платформа, которая использует веб-технологии для предоставления программного доступа к некой функциональности, получаемой из веб. Данная функциональность включает доступ к средствам хранения данных и вычислительной мощности, но не ограничивается им. Хотелось бы подкорректировать этот вариант следующим образом:

Степень полезности: трансформационная

Проникновение на рынок: от 5 до 10% от целевой аудитории

Степень зрелости: начало повсеместного использования

Примеры вендоров: Amazon, Google, Microsoft, salesforce.com

4. Проблемы обеспечения информационной безопасности в облачных сервисах.

При перемещении данных и приложений в облака мы фактически уходим от понятия периметра, на котором строится вся защита классических систем: защищаться теперь должен не периметр, не инфраструктура обработки, хранения и передачи данных, принадлежность которой может быть неочевидной, а сама информация. Вопросы безопасности волнуют не только клиента — как провайдер будет обращаться с его данными, но и провайдера — насколько можно доверять клиенту, от каких внешних и внутренних угроз необходимо обеспечить защиту инфраструктуры. При этом основная доля рисков по защите данных ложится именно на провайдера — поставщика услуг.

Можно выделить следующие группы проблем информационной безопасности, возникающих при использовании облачных технологий, которые тормозят их внедрение:

1. Технологические и организационные проблемы:
   - необходимость изменения классических (изученных, отработанных и проверенных) подходов к обеспечению безопасности;
   - практически полное отсутствие соответствующих стандартов по безопасности (особенно в России);
   - отсутствие методик оценки качества, оценки эффективности и оценки защищенности;
   - недоработанные модели угроз и модели нарушителя;
   - сложность оценки рисков;
   - сложности в отслеживании причин нарушения безопасности;
   - небезопасные программные интерфейсы (API);
   - угроза завладения данными провайдером или его сотрудниками (инсайдерство) либо какой-либо третьей силой,
   - отсутствие либо недостаток контроля над серверами и технологическими процессами;
   - сомнения в корректности результатов облачных вычислений;
   - специфические уязвимости, возникающие при использовании средств виртуализации в облаках: возможность несанкционированного взаимодействия между хостами и виртуальными машинами, проблемы с изоляцией хостов и виртуальных машин, различные виды атак, использующих, в частности, уязвимости гипервизоров.
   - специфические требования к идентификации и аутентификации;
   - дополнительные проблемы защиты подключений узлов организации к серверам провайдера-поставщика услуг.
2. Юридические проблемы:
   - отсутствие стандартов и законодательных актов;
   - размытая область ответственности из-за динамически изменяющейся инфраструктуры.
3. Антропогенные проблемы:
   - психологические сложности из-за необходимости передачи данных сторонним компаниям;
   - сложность оценки уровня доверия провайдеров;
   - недоверие и опаска по отношению к новым технологиям, это может привести к неэффективной схеме использования облачных технологий, что увеличит риски,

– боязнь сокращений IT-персонала, что может привести к повышению риска инсайдерства.

Вопросами безопасности облачных систем занимается сразу несколько альянсов, наиболее авторитетным из которых считается Cloud Security Alliance (CSA), основанный в 2008 г. ведущими специалистами информационной безопасности предприятий, участвовавших в ассоциации Information Systems Security Association (ISSA), и ставящий своей целью распространение передового опыта по обеспечению безопасности при работе с облачными сервисами. В частности, этим альянсом был выпущен документ Security Guidance for Critical Areas of Focus in Cloud Computing – руководство по критически важным вопросам безопасного облачных вычислений.

В Европе аналогичные функции выполняет организация Jericho Forum, созданная в 2004 году как площадка для обсуждения проблем защиты данных, возникающих в связи с уходом развитием модели без защищаемого периметра (депериметризации). Jericho Forum работает прежде всего с архитектурой, ориентированной на сотрудничество (Collaboration Oriented Architecture, COA). С появлением облачных вычислений Jericho Forum предложил руководящий документ Securely Collaborating in Clouds, в котором принципы COA распространены и на эту сферу [7].

Концепция облачных вычислений подвергалась активной критике, в частности, со стороны сообщества свободного программного обеспечения, например, со стороны Ричарда Столлмана: «Использовать веб-приложения для своих вычислительных процессов не следует, например, потому, что вы теряете над ними контроль. И это не лучше, чем использовать любую проприетарную программу. Делайте свои вычисления на своём компьютере, используя программы, уважающие вашу свободу. Если вы используете любую проприетарную программу или чужой веб-сервер, вы становитесь беззащитными. Вы становитесь игрушкой в руках того, кто разработал это ПО» [12].

И эти опасения в целом оправданы, хотя инвестиции провайдеров облачных услуг в средства безопасности, как правило, гораздо выше, чем у непрофильных организаций, что в теории может привести к более высокому уровню защищенности. Но здесь мы опять возвращаемся к вопросу оценки уровня доверия к провайдеру. Не случайно говорят о появлении новых видов безопасности: репутационной (reputation) и прогностической (predictive) безопасности.

По словам Максима Эмма [8], директора департамента аудита компании Информзащита, с точки зрения оценки провайдера облачных вычислений в области обеспечения нформационной безопасности этим провайдером и западными компаниями рекомендовано придерживаться определенной методологии: аудит по стандарту SAS 70 Type II (этот стандарт не является специализированным для облачных вычислений, но он стал основным в отсутствие соответствующих регламентирующих актов). Желательны сертификация провайдера по ISO 27001 или следование практикам ISO 27002. К формальным способам оценки безопасности, которые могут применять российские компании, относится аттестация по требованиям ФСТЭК, наличие сертифицированных средств защиты, наличие лицензий ФСТЭК и ФСБ, наличие сертификата EIA/TIA-492 для ЦОД.

Говоря о проблемах безопасности данных, возникающих в связи с применением облачных сервисов, нельзя не упомянуть применение самих облачных сервисов в различных подсистемах обеспечения безопасности данных, так называемая in-the-cloud-безопасность. Наиболее распространенным вариантом подобных схем является использование облаков для целей резервного копирования: как минимум можно использовать облачные хранилища как место хранения резервных копий данных, а кроме того, почти все основные производители ПО резервного копирования предоставляют встроенные сервисы для полноценной работы с резервными копиями в облачной среде. Например, Acronis предоставляет услуги облачных хранилищ резервных копий как для мелких компаний, так и для крупных предприятий [5].

Еще одним примером применения облачных технологий для повышения безопасности информационных систем может служить современное антивирусное ПО. В частности, в состав различных продуктов Лаборатории Касперского включены функции интеграции с облачной сетью безопасности Kaspersky Security Network, которая обеспечивает быструю реакцию на новые угрозы в режиме реального времени [3], [4]. Потенциально опасный файл или веб-сайт проверяется онлайн, а не с помощью сигнатур, которые хранятся локально, на самом компьютере, причем проверка идет в реальном времени и с использованием максимально актуальных баз. Кроме выявления новых угроз, подобная структура позволяет определять и источники заражения. При этом, как утверждают в компании, вероятность ложного срабатывания минимум в 100 раз ниже, нежели при классическом детектировании.

Уже сейчас можно сказать, что спорить о том, работать с облачными технологиями или нет, уже поздно. Облака прочно вошли в нашу жизнь, и сейчас от разработки и исследования систем безопасности облачных технологий во многом будет зависеть будущее как самих сервисов, так и компаний, их использующих.

Литература

[1] Батлер Б. Насколько широко используются облачные технологии? Зависит от того, как спрашивают [Электронный ресурс] // Открытые системы [сайт]. URL: http://www.osp.ru/news/articles/2013/18/13035508/ (дата обращения: 16.08.2013).

[2] Горелов А. Куда идут «облака» [Электронный ресурс] // Компьютер Пресс [сайт]. URL: http://www.compress.ru/article.aspx?id=22659&iid=1040 (дата обращения: 16.08.2013).
[3] Калькуль М. Ясное небо до самого горизонта: «облачные» вычисления и безопасность «из облака» [Электронный ресурс] // Secure List [сайт]. URL: http://www.securelist.com/ru/analysis?pubid=204007652 (дата обращения: 16.08.2013).
[4] Машевский Ю. Антивирусный прогноз погоды: облачно » [Электронный ресурс] // Secure List [сайт]. URL: http://www.securelist.com/ru/analysis/208050657/Antivirusnyy_prognoz_pogody_oblachno (дата обращения: 16.08.2013).
[5] Облачное хранилище Acronis [Электронный ресурс] // Компания Acronis [сайт]. URL: http://www.acronis.ru/solutions/enterprise/cloud.html (дата обращения: 16.08.2013).
[6] Прохоров А. Прогнозы развития информационных технологий [Электронный ресурс] // Компьютер Пресс [сайт]. URL: http://www.compress.ru/Archive/CP/2006/1/3/ (дата обращения: 16.08.2013).
[7] Черняк Л. Безопасность: облако или болото? [Электронный ресурс] // Открытые системы [сайт]. URL: http://www.osp.ru/os/2010/01/13000673/ (дата обращения: 16.08.2013).
[8] Эмм М. Облачные вычисления. Плюсы и минусы с точки зрения безопасности [Электронный ресурс] // Информационная безопасность в СПбГЭУ [сайт]. URL: http://pycode.ru/2011/02/cloud-computing/ (дата обращения: 16.08.2013).
[9] NIST Cloud Computing Program [Электронный ресурс] // National Institute of Standards and Technology [сайт]. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (дата обращения: 16.08.2013).
[10] NIST Референтная (эталонная) архитектура облачных вычислений (Cloud Computing Reference Architecture) Версия 1.0. [Электронный ресурс] // О Cloud Computing на русском [сайт]. URL: http://cloud.sorlik.ru/reference_architecture.html (дата обращения: 16.08.2013).
[11] Hewitt C. ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing // Internet Computing. 2008. September/October. Vol. 12. № 5. P. 96—99. URL: http://www.computer.org/csdl/mags/ic/2008/05/mic2008050096-abs.html (дата обращения: 16.08.2013).
[12] Stallman R. Cloud computing is a trap, warns GNU founder Richard Stallman // The Guardian. 2008/09/29. URL: http://www.guardian.co.uk/technoogy/2008/sep/29/cloud.computing.richard.stallman (дата обращения: 16.08.2013).

Cloud systems: strategy of development and security

Olga Y. Peskova

The paper presents the classification of cloud services, service models and deployment models, The set of requirements to cloud services and results of technological forecasts on curve Hype Cycle for cloud computing are given, the most interesting and critical from the point of view of cloud security technology. The main problems of safety in cloud services are considered. The classification of information security issues of cloud technologies by three categories is offered: technological and organizational problems, legal problems, man-made problems.