# Модель угроз информационной безопасности облачных вычислений

Федоренко Е.А.
*Петрозаводский Государственный Университет*
*katerinafedorenk@mail.ru*

Ивашко Е. Е.
*Институт прикладных математических исследований Карельского научного центра РАН*
*ivashko@krc.karelia.ru*

## Аннотация

Рост скорости обмена информацией, развитие многоядерных процессоров, увеличение емкостей носителей информации, развитие технологии многопоточного программирования определили появление новой технологии в сетевой инфраструктуре – облачных вычислений. Однако для дальнейшего развития распределенных сетевых приложений и концентрации вычислительных ресурсов все более важной становится проблема обеспечения информационной безопасности. Целью данной работы является выявление основных уязвимостей и построение модели угроз информационной безопасности облачных вычислений.

## 1. Введение

Существует достаточно много определений и описаний характеристик облачных вычислений. Согласно [7], облачные вычисления — это модель обеспечения повсеместного и удобного сетевого доступа по требованию к общему набору настраиваемых вычислительных ресурсов, которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и/или обращению к провайдеру.

Поднимая вопрос актуальности облачных вычислений, необходимо упомянуть о статистике роста рынка этих услуг, прогнозах и крупных знаковых внедрениях. Можно с уверенностью сказать, что все современные пользователи Интернет пользуются услугами облачных сервисов, популярными из которых являются предоставление хостинга, электронная почта, социальные сети. Основными преимуществами данной технологии являются эластичность – возможность осуществления масштабирования ресурсов, экономичность и эффективность, надежность, удаленный доступ к данным. На данный момент гигантами в предоставлении облачный услуг являются Amazon EC2 и S3, Microsoft Azure, IBM Smart Cloud, OpenStack и многие другие.

Облачные технологии имеют поддержку на государственном уровне ведущих стран. Перспективность и экономическая эффективность технологий «облачных» вычислений признается и на государственном уровне – ведущие страны мира имеют собственные программы развития «облачных» технологий. Например, в России программа «Информационное общество (2011 - 2020 годы)» предусматривает, в частности, развитие облачных технологий. В США разработан специальный документ «Federal Cloud Computing Strategy», включающий рекомендации по внедрению облачных вычислений на государственном уровне. В Японии разработан проект создания массовой облачной инфраструктуры для госсектора «Облако Касумигасеки».

В настоящее время технология собрала в себя основы многих давно известных технологий - сервис-ориентированной архитектуры, WEB 2.0, виртуализации и, можно сказать, является естественным продолжением аутсорсинга.

Несмотря на свои преимущества, технология имеет серьезные недостатки. Проблема информационной безопасности в облачных вычислениях является одним из сдерживающих факторов для внедрения их в серьезные разработки на государственном и мировом уровне.

Важным вопросом является управление рисками в облачных системах. Пользователь, прежде всего, должен проанализировать все аспекты, в том числе и зону ответственности за безопасность, договора о предоставлении услуг (SLA). Опрос, проведенный ISACA в 2010 году, позволил выявить ряд интересных тенденций. Из общего числа опрошенных ИТ-специалистов 45% полагают, что риски значительно перевешивают

преимущества, и только 10% готовы рассмотреть возможность перевода критически важных приложений в облако [1].

Пользователь услуг чаще всего не знает, где расположены его данные и куда они могут быть перемещены, а так как перенос персональных данных за пределы страны может быть нарушением неприкосновенности частной жизни в некоторых случаях, то это является серьезной проблемой. Также важной проблемой является то, что технология подразумевает под собой совместное использование ресурсов (multi-tenancy) и размещение данных, в том числе и финансовой информации, большого числа пользователей централизованно в одном месте. В этом случае нельзя исключать интерес получения доступа к ним со стороны злоумышленников. Нельзя забывать о том, что провайдеры облачных систем не могут заранее определить своих пользователей. В их число могут входить как благонамеренные лица, так и злоумышленники. Например, исследователи по безопасности обнаружили ботнет Zeus для кражи паролей бот-сетей, работающих на серверах компании Amazon EC2. Хакеры взломали веб-сайт, который размещен на серверах Amazon, а затем тайно установили командование и управление инфраструктурой [10].

## 3. Основные типы «облачных» сервисов

Для выявления потенциальных уязвимостей и построения модели угроз систем облачных вычислений необходимо рассмотреть основные типы и модели обслуживания «облачных» сервисов. Представленная ниже классификация разработана Национальным институтом стандартов и технологий США (NIST) [7].

Наиболее распространенными являются три следующие модели «облачных» сервисов:

1. **Программное обеспечение как услуга** (SaaS, англ. Software-as-a-Service) – модель, в которой потребителю предоставляется возможность использования прикладного программного обеспечения провайдера, работающего в облачной инфраструктуре и доступного из различных клиентских устройств или посредством тонкого клиента, например, из браузера (например, веб-почта) или интерфейс программы.
2. **Платформа как услуга** (PaaS, англ. Platform-as-a-Service) – модель, когда потребителю предоставляется возможность использования облачной инфраструктуры для размещения базового программного обеспечения для последующего размещения на нём новых или существующих приложений.
3. **Инфраструктура как услуга** (IaaS, англ. Infrastructure-as-a-Service) – модель, в которой потребителю предоставляется возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, сетевыми и другими фундаментальными вычислительными ресурсами.

Выделяют четыре следующие модели развертывания «облачных» сервисов по отношению к кругу пользователей:

1. **Частное облако** (англ. private cloud) – инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации.
2. **Публичное облако** (англ. public cloud) – инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации).
3. **Гибридное облако** (англ. hybrid cloud) – это комбинация из двух или более различных облачных инфраструктур (частных, публичных или коммунальных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями переносимости данных и приложений (например, кратковременное использование ресурсов публичных облаков для балансировки нагрузки между облаками).
4. **Общественное облако** (англ. community cloud) – вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики, и соответствия различным требованиям).

## 4. Технологии построения «облачных» систем

Информационная инфраструктура облачных сервисов включает в себя аппаратное обеспечение (центр обработки данных высокой доступности), специализированное программное обеспечение организации облачных сервисов (облачная платформа, системы виртуализации и др.) и

специализированное прикладное программное обеспечение, адаптированное для использования через Интернет в качестве облачного сервиса (например, web-интерфейс электронной почты).

Чтобы лучше понять, как работает облако, для начала необходимо рассказать о виртуализации. Согласно [8], технология подразумевает под собой «изоляцию вычислительных процессов и ресурсов друг от друга». С помощью программных решений можно преобразовать аппаратные ресурсы компьютера, включая ЦП, ОЗУ, жесткий диск и сетевой контроллер, для создания полнофункциональной ВМ (виртуальной машины). В статье [2] дается объяснение работы технологии: «ВМ – программная система, виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и операционные системы. Виртуализация дает возможность переносить виртуальные машины с одного физического сервера на другой с тем, чтобы сбалансировать загрузку. Также нельзя не учесть важного звена в схеме – это схемы управления виртуальными машинами, в которых учитывается динамическая природа виртуализации и новые возможности, предоставляемые виртуализацией. Такая система управления лучше всего реализуется в виде слоев, причем локальное управление осуществляется на сервере, а управление инфраструктурой, осуществляемое на более высоком уровне, предназначено для «дирижирования» всей виртуальной средой».

Упомянутые программные решения могут быть как проприетарными, так и свободными. К первым относятся Microsoft Hyper-V, VMware ESX, Oracle VM, LynxSecure, IBM z/VM. К свободным программным решениям (Open Sourse) относятся KVM, OpenVZ, Xen, VirtualBox, Lguest.

По сути дела, как упоминается в [2], «облачные технологии не являются чем-то радикально новым в сетевой инфраструктуре. Это всего лишь развитие виртуализации, в котором задействовано большое число узлов, совместно использующих память, с балансировкой нагрузки входящих подключений, кэшированием, фильтрацией, и находящихся под управлением».

Продолжая тему, необходимо рассказать об аппаратной и о программной виртуализации. Согласно [8], «Аппаратная виртуализация (hardware-assisted/hardware-based virtualization, HVM, VMX) – семейство технологий, позволяющих предоставлять для программной среды (ОС) полностью эмулируемое (виртуальное) окружение с прозрачным доступом к аппаратному обеспечению». В настоящее время крупные производители процессоров, Intel и AMD уже предлагают модели (Intel VT, AMD-V), обладающие расширенным набором инструкций и позволяющих напрямую использовать ресурсы аппаратуры в виртуальных машинах. Платформы, использующие аппаратную виртуализацию: Hyper-V, IBM LPAR, Xen, VMware, KVM. Как говорится в [9], «классическая архитектура программной виртуализации подразумевает наличие хостовой операционной системы, поверх которой запускается платформа виртуализации, эмулирующая работу аппаратных компонентов и управляющая аппаратными ресурсами в отношении гостевой операционной системы... Безопасность виртуальных машин находится под угрозой, поскольку получение контроля на хостовой операционной системой автоматически означает получение контроля над всеми гостевыми системам».

## 5. Модель угроз

Рассмотрим подробнее уязвимые места «облачных» сервисов в зависимости от видов предоставляемых услуг, схема которых представлена на рис. 1.

### 5.1. Проникновение злоумышленника.

В процессе аутентификации система подвергается риску проникновения злоумышленников. Основные методы проникновения — подбор или хищение паролей, «социальная инженерия», атаки типа «man in the middle» и др. В результате успешного проникновения злоумышленник получает доступ к системе с правами пользователя. При этом объем информации, доступный злоумышленнику незначителен. Однако для проникновения и сбора информации используются специально разрабатываемые программы, способные выполнять автоматически большую или всю часть работы по хищению, анализу и использованию информации. Следует также отметить, что подобные проникновения в «облачные» системы крайне сложно обнаружить.

### 5.2. Взлом приложения, предоставляемого по технологиям SaaS.

В модели SaaS приложение запускается на облачной инфраструктуре и доступно через тонкий клиент (как правило, веб-браузер). В целом, SaaS обеспечивает наиболее интегрированную функциональность, встроенную

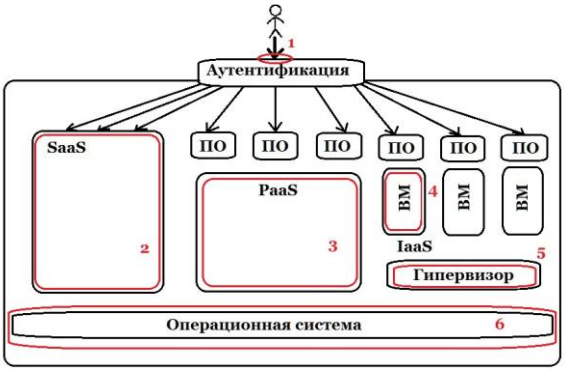

Рис. 1. Модель угроз

непосредственно в предложение, с наименьшей потребительской расширяемостью и относительно высоким уровнем интегрированной безопасности. Клиенту не доступно управление серверами, операционными системами, хранением данных и даже некоторыми возможностями приложений. По этой причине в модели SaaS основная обязанность по обеспечению безопасности практически полностью ложится на поставщиков. При нахождении уязвимости в приложении, злоумышленник потенциально получает доступ к информации всех клиентов сервиса. Это чревато масштабными утечками данных — как персональной, так и финансовой информации. Например, из «Facebook» произошла утечка аутентификационных ключей к профилям пользователей, вследствие чего рекламные фирмы имели доступ к личным данным всех пользователей «Facebook» в течение нескольких лет [11].

### 5.3. Получение доступа к системному ПО PaaS.

В рамках модели PaaS клиентам предоставляется, как правило, достаточно стабильное и прошедшее тщательное тестирование ПО. Как правило, риски выявления критичных с точки зрения информационной безопасности ошибок в таком ПО малы. При этом, такие ошибки оперативно устраняются разработчиками. Однако дополнительные риски несет широкое распространение ПО, предоставляемого в рамках PaaS. Кроме того, такое ПО, как правило, имеет большие права на системе, в рамках которой выполняется. В модели PaaS пользователи должны обращать внимание также на вопросы, связанные с управлением API, такие как подтверждение прав доступа, авторизация и проверка. Например, в марте 2011 года сервис популярной облачной PaaS платформы Heroku был недоступен [12].

### 5.4. Получение доступа к виртуальным машинам.

Системное ПО модели IaaS представляет собой кроме средств автоматизации и управления ресурсами еще и средства виртуализации. IaaS предоставляет большую расширяемость, чем остальные модели. Это, как правило, означает то, что интегрированных функций безопасности мало и вся защита ложится на плечи потребителей.

### 5.5. Получение доступа к гипервизору.

Вмешательство в работу гипервизора может привести к тому, что одна виртуальная машина может получить доступ к памяти и ресурсам другой, перехватывать ее сетевой трафик, отбирать ее физические ресурсы и даже совсем вытеснить виртуальную машину с сервера. Также существует опасность внедрения вредоносного программного обеспечения, которое после получения контроля на хостовой операционной системе виртуализует ее и осуществляет все действия за ее пределами. Пример разработки руткита, позволяющего вынести вредоносный код за пределы пользовательской операционной системы, сделав его принципиально невидимым изнутри нее – Subvirt, созданный в лабораториях Microsoft [3].

Нельзя также исключать атаки с использованием оценок производительности гипервизора. В их число входят атаки с использованием таймеров (базовая оценка производительности с попыткой «поймать» код гипервизора на перехвате), атаки с использованием профилирования ресурсов (попытки определить характер использования RAM и кэшей процессора гипервизором), атаки с использованием синхронизации (использование нескольких потоков исполнения (ядер) для десинхронизации действий гипервизора на них) [4].

Еще один пример руткита, Blue Pill (англ. «Голубая пилюля»), суть которого заключается в захвате запущенного экземпляра операционной системы (захват производится при запуске ОС) «тонким» гипервизором и виртуализацией им остальной части компьютера. Предыдущая операционная система будет все еще поддерживать существующие в ней ссылки на все устройства и файлы, но почти все, включая аппаратные прерывания, запросы данных и даже системное время будут перехватываться

гипервизором, который будет отсылать фальшивые ответы [5].

### 5.6. Получение доступа к ОС облака.

Операционная система «облачного» сервиса является наиболее низким уровнем, подвергающимся опасности. При этом, как правило, методы защиты ОС информационной системы разработаны хорошо и реализуются провайдерами достаточно полно. Однако наибольший риск для операционной системы «облачного» сервиса является не внешний злоумышленник, а внутренний — инсайдер, имеющий доступ к системе в рамках своих должностных обязанностей.

## 6. Заключение

Технологии облачных вычислений стремительно завоевывают популярность. Крупнейшие ИТ-компании мира являются также и ключевыми игроками «облачного» рынка. Пристальное внимание «облачным» технологиям уделяется и со стороны государственных ведомств ведущих стран. Однако при увеличении клиентской базы «облачных» систем, росте объемов информации, передаваемых, обрабатываемых и хранимых с использованием «облачных» сервисов, возрастают и риски, связанные с обеспечением информационной безопасности.

В работе представлено описание комплексной модели угроз «облачного» сервиса, предоставляющего наиболее распространенные услуги — IaaS, PaaS и SaaS. Представлены примеры использования уязвимостей «облачных» сервисов различными вредоносными программами.

Модель угроз является ключевым компонентом при разработке политики, методов и системы обеспечения информационной безопасности.

## 7. Список литературы


[1] Сри Пракаш. *Управление облачными рисками* [Электронный ресурс]. – Режим доступа: http://www.osp.ru/cloud/2011/0311/13008215/, свободный. (дата обращения 21.04.2012).

[2] M. Tim Jones. *Anatomy of an open source cloud* [Электронный ресурс]. – Режим доступа: http://www.ibm.com/developerworks/library/os-cloud-anatomy/index.html, свободный. Яз. англ. (дата обращения 20.04.2012).

[3] Алиса Шевченко. *SubVirt — очередная страшилка* [Электронный ресурс]. – Режим доступа: http://www.securelist.com/ru/blog/181973674/SubVirt_ocherednaya_strashilka, свободный. (дата обращения 21.04.2012).

[4] Никита Абдуллин. *Аппаратная виртуализация и вредоносное ПО* [Электронный ресурс]. – Режим доступа: https://www.defcon-russia.ru/second/nabdullin_virt.pdf, свободный. (дата обращения 21.04.2012).

[5] *Blue Pill (software).* Wikipedia, the free encyclopedia [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/Blue_Pill_(software), свободный. Яз. англ. (дата обращения 22.04.2012).

[6] *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 10.04.2012).

[7] Peter Mell, Timothy Grance. *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology* [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, свободный. Яз. англ. (дата обращения 20.10.2011).

[8] *Виртуализация.* Wikipedia, the free encyclopedia [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Виртуализация, свободный. (дата обращения 22.04.2012).

[9] Александр Самойленко. *Технологии аппаратной виртуализации.*[Электронный ресурс]. – Режим доступа: http://www.vmgu.ru/articles/Tekhnologii-apparatnoi-virtualizatsii, свободный. (дата обращения 21.04.2012).

[10] Dancho Danchev. *Zeus crimeware using Amazon's EC2 as command and control server* [Электронный ресурс]. – Режим доступа: http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110, свободный. Яз. англ. (дата обращения 20.04.2012).

[11] Владислав Новый. *Facebook дал утечку* [Электронный ресурс]. – Режим доступа: http://www.gazeta.ru/business/2011/05/11/3612321.shtml, свободный. (дата обращения 22.04.2012).

[12] *Облачные вычисления, «дырявые» облака и способы защиты данных* [Электронный ресурс]. – Режим доступа: http://www.4by4.ru/ru/analytics/oblachnye-vychisleniya-dyryavye-oblaka-i-sposoby-zashchity-dannyh, свободный. (дата обращения 22.04.2012).