**Лекция 10**

# АНАЛИЗ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

*Статья посвящена анализу современных подходов, обеспечивающих безопасность облачных сервисов. Поскольку облачные вычисления являются одной из наиболее быстро растущих областей среди инфор- мационных технологий, крайне важно обеспечить безопасность и надежность процессов, происходя- щих в облаках и обезопасить взаимодействие между клиентом и поставщиком облачных сервисов. Учи- тывая, что опасения по поводу утери данных и их компрометация являются одной из главных причин того, что некоторые компании не переносят свои вычисления в облака.* ***Объектом*** *исследования и ана- лиза данной работы являются облачные сервисы, которые предоставляться различными провайдерами облачных сервисов.* ***Целью*** *исследования данной работы является сравнение существующих подходов, обеспечивающих информационную безопасность облачных сервисов, а также предложение нового под- хода, основанного на принципе диверсности. Существует множество подходов, обеспечивающих их без- опасность, используя как традиционные, так и специфичные для облачных сред методы. Много-облач- ный подход является одним из наиболее перспективных стратегий повышения надежности за счет ре- зервирования облачных ресурсов на серверах различных провайдеров облачных сервисов. Показано, что необходимо использовать диверсность для обеспечения надежности и безопасности критических ком- понентов систем. Принцип диверсности заключается в использовании уникальной версии каждого ре- сурса благодаря особой комбинации провайдера облачных вычислений, географического расположения центров обработки данных, моделей представления облачных сервисов и моделей развертывания облач- ной инфраструктуры. Подробно говорится о различиях между облачными провайдерами и о том, какие комбинации услуг предпочтительнее других, с точки зрения производительности. Кроме того, рас- сматриваются передовые практики по обеспечению безопасности облачных ресурсов.* ***Как результат****, в данной работе делается заключение о том, что существует проблема недостаточной безопасности и надежности облачных вычислений и того, как можно уменьшить угрозы, чтобы избежать отказа по общей причине и как следствие – потерю конфиденциальных данных или простоя системы, используя диверсность облачных сервисов.*

***Ключевые слова:*** *облачные сервисы; много-облачная стратегия; подход к обеспечению облачной без- опасности; диверсность; облачные провайдеры; модель предоставления облачных сервисов; модель раз- вертывания облачной инфраструктуры; отказ по общей причине; угрозы безопасности облачных вы- числений.*

# Введение

На сегодняшний день облачные вычисления яв- ляются одной из наиболее быстро развивающейся об- ластью среди информационных технологий. Все больше проектов производят миграцию вычисли- тельных ресурсов из своих центров обработки дан- ных в облачные хранилища, доверяя свои данные об- лачным провайдерам. Однако по прежнему остается множество скептиков, полагающих что это является слишком опасным и их данные будут утеряны или они попадут к злоумышленникам. Безусловно ин- формационная безопасность облачных вычислений не является безупречной, при этом стоит заметить, что существует множество способов уменьшить риски. Дискуссия по поводу решения этой проблемы ведётся достаточно давно. Многие облачные провай-

деры принимают ряд мер для существенного повы- шения безопасности, а также дают рекомендации как пользователи их сервисов могут поспособствовать улучшению ситуации со своей стороны. Так как от- ветственность за безопасность лежит не только на провайдере, но и на компаниях, которые пользуются их услугами. При этом человеческий фактор по- прежнему остается главной уязвимостью, так как злонамеренное или случайное пренебрежения поли- тиками безопасности способно свести на нет все меры безопасности.

Одним из наиболее распространённых подходов к обеспечению надежности и сохранности данных пользователей облачных хранилищ является резер- вирования, несмотря на это, уязвимость заложенная в одной версии может распространится на все осталь- ные, так как они являются идентичными копиями.

 В. В. Фролов, 2020

Исходя из выше сказанного создание уникальных ко- пий позволит уменьшить риски потери данных вследствие отказа по общей причине (ОПОП). ОПОП

– это случайный отказ двух или более конструкций, систем или компонентов, вызванный любым скры- тым недостатком при проектировании или изготовле- нии, из-за ошибок в эксплуатации или обслужива- нии, который вызывается любым событием, вызван- ным естественным явлением, эксплуатацией техно- логического процесса установки, или действие, вы- званное человеком или любым внутренним событием в контрольно-измерительной системе [1].

Одним из наиболее эффективных решений про- блемы ОПОП является принцип диверсности, со- гласно которому каждая версия системы должна быть уникальной. Исходя из выше сказанного, веро- ятность возникновения ОПОП сводится к мини- муму [2]. Диверсность является принципом в изме- рительных системах, позволяющим определять раз- личные параметры, использовать разные технологии, использовать разные логические схемы или алго- ритмы или использовать разные средства приведения в действие, чтобы обеспечить несколько способов обнаружения и реагирования на существенно важные события.

Проблемы безопасности облачных вычислений и пути их решения обсуждаются различными иссле- дователями во многих странах мира. В работе

«Security and Security and Privacy Issues in Cloud Com- puting» предложена обобщенная классификация угроз и средств защиты облачных вычислений [3]. Авторы «Cloud Computing Use Case Discussion Group» [4] обсуждают различные сценарии использо- вания облачных вычислений и связанные с ними тре- бования. Они рассматривают варианты использова- ния с разных точек зрения, включая клиентов, разра- ботчиков и инженеров безопасности. В статье «Cloud computing: benefits, risks and recommendations for in- formation security» [5] исследованы различные риски информационной безопасности, связанные с исполь- зованием облачных вычислений, а также затронута тема вероятности рисков, возникших по причине су- ществования уязвимости в облачных вычислениях. Аналогичные вопросы обсуждались в «Cloud Security Alliance (CSA) [6]. В работе «Cloud Security Is- sues» [7] обсуждают спецификации и цели Amazon Compute Service Level Agreement (ACSLA), связан- ные с расположением, разделением и восстановле- нием данных. В следующей работе «Cloud computing security issues and challenges» [8] обсуждаются про- блемы безопасности высокого уровня в модели об- лачных вычислений, такие как целостность данных, безопасность конфиденциальной информации. Также сообщается о различных стандартах управле- ния безопасностью. В статье «On Technical Security

Issues in Cloud Computing» [9] обсуждаются техниче- ские проблемы безопасности, возникающие при ис- пользовании модели облачных вычислений, такие, как XML-атаки, атаки связанные с браузерами, и атаки с использованием переполнения (SYN flood). Авторы статьи «Understanding Cloud-Computing Vul- nerabilities» [10] обсуждают уязвимости в системе безопасности, существующие в облачной платформе. Они сгруппировали возможные уязвимости связан- ные с технологией облачных вычислений, ее харак- теристиками и используемые меры по обеспечению безопасности. Исследование «A survey on security issues in service delivery models of cloud computing»

1. рассматривает проблемы безопасности модели предоставления облачных услуг, уделяя особое вни- мание модели SaaS. Основной идеей «Organizational cloud security and control: a proactive approach» [12] является рассмотрение механизмов контроля без- опасности облачных вычислений с точки зрения их этического использования. В книге «Security, Privacy, and Digital Forensics in the Cloud» [13] подробно раз- бираются многие аспекты безопасности и приватно- сти облаков.

Целью данной статьи является сравнение суще- ствующих подходов, обеспечивающих информаци- онную безопасность облачных сервисов, а также предложение нового подхода, основанного на прин- ципе диверсности. Во-первых, была рассмотрена те- кущая ситуация с безопасностью облачных сервисов и предоставлены некоторые рекомендации по защите облачных вычислений, основанные на практике их использования (Раздел 1). Во-вторых, был освещен и описан такой перспективный подход, как много-об- лачные вычисления, которые могут существенно по- высить надежность облачных сервисов, основанный на использовании нескольких облачных провайдеров одновременно (Раздел 2). Далее предлагается реали- зация принципа диверсности для обеспечения без- опасности критичных, с точки зрения безопасности, облачных ресурсов (Раздел 3). В последнем разделе рассматриваются плюсы и минусы подходов, обеспе- чивающих безопасность облачных сервисов, и пред- ставлены планы на дальнейшие этапы исследования.

# Анализ обеспечения безопасности облачных сервисов

## Введение в облачные сервисы

Облачные вычисления имеют четыре модели предоставления услуг и три основных моделей раз- вертывания. Модели развертывания бывают следую- щих видов [14 – 16]:

* приватное облако, в котором облачная плат- форма предназначена для конкретной организации;
* публичное облако, в котором облачная плат- форма доступна для публичных пользователей, кото- рые могут там регистрироваться и использовать име- ющеюся инфраструктуру;
* гибридное облако – частное облако, которое может распространяться на использование ресурсов в публичных облаках.

Публичные облака являются наиболее уязвимой моделью развертывания, поскольку они доступны для широкого круга пользователей, которые могут размещать там свои службы, используемые зло- умышленниками для кибератак. Модели предостав- ления облачных услуг включают в себя:

* Инфраструктура как сервис (IaaS) – модель, в которой облачные провайдеры предоставляют вы- числительные ресурсы, хранилища данных и сети в качестве интернет сервисов. Эта сервисная модель основана на технологии виртуализации. Amazon EC2, Compute engine от Google cloud, Virtual machine от Microsoft Azure являются наиболее известными сервисами модели IaaS.
* Платформа как сервис (PaaS) – модель, в кото- рой облачные провайдеры предоставляют плат- формы, инструменты и другие бизнес сервисы, кото- рые позволяют пользователям разрабатывать, разво- рачивать и управлять их собственными приложени- ями, при этом не требуется устанавливать эти плат- формы и заниматься поддержкой инструментов на своих компьютерах. Модель PaaS может быть распо- ложена на верхнем уровне модели IaaS или непосред- ственно над облачными инфраструктурами. При этом Google App Engine, Microsoft Azure Web App и AWS Elastic Beanstalk являются наиболее извест- ными представителями модели PaaS.
* Программа как сервис (SaaS) – модель, в кото- рой облачные провайдеры предоставляют приложе- ния, расположенные на облачной инфраструктуре в качестве интернет сервисов для конечных пользова- телей, не требуя от заказчиков сервисов устанавли- вать программное обеспечение на их компьютеры. Эта модель может быть расположена на верхнем уровне модели PaaS, IaaS или непосредственно над облачными инфраструктурами. Стоит отметить, что Atlassian (Jira, Bitbucket, Bamboo), G Suite (Gmail, Google Drive, Docs) и Microsoft Office 365 (Word, Out- look, OneDrive) являются ведущими провайдерами услуг модели SaaS, известные широкому кругу поль- зователей по всему миру.
* Функция как сервис (FaaS) – модель, в которой облачные провайдеры предоставляют возможность запускать программный код практически для любого вида приложений или серверной службы без необхо- димости его администрировать. Затем этот код мо- жет быть выполнен в ответ на событие, которое воз- никло по запросу пользователя, к примеру, нажатие

кнопки мыши или ввод с клавиатуры. Эта модель мо- жет быть расположена на верхнем уровне любого об- лачного сервиса с предыдущих моделей. Известными представителями данной модели являются AWS Lambda, Google Cloud Functions и Microsoft Azure Functions.

Каждая модель предоставления услуг имеет раз- личные возможные реализации, что усложняет разра- ботку стандартной модели безопасности для каждой модели предоставления услуг. Более того, эти мо- дели предоставления услуг могут сосуществовать в одной облачной платформе, что приводит к дальней- шему усложнению процесса управления безопасно- стью.

В модели облачных вычислений участвуют раз- личные заинтересованные стороны: провайдер об- лачных вычислений (объект, который поставляет ин- фраструктуры потребителям облачных вычислений), поставщик сервисов (объект, который использует об- лачную инфраструктуру для доставки приложений или услуг конечным пользователям) и потребитель услуг (субъект, который использует службы, разме- щенные в облачной инфраструктуре), а также третья сторона, которая оказывает поддержку облачному провайдеру, либо поставщику сервисов.

## Угрозы безопасности облачных вычислений

Классифицируем ключевые угрозы безопасно- сти облачных вычислений, которые характерны для конкретных моделей предоставления услуг так и для всех облачных сервисов в целом, результаты пред- ставлены в таблице 1 [1]. При этом важно понимать, что некоторые из этих угроз находятся в ведении об- лачных провайдеров, в то время как за другие несут ответственность поставщики облачных сервисов или их пользователи, следовательно, осознание такого разделения помогает лучше противостоят этим угро- зам.

## Подходы к обеспечению облачных вычислений

В многопользовательской среде, которая исполь- зуется в облачных вычислениях, обеспечение инфор- мационной безопасности является непростой зада- чей. Безопасность должна быть реализована на каж- дом уровне архитектуры облачных приложений. Фи- зическая безопасность, конечно же, обеспечивается провайдером облачных вычислений, что является до- полнительным преимуществом использования об- лака. За безопасность сети и приложений отвечает пользователь. Существует ряд техник, позволяющих снизить риски нарушения безопасности:

Таблица 1

Классификация угроз для облачных вычислений

|  |  |
| --- | --- |
| **Угроза** | **Описание** |
| Угрозы исходящие изнутри (инсайдеры):* злоумышленник находится на стороне облачного провайдера;
* злоумышленник находится на стороне поставщика облачных сервисов;
* злоумышленник является третьей сто- роной, оказывающей поддержку либо провай- деру, либо пользователям.
 | Угроза доступа инсайдеров к данным клиентов, исполь- зующих облачные сервисы, возрастает, поскольку каж- дая из моделей доставки может создавать потребность в нескольких внутренних пользователях:SaaS – администраторы облачного провайдера и по- ставщика его сервисов;PaaS - разработчики приложений и управляющие те- стовым окружением;IaaS – консультанты облачной платформы с третьей стороны. |
| Угрозы исходящие извне:* удаленная программная атака облач- ной инфраструктуры;
* удаленная программная атака облач- ных приложений;
* удаленная аппаратная атака на облако;
* удаленная программная и аппаратная атака на программное и аппаратное обеспече- ние конечных точек организаций пользовате- лей облака;
* социальная инженерия пользователей облачных провайдеров и пользователей облач-

ных сервисов. | Можно предположить, что угроза со стороны внешних злоумышленников в большей степени распространяется на публичные облака, однако все типы моделей предо- ставления облачных сервисов подвержены влиянию внешних злоумышленников, особенно в приватных обла- ках, где могут быть заданы конечные точки пользовате- лей. Облачные провайдеры с большими хранилищами данных, в которых хранятся данные кредитных карт, лич- ная информация и конфиденциальная или интеллекту- альная собственность, будут подвергаться атакам со сто- роны групп со значительными ресурсами, которые пыта- ются получить эти данные. |
| Утечка данных:* отказ безопасных прав доступа в не- скольких доменах;
* отказ электронных и физических транспортных систем для облачных данных и

резервного копирования. | Угроза массовой утечки данных среди многих потенци- ально конкурирующих организаций, использующих од- ного и того же облачного провайдера, может быть вы- звана человеческой ошибкой или неисправным оборудо- ванием, что приведет к компрометации информации. |
| Разделение данных:* неправильно определенны периметры безопасности;
* неправильная настройка виртуальных машин и гипервизоров.
 | Целостность данных в сложных средах облачного хо- стинга, таких как модель SaaS, настроенных для совмест- ного использования вычислительных ресурсов клиен- тами, может создать угрозу для целостности данных. |
| Доступ пользователя:– слабая процедура идентификация и управления доступом. | Внедрение неэффективных процедур контроля доступа создает много уязвимостей. Например, недовольные бывшие сотрудники организаций, поставляющие облач- ные сервисы, поддерживают удаленный доступ для адми- нистрирования облачных сервисов клиентов и могутнанести преднамеренный ущерб их источникам данных. |
| Качество данных:– введение неисправных компонентов приложения или инфраструктуры. | Угроза влияния качества данных возрастает, поскольку облачные провайдеры размещают данные многих клиен- тов. Введение неисправного или неправильно сконфигу- рированного компонента, требуемого другим пользова- телем облака, может потенциально повлиять на целост- ность данных для других пользователей облака, сов-местно использующих инфраструктуру. |
| Управление изменениями:* тестирование на проникновение клиен- тов, которое влияет на других облачных клиен- тов;
* изменения инфраструктуры в системах провайдеров, клиентов и сторонних пользова-

телей облачных сервисов, которые влияют на облачных клиентов. | Поскольку поставщик облачных сервисов несет все боль- шую ответственность за управление изменениями во всех моделях предоставления облачных вычислений, суще- ствует угроза того, что изменения могут привести к нега- тивным последствиям. Это может быть вызвано про- граммными или аппаратными изменениями в существу- ющих облачных сервисах. |

Продолжение табл. 1

|  |  |
| --- | --- |
| **Угроза** | **Описание** |
| Угроза отказа в обслуживании:* распределенная пропускная способ- ность сети с отказом в обслуживании;
* отказ в обслуживании сетевого DNS;
* отказ в предоставлении данных прило- жения.
 | Угроза отказа в обслуживании по отношению к доступ- ным ресурсам облачных вычислений, как правило, явля- ется внешней угрозой для публичных облачных серви- сов. Однако угроза может повлиять на все модели облач- ных сервисов, поскольку внешние и внутренние агентыугроз могут вводить компоненты приложений или обору- дования, которые вызывают отказ в обслуживании. |
| Физическое нарушение:* нарушение IT-услуг облачного провай- дера через физический доступ;
* нарушение облачных IT-сервисов кли- ентов через физический доступ;
* нарушение услуг сторонних провайде- ров WAN.
 | Угроза нарушения работы облачных сервисов, вызванная физическим доступом, различна для крупных поставщи- ков облачных сервисов и их клиентов. Эти поставщики должны иметь опыт в обеспечении безопасности круп- ных центров обработки данных, и должны учитывать устойчивость среди других стратегий доступности. Су- ществует угроза того, что пользовательская инфраструк- тура в облаке может быть физически нарушена как из- нутри, так и извне, где менее безопасные офисные средыили удаленная работа являются стандартной практикой. |
| Использование слабых процедур восстановле- ния:– вызов неадекватных процессов аварий- ного восстановления или процессов непрерыв- ности бизнеса. | Угроза инициирования неадекватных процедур восста- новления и управления инцидентами усиливается, когда пользователи облачных вычислений рассматривают воз- можность восстановления своих собственных систем па- раллельно с системами, управляемыми сторонними по- ставщиками облачных сервисов. Если эти процедуры непроверены, то они могут значительно влиять на время восстановления. |

* Информационно-ориентированная безопас- ность – техника самозащиты данных, которая тре- бует, чтобы интеллект был помещен в сами данные. Данные должны быть самоописуемыми и защи- щаться, независимо от их среды. При обращении к ним, данные обращаются к своей политике и пыта- ются воссоздать безопасную среду, которая прове- рена как надежная с использованием инфраструк- туры доверенных вычислений.
* Высоконадежная аттестация удаленного сер- вера – многообещающий подход к решению про- блемы отсутствия прозрачности, который основан на надежных вычислениях. В доверенной вычислитель- ной среде на облачном сервере устанавливается до- веренный монитор, который может отслеживать или проверять операции облачного сервера. Надежный монитор может предоставить подтверждение соот- ветствия владельцу данных, гарантируя, что опреде- ленные политики доступа не были нарушены. Для обеспечения целостности монитора, доверенные вы- числения также позволяют выполнять безопасную загрузку этого монитора рядом (и надежно изолиро- ваны) от операционной системы и приложений. Мо- нитор может применять политики контроля доступа и выполнять задачи мониторинга или аудита. Для подтверждения соответствия подписывается код мо- нитора и заявление о соответствии, выданное мони- тором. Когда владелец данных получает это подтвер-

ждение соответствия, он может проверить, что вы- полняется правильный код монитора и что облачный сервер выполнил политики контроля доступа.

* Бизнес-аналитика с улучшенной конфиден- циальностью – другой подход для сохранения кон- троля над данными, который заключается в необхо- димости шифрования всех облачных данных. Про- блема в этом подходе заключается в том, что шифро- вание ограничивает использование данных. В част- ности, поиск и индексация данных становится про- блематичным, или даже невозможной задачей. Например, если данные хранятся в виде открытого текста, можно эффективно искать документ, указав ключевое слово. Это невозможно сделать с помощью традиционных рандомизированных схем шифрова- ния, хотя существуют универсальные схемы шифро- вания, которые позволяют выполнять операции и вы- числения на зашифрованных текстах.
* Бастионные хосты – это виртуальные ма- шины, которые находятся в общедоступной подсети

клиента и обычно доступны с использованием SSH или RDP. Как только удаленное соединение установ- лено с хостом-бастионом, оно действует как «скачко- образный» сервер, позволяя клиентам использовать SSH или RDP для входа в другие виртуальные ма- шины (в пределах частных подсетей) глубже в поль- зовательском виртуальном приватном облаке (VPC). При правильной настройке с использованием групп

безопасности и сетевых списков ACL (NACL) ба- стион по сути действует как мост к пользовательским частным виртуальным машинам через Интернет [17]. Однако, главным принципом обеспечения без-

опасности облачных вычислений является следова- ние рекомендаций от облачных провайдеров [18-20]. Рассмотрим основные советы, которые они дают. Прежде всего, потребители облачных услуг должны полностью понимать свои сети и приложения, чтобы определить, как обеспечить функциональность, устойчивость и безопасность для облачных приложе- ний и систем. Надлежащая проверка должна выпол- няться в течение всего жизненного цикла приложе- ний и систем, развертываемых в облаке, включая планирование, разработку и развертывание, опера- ции и вывод из эксплуатации. Важно понимать, что как провайдер облака, так и пользователь несут от- ветственность за безопасность облака. При подписа- нии соглашение с провайдером, должно быть огово- рено, за какие аспекты облачной безопасности отве- чает пользователь и за какие аспекты будет забо- титься провайдер.

Следующий важный момент – это управление доступом. Для управления доступом обычно требу- ется три возможности: способность идентифициро- вать и аутентифицировать пользователей, возмож- ность назначать пользователям права доступа и воз- можность создавать и применять политики контроля доступа к ресурсам. Следует использовать многофак- торную аутентификацию, чтобы уменьшить риск компрометации учетных данных. Похищенные учет- ные данные привилегированного пользователя поз- воляют злоумышленнику контролировать и настраи- вать ресурсы потребителя облака. Использование множества факторов требует от злоумышленника приобретения нескольких независимых элементов аутентификации, что снижает вероятность компро- метации. Следует запланировать набор ролей для вы- полнения общих и индивидуальных обязанностей. Эти роли должны гарантировать, что никто не смо- жет негативно повлиять на весь виртуальный центр обработки данных. Провайдеры предлагают не- сколько различных типов услуг хранения, таких как виртуальные диски, хранилище больших двоичных объектов и службы доставки контента. Каждая из этих служб может иметь уникальные политики до- ступа, которые должны быть назначены для защиты данных, которые они хранят. Потребители облачных услуг должны понимать и настраивать эти специфич- ные для службы политики доступа.

Помимо контроля доступа, защита данных вклю- чает три отдельные задачи: защита данных от несанк- ционированного доступа, обеспечение постоянного доступа к критически важным данным в случае оши- бок и сбоев и предотвращение случайного раскрытия данных, которые предположительно были удалены.

Важно шифровать данные в состоянии покоя, чтобы защитить их от разглашения из-за несанкциониро- ванного доступа. Провайдеры обычно предостав- ляют возможности шифрования для услуг хранения, которые они предлагают. Также следует правильно управлять связанными ключами шифрования, чтобы обеспечить эффективное шифрование. Провайдеры предлагают потребителям выбор ключей, управляе- мых ими самими или потребителем.

Провайдеры предоставляют значительные гаран- тии от потери постоянных данных. Однако, ни одна система не является идеальной, и крупные постав- щики облачных услуг могут случайно потерять дан- ные клиентов. В дополнение к ошибкам провайдеров, пользователи облачных сервисов могут также совер- шать ошибки, которые могут привести к потере дан- ных. Необходимо убедиться, что процессы резерв- ного копирования и восстановления данных соответ- ствуют потребностям организации, использующей облачные сервисы. Провайдеры часто копируют дан- ные, чтобы обеспечить постоянство. В ходе работы системы конфиденциальные данные могут попасть в службы регистрации и мониторинга, резервные ко- пии, службы распространения контента и другие ме- ста. Следует проанализировать развертывание об- лака, чтобы понять, где могут быть скопированы или кэшированы конфиденциальные данные, и опреде- лить, что нужно сделать, чтобы эти копии были уда- лены.

Провайдер отвечает за мониторинг инфраструк- туры и услуг, предоставляемых потребителям, но не отвечает за мониторинг систем и приложений, созда- ваемых пользователями с использованием предо- ставляемых услуг. Однако они предоставляют потре- бителю информацию мониторинга, связанную с ис- пользованием услуг пользователей. Эта информация может быть использована в качестве первой линии мониторинга для обнаружения несанкционирован- ного доступа к системам и приложениям или их ис- пользования, а также неожиданного поведения или использования систем и приложений или их пользо- вателей.

При гибридном облачном развертывании, кото- рое перемещает некоторые ресурсы на хранилища провайдера, но сохраняет много ресурсов на месте, необходимо объединить предоставленную провайде- ром информацию мониторинга пользователей на ос- нове облака и информацию мониторинга локальных пользователей для создания полной картины положе- ния информационной безопасности организации.

Угрозы информационной безопасности могут появиться в любой точке облачной инфраструктуры. Если эти уязвимости не обнаружены и не закрыты, предприятие оставляет возможность для угроз без- опасности войти в свое облачное развертывание.

Многие облачные провайдеры позволят пользовате- лям выполнять тесты на проникновение для поиска этих уязвимостей. Некоторые провайдеры могут вы- полнить это тестирование самостоятельно. Обеспе- чение того, чтобы эти тесты выполнялись на регуляр- ной основе, позволяет искать любые уязвимости, ко- торые появились в системе пользователя облачных сервисов.

# Много-облачные вычисления

## Введение в много-облачную стратегию

Много-облачная стратегия – это использование двух или более сервисов различных провайдеров об- лачных вычислений, а также использование различ- ных моделей предоставления сервисов [21]. Первона- чально многие организации придерживались страте- гии использования нескольких облаков, потому что они не были уверены в надежности облака. Много- облачные вычисления по-прежнему рассматрива- ются как способ предотвратить потерю данных или избежать простоев из-за сбоя локализованного ком- понента в облаке. Возможность избежать привязки к конкретным провайдерам также была важным стиму- лом на раннем этапе внедрения нескольких облаков. Несмотря на то, что проблемы избыточности и привязки к провайдерам по-прежнему являются дви- жущей силой многих развертываний в много-облач- ных средах, они также в значительной степени обу- словлены более широкими деловыми или техниче- скими целями предприятия. Эти цели могут вклю- чать использование более конкурентоспособных по цене облачных услуг или использование преиму- ществ скорости, емкости или функций, предлагае- мых конкретным поставщиком облачных услуг в

конкретной географии.

Кроме того, некоторые организации используют много-облачные стратегии по причинам суверени- тета данных. Некоторые законы, правила и корпора- тивные политики требуют, чтобы корпоративные данные физически находились в определенных ме- стах. Много-облачные вычисления могут помочь ор- ганизациям удовлетворить эти требования, по- скольку они могут выбирать из нескольких центров обработки данных или зон доступности нескольких провайдеров сервисов модели IaaS. Такая гибкость в размещении облачных данных также позволяет орга- низациям размещать вычислительные ресурсы как можно ближе к конечным пользователям для дости- жения оптимальной производительности и мини- мальной задержки.

Однако существует ряд издержек, вызванные использованием данной стратегии, например, для развертывания нескольких облаков требуется, чтобы

технический персонал обладал навыками работы с несколькими видами облачных платформ или прибе- гать к консультациям провайдера. Рабочая нагрузка или управление приложениями в много-облачных средах также может быть проблемой, поскольку ин- формация перемещается с одной облачной плат- формы на другую.

Также важно понимать разницу с гибридной мо- делью развертывания. Много-облачные и гибридные облачные вычисления похожи, но отличаются в це- лях и задач применения. В целом, гибридное облако относится к среде облачных вычислений, в которой используется сочетание локального приватного об- лака и стороннего публичного облака с согласова- нием между ними. Предприятие часто применяет ги- бридное облако для решения конкретной задачи, та- кой как способность выполнять рабочие нагрузки в домашних условиях, а затем врываться в публичное облако при резком росте вычислительных ресурсов.

Однако, как отмечалось выше, много-облачные вычисления обычно относятся к использованию не- скольких провайдеров публичных облаков и пред- ставляют собой более общий подход к управлению и оплате облачных услуг таким образом, который ка- жется наилучшим для данной организации. Хотя, необходимо отметить, что использование нескольких облаков не исключает возможности использования гибридного облака, и оно может быть частью развер- тывания нескольких облаков. Две модели не явля- ются взаимоисключающими, их использование про- сто зависит от того, чего пользователь облачных вы- числений надеется достичь.

## Анализ производительности облачных вычислений

Важным фактором при планировании использо- вания много-облачной стратегии является произво- дительность облачных сервисов. Данная тема рас- сматривается во многих работах, таких как «Explor- ing Uncertainty of Delays as a Factor in End-to-End Cloud Response Time» [22] и «Dependability of Ser- vice-Oriented Computing: Time-Probabilistic Failure Modelling» [23]. Для получения последних результа- тов в этой области можно обратиться к интересному докладу «ThousandEyes Cloud-Performance Bench- mark 2019-2020» [24], в котором проводился анализ производительности пяти крупнейших облачных провайдеров (AWS, GCP, Azure, Alibaba Cloud, IBM Cloud). Также они рассматривали вопрос применения много-облачной стратегии. В результате чего, они пришли к выводу, что несмотря на то, что произво- дительность сети не была традиционной метрикой, которую следует учитывать при разработке много- облачной стратегии, однако глобальные изменения

производительности подтверждают необходимость использования нескольких облачных сред.

Таким образом, AWS, Azure и GCP напрямую взаимодействуют друг с другом в полной сетке со- единений, устраняя зависимость от сторонних интер- нет провайдеров для много-облачной связи. Эти три облачных провайдера имеют обширные сети и хо- рошо связаны между собой несколькими популяр- ными средствами размещения. Основываясь на про- тестированных ими комбинациях, IBM продемон- стрировал тесную связь с GCP и Azure, но имел не- равномерную связь с AWS и Alibaba Cloud. Каса- тельно Alibaba Cloud, они заметили сильное взаимо- действие с Azure и GCP в хорошо связанных геогра- фических регионах, таких как Восток США, Запад и Лондон, но не в Азии. Облачные сервисы Alibaba Cloud и AWS по большей части не имели прямого пи- ринга независимо от географии. Следовательно, важно учитывать фактор пиринга и прямого подклю- чения к облачному провайдеру, повышающий произ- водительность по сравнению с подключением через Интернет-провайдера, при выборе областей разме- щения облачных сервисов для проектирования архи- тектуры много-облачных приложений. На рис. 1 [24] представлены результаты измерений средней за- держки в зоне доступности на протяжении 4 недель для крупнейших облачных провайдеров.

# Обеспечение безопасности облачных ресурсов основанный

**на принципе диверсности**

Диверсность является широко используемым принципом обеспечения безопасности и надежности критично важных систем, базирующимся на созда- нии избыточности не за счет резервирования си- стемы, а при помощи проектирования нескольких уникальных версии для каждого компонента. Таким образом, отказ одной версии не приведет к отказу остальных версий, а значит удастся избежать отказа всей системы. Хотя реализация такого принципа на практики не всегда рациональна по причине повыше- ния издержек на разработку системы, в которой он применяется. Несмотря на это, для самых критичных компонентов системы такой подход может быть чрезвычайно полезным. Так как он позволяет сохра- нить критичные данные или избежать простоя си- стемы.

Для программного обеспечения диверсность можно применить на любых этапах жизненного цикла ПО, в зависимости от чего, будут различаться виды диверсности. Самым популярным из которых является применения диверсности при проектирова-



Рис. 1. Результаты измерения средней задержки в зоне доступности

нии системы. Который в свою очередь делиться на N- версионное программирование, Само-проверяюще- еся программирование и Блоки восстановления [25]. В N-версионном программировании обычно исполь- зуют различные языки программирования, операци- онные системы, команды разработчиков и т.д., тем самым делая версии программы отличными друг от друга.

В облачных вычислениях наиболее близким к диверсности является много-облачная стратегия, в которой используются различные сервисы от разных облачных провайдеров. Однако в большинстве слу- чаев такая стратегия не призвана повысить безопас- ность, а скорее снижает издержки на поддержание облачных вычислений. Таким образом, близкие по реализации, но различные по целям много-облачная стратегия и диверсность могут применяться одновре- менно, при этом важно находить баланс между без- опасностью и производительностью и стоимостью облачных ресурсов.

Исходя из вышесказанного, можно предложить реализацию принципа диверсности для использова- ния облачных ресурсов. Как показано на рис. 2, пред- лагается использовать одновременно трех облачных провайдеров, для каждого из которых применять три модели предоставления облачных сервисов и разме- щать их в различных регионах. Также возможно ис- пользовать как публичное, так и приватное разверты- вание облачных ресурсов.

Особое внимание стоит уделить диверсности облачных сервисов, поскольку, помимо различных моделей представления, сервисы могут отличаться используемыми технологиями, языками программи- рования, операционными системами, инструментами разработки и поддержания инфраструктуры. Если

рассматривать сервисы модели IaaS, то очевидным решением будет выбирать виртуальные машины с различными операционными системами, например, Ubuntu, Centos, Windows Server. На уровне модели PaaS пользователи имеют дело с сервис-ориентиро- ванной архитектурой, а значит могут применять принцип диверсности с помощью использования раз- личных готовых сервисов. Одним из самых популяр- ных видов сервисов для этой модели являются сер- висы, предоставляющие базы данных, для них тоже можно применить принцип диверсности, например, использовать MySQL, PostgreSQL и SQL Server си- стемы управления базами данных. В целом, набор предоставляемых сервисов модели PaaS является главным отличием провайдеров облачных сервисов, поэтому имеет смысл ознакомится с их решениями и использовать различные сервисы одновременно, как с точки зрения безопасности и надежности, так и для повышения гибкости системы и снижения издержек на ее обслуживание.

Существует большое количество облачных сер- висов модели SaaS, предоставляемых различными компаниями, что приводит к естественному появле- нию диверсности, вызванное рыночной конкурен- цией. Одним из примеров реализации принципа ди- версности сервисов данной модели является исполь- зование различных облачных хранилищ данных.

Например, большое количество людей пользу- ется Google Drive, OneDrive или Dropbox для хране- ния, как своей личной, так и коммерческой информа- ции. Одновременное использование различных хра- нилищ позволяет повысить количество информации, которое можно бесплатно там размещать. Однако это также можно использовать с целью повышения надежности хранимой там



Amazon Web

Services

Microsoft

Azure

Google Cloud

Platform



IaaS

PaaS

SaaS



Europe

Asia Pacific

North America



Public cloud

Private cloud

Hybrid cloud

Рис. 2. Схема диверсности для облачных вычислений

информации, размещая одну и ту же критичную ин- формацию в различных облачных хранилищах дан- ных.

Одним из наиболее перспективным направле- нием в облачных сервисах является модель FaaS, ко- торая позволяет пользователям загружать только свой программный код, а весь процесс по обслужива- нию и поддержанию программы и необходимой для нее инфраструктуры переложить на облачного про- вайдера. Таким образом масштабирование приложе- ния осуществляется на уровне конкретной функции, которая вызывается в ответ на запрос пользователя. В такой ситуации разработчики должны лишь вы- брать на каком языке будет их приложение и загру- жать соответствующие функции, написанные на этом языке. В такой ситуации принцип диверсности может применяться при выборе языка программирования. К примеру, использовать одинаковые по функционалу программные функции, но написанные на разных языках, таких как Java, Python и Node.js. Однако среди разных облачных провайдеров выбор языков может отличаться, следовательно это стоит учиты- вать при использовании нескольких облаков одно- временно. Схема диверсности облачных сервисов для различных моделей представления дана на рис. 3.

# Заключение

Обеспечение безопасности облачных сервисов во многом делегируется самому провайдеру облач- ных вычислений, однако несмотря на это, он не отве- чает за то, как пользуются его сервисами. Поэтому необходимо тщательно следить за уязвимостями и

снижать вероятность угроз, исходящих из особенно- стей облачных вычислений, так и традиционных для информационного пространства. Слабым местом лю- бых облачных вычислений являются люди, которые их используют, и среда доступа от облака до конеч- ных пользователей. Использование гибридной мо- дели развертывания, комбинируя с много-облачной стратегией в связке с принципом диверсности позво- лит минимизировать риски нарушения информаци- онной безопасности. При этом не стоит забывать про баланс между расходами на безопасность и поддер- жанием высокой производительности для макси- мально эффективного использования преимуществ облаков.

Существует ряд подходов к обеспечению без- опасности облачных ресурсов, большинство из кото- рых направлены на повышения осознанности проис- ходящего в облаке, либо на безопасный доступ к об- лачным сервисам. В остальном, все подходы схожи с традиционными, для информационных ресурсов, ме- рами безопасности. При этом основные правила, поз- воляющие снизить риски потери своих данных или их компрометации, описаны в рекомендациях по обеспечению безопасности от самих провайдеров об- лачных вычислений. Диверсность способна увели- чить надежность и безопасность сервисов по боль- шей части как подстраховка от угроз исходящих от провайдера, как случайных так и преднамеренных. Однако недостаточно качественное обучение персо- нала по безопасной работе с облаками может пере- черкнуть все остальные меры обеспечения безопас- ности облачных сервисов.

Ubuntu

Centos

Windows Server

MySQL

PostgreSQL

SQL Server



Google Drive

OneDrive

Dropbox

Java

Python

Node.js

AWS

Azure

Google Cloud

Рис. 3. Диверсность облачных сервисов

В дальнейшем следует провести эксперимент по оценке влияния диверсности облачных сервисов на надежность и информационную безопасность си- стемы, в которой они применяются. Также для при- менения принципа диверсности на практике следует проанализировать стоимость его внедрения в облач- ные сервисы, чтобы оценить насколько рентабельно использование такого подхода и для каких случаев это будет уместно.