ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 004.77.056 **doi: 10.32620/reks.2020.1.07**

В. В. ФРОЛОВ

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ»

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 информационных технологий, крайне важно обеспечить безопасность и надежность процессов, происходящих в облаках и обезопасить взаимодействие между клиентом и поставщиком облачных сервисов. Учитывая, 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 анализа 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 подхода, основанного на принципе диверсности. Существует множество подходов, обеспечивающих их безопасность, используя как традиционные, так и специфичные для облачных сред методы. Много-облачный подход является одним из наиболее перспективных стратегий повышения надежности за счет резервирования облачных ресурсов на серверах различных провайдеров облачных сервисов. Показано, что необходимо использовать диверсность для обеспечения надежности и безопасности критических компонентов систем. Принцип диверсности заключается в использовании уникальной версии каждого ресурса благодаря особой комбинации провайдера облачных вычислений, географического расположения центров обработки данных, моделей представления облачных сервисов и моделей развертывания облачной инфраструктуры. Подробно говорится о различиях между облачными провайдерами и о том, какие комбинации услуг предпочтительнее других, с точки зрения производительности. Кроме того, рассматриваются 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 безопасности; диверсность; облачные провайдеры; модель предоставления облачных сервисов; модель развертывания облачной инфраструктуры; отказ по общей причине; угрозы безопасности облачных вычислений.*

Введение

На сегодняшний день облачные вычисления являются одной из наиболее быстро развивающейся областью среди информационных технологий. Все больше проектов производят миграцию вычислительных ресурсов из своих центров обработки данных в облачные хранилища, доверяя свои данные облачным провайдерам. Однако по прежнему остается множество скептиков, полагающих что это является слишком опасным и их данные будут утеряны или они попадут к злоумышленникам. Безусловно информационная 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 провайдеры принимают ряд мер для существенного повышения безопасности, а также дают рекомендации как пользователи их сервисов могут поспособствовать улучшению ситуации со своей стороны. Так как ответственность за безопасность лежит не только на провайдере, но и на компаниях, которые пользуются их услугами. При этом человеческий фактор попрежнему остается главной уязвимостью, так как злонамеренное или случайное пренебрежения политиками безопасности способно свести на нет все меры безопасности.

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

Исходя из выше сказанного создание уникальных копий позволит уменьшить риски потери данных вследствие отказа по общей причине (ОПОП). ОПОП – это случайный отказ двух или более конструкций, систем или компонентов, вызванный любым скрытым недостатком при проектировании или изготовлении, из-за ошибок в эксплуатации или обслуживании, который вызывается любым событием, вызванным естественным явлением, эксплуатацией технологического процесса установки, или действие, вызванное человеком или любым внутренним событием в контрольно-измерительной системе [1].

Одним из наиболее эффективных решений проблемы ОПОП является принцип диверсности, согласно которому каждая версия системы должна быть уникальной. Исходя из выше сказанного, вероятность возникновения ОПОП сводится к минимуму [2]. Диверсность является принципом в измерительных системах, позволяющим определять различные параметры, использовать разные технологии, использовать разные логические схемы или алгоритмы 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 исследователями во многих странах мира. В работе «Security and Security and Privacy Issues in Cloud Computing» предложена обобщенная классификация угроз и средств защиты облачных вычислений [3]. Авторы «Cloud Computing Use Case Discussion Group» [4] обсуждают различные сценарии использования облачных вычислений и связанные с ними требования. Они рассматривают варианты использования с разных точек зрения, включая клиентов, разработчиков и инженеров безопасности. В статье «Cloud computing: benefits, risks and recommendations for information security» [5] исследованы различные риски информационной безопасности, связанные с использованием облачных вычислений, а также затронута тема вероятности рисков, возникших по причине существования уязвимости в облачных вычислениях. Аналогичные вопросы обсуждались в «Cloud Security Alliance (CSA) [6]. В работе «Cloud Security Issues» [7] обсуждают спецификации и цели Amazon Compute Service Level Agreement (ACSLA), связанные с расположением, разделением и восстановлением данных. В следующей работе «Cloud computing security issues and challenges» [8] обсуждаются проблемы безопасности высокого уровня в модели облачных вычислений, такие как целостность данных, безопасность конфиденциальной информации. Также сообщается о различных стандартах управления безопасностью. В статье «On Technical Security Issues in Cloud Computing» [9] обсуждаются технические проблемы безопасности, возникающие при использовании модели облачных вычислений, такие, как XML-атаки, атаки связанные с браузерами, и атаки с использованием переполнения (SYN flood). Авторы статьи «Understanding Cloud-Computing Vulnerabilities» [10] обсуждают уязвимости в системе безопасности, существующие в облачной платформе. Они сгруппировали возможные уязвимости связанные с технологией облачных вычислений, ее характеристиками и используемые меры по обеспечению безопасности. Исследование «A survey on security issues in service delivery models of cloud computing» [11] рассматривает проблемы безопасности модели предоставления облачных услуг, уделяя особое внимание модели SaaS. Основной идеей «Organizational cloud security and control: a proactive approach» [12] является рассмотрение механизмов контроля безопасности облачных вычислений с точки зрения их этического использования. В книге «Security, Privacy, and Digital Forensics in the Cloud» [13] подробно разбираются многие аспекты безопасности и приватности облаков.

Целью данной статьи является сравнение существующих подходов, обеспечивающих информационную безопасность облачных сервисов, а также предложение нового подхода, основанного на принципе диверсности. Во-первых, была рассмотрена текущая 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-облачные вычисления, которые могут существенно повысить надежность облачных сервисов, основанный на использовании нескольких облачных провайдеров одновременно (Раздел 2). Далее предлагается реализация принципа диверсности для обеспечения безопасности критичных, с точки зрения безопасности, облачных ресурсов (Раздел 3). В последнем разделе рассматриваются плюсы и минусы подходов, обеспечивающих безопасность облачных сервисов, и представлены планы на дальнейшие этапы исследования.

1. Анализ обеспечения безопасности облачных сервисов

1.1. Введение в облачные сервисы

Облачные вычисления имеют четыре модели предоставления услуг и три основных моделей развертывания. Модели развертывания бывают следующих видов [14 – 16]:

– приватное облако, в котором облачная платформа предназначена для конкретной организации;

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

– публичное облако, в котором облачная платформа доступна для публичных пользователей, которые могут там регистрироваться и использовать имеющеюся 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 злоумышленниками для кибератак. Модели предоставления облачных услуг включают в себя:

- Инфраструктура как сервис (IaaS) – модель, в которой облачные провайдеры предоставляют вычислительные 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 которой облачные провайдеры предоставляют платформы, инструменты и другие бизнес сервисы, которые позволяют пользователям разрабатывать, разворачивать и управлять их собственными приложениями, при этом не требуется устанавливать эти платформы и заниматься поддержкой инструментов на своих компьютерах. Модель PaaS может быть расположена на верхнем уровне модели IaaS или непосредственно над облачными инфраструктурами. При этом Google App Engine, Microsoft Azure Web App и AWS Elastic Beanstalk являются наиболее известными представителями модели PaaS.

- Программа как сервис (SaaS) – модель, в которой облачные провайдеры предоставляют приложения, расположенные на облачной инфраструктуре в качестве интернет сервисов для конечных пользователей, не требуя от заказчиков сервисов устанавливать 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, Outlook, OneDrive) являются ведущими провайдерами услуг модели SaaS, известные широкому кругу пользователей 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 необходимости его администрировать. Затем этот код может быть выполнен в ответ на событие, которое возникло по запросу пользователя, к примеру, нажатие кнопки мыши или ввод с клавиатуры. Эта модель может быть расположена на верхнем уровне любого облачного сервиса с предыдущих моделей. Известными представителями данной модели являются AWS Lambda, Google Cloud Functions и Microsoft Azure Functions.

Каждая модель предоставления услуг имеет различные возможные реализации, что усложняет разработку стандартной модели безопасности для каждой модели предоставления услуг. Более того, эти модели предоставления услуг могут сосуществовать в одной облачной платформе, что приводит к дальнейшему усложнению процесса управления безопасностью.

В модели облачных вычислений участвуют различные заинтересованные стороны: провайдер облачных вычислений (объект, который поставляет инфраструктуры потребителям облачных вычислений), поставщик сервисов (объект, который использует облачную инфраструктуру для доставки приложений или услуг конечным пользователям) и потребитель услуг (субъект, который использует службы, размещенные в облачной инфраструктуре), а также третья сторона, которая оказывает поддержку облачному провайдеру, либо поставщику сервисов.

1.2. Угрозы безопасности облачных вычислений

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

1.3. Подходы к обеспечению облачных вычислений

В многопользовательской среде, которая используется в облачных вычислениях, обеспечение информационной безопасности является непростой задачей. Безопасность должна быть реализована на каждом уровне архитектуры облачных приложений. Физическая безопасность, конечно же, обеспечивается провайдером облачных вычислений, что является дополнительным преимуществом использования облака. 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 стороной, оказывающей поддержку либо провайдеру, либо пользователям.	Угроза доступа инсайдеров к данным клиентов, использующих облачные сервисы, возрастает, поскольку каждая из моделей доставки может создавать потребность в нескольких внутренних пользователях: SaaS – администраторы облачного провайдера и поставщика его сервисов; PaaS - разработчики приложений и управляющие тестовым окружением; IaaS – консультанты облачной платформы с третьей стороны.
Угрозы исходящие извне: – удаленная программная атака облачной инфраструктуры; – удаленная программная атака облачных приложений; – удаленная аппаратная атака на облако; – удаленная программная и аппаратная атака на программное и аппаратное обеспечение конечных точек организаций пользователей облака; – социальная инженерия пользователей облачных провайдеров и пользователей облачных сервисов.	Можно предположить, что угроза со стороны внешних злоумышленников в большей степени распространяется на публичные облака, однако все типы моделей предоставления облачных сервисов подвержены влиянию внешних злоумышленников, особенно в приватных облаках, где могут быть заданы конечные точки пользователей. Облачные провайдеры с большими хранилищами данных, в которых хранятся данные кредитных карт, личная информация и конфиденциальная или интеллектуальная собственность, будут подвергаться атакам со стороны групп со значительными ресурсами, которые пытаются получить эти данные.
Утечка данных: – отказ безопасных прав доступа в нескольких доменах; – отказ электронных и физических транспортных систем для облачных данных и резервного копирования.	Угроза массовой утечки данных среди многих потенциально конкурирующих организаций, использующих одного и того же облачного провайдера, может быть вызвана человеческой ошибкой или неисправным оборудованием, что приведет к компрометации информации.
Разделение данных: – неправильно определенны периметры безопасности; – неправильная настройка виртуальных машин и гипервизоров.	Целостность данных в сложных средах облачного хостинга, таких как модель SaaS, настроенных для совместного использования вычислительных ресурсов клиентами, 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 облачные сервисы, поддерживают удаленный доступ для администрирования облачных сервисов клиентов и могут нанести преднамеренный ущерб их источникам данных.
Качество данных: – введение неисправных компонентов приложения или инфраструктуры.	Угроза влияния качества данных возрастает, поскольку облачные провайдеры размещают данные многих клиентов. Введение неисправного или неправильно сконфигурированного компонента, требуемого другим пользователем облака, может потенциально повлиять на целостность данных для других пользователей облака, совместно использующих инфраструктуру.
Управление изменениями: – тестирование на проникновение клиентов, которое влияет на других облачных клиентов; – изменения инфраструктуры в системах провайдеров, клиентов и сторонних пользователей облачных сервисов, которые влияют на облачных клиентов.	Поскольку поставщик облачных сервисов несет все большую ответственность за управление изменениями во всех моделях предоставления облачных вычислений, существует угроза того, что изменения могут привести к негативным последствиям. Это может быть вызвано программными или аппаратными изменениями в существующих облачных сервисах.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Продолжение табл. 1

Угроза	Описание
Угроза отказа в обслуживании: – распределенная пропускная способность сети с отказом в обслуживании; – отказ в обслуживании сетевого DNS; – отказ в предоставлении данных приложения.	Угроза отказа в обслуживании по отношению к доступным ресурсам облачных вычислений, как правило, является внешней угрозой для публичных облачных сервисов. Однако угроза может повлиять на все модели облачных сервисов, поскольку внешние и внутренние агенты угроз могут вводить компоненты приложений или оборудования, которые вызывают отказ в обслуживании.
Физическое нарушение: – нарушение IT-услуг облачного провайдера через физический доступ; – нарушение облачных IT-сервисов клиентов через физический доступ; – нарушение услуг сторонних провайдеров WAN.	Угроза нарушения работы облачных сервисов, вызванная физическим доступом, различна для крупных поставщиков облачных сервисов и их клиентов. Эти поставщики должны иметь опыт в обеспечении безопасности крупных центров обработки данных, и должны учитывать устойчивость среди других стратегий доступности. Существует угроза того, что пользовательская инфраструктура в облаке может быть физически нарушена как изнутри, так и извне, где менее безопасные офисные среды или удаленная работа являются стандартной практикой.
Использование слабых процедур восстановления: – вызов неадекватных процессов аварийного восстановления или процессов непрерывности бизнеса.	Угроза инициирования неадекватных процедур восстановления и управления инцидентами усиливается, когда пользователи облачных вычислений рассматривают возможность восстановления своих собственных систем параллельно с системами, управляемыми сторонними поставщиками облачных сервисов. Если эти процедуры не проверены, то они могут значительно влиять на время восстановления.

– Информационно-ориентированная безопасность – техника самозащиты данных, которая требует, чтобы интеллект был помещен в сами данные. Данные должны быть самоописуемыми и защищаться, независимо от их среды. При обращении к ним, данные обращаются к своей политике и пытаются воссоздать безопасную среду, которая проверена как надежная с использованием инфраструктуры доверенных вычислений.

– Высоконадежная аттестация удаленного сервера – многообещающий подход к решению проблемы отсутствия прозрачности, который основан на надежных вычислениях. В доверенной вычислительной среде на облачном сервере устанавливается доверенный монитор, который может отслеживать или проверять операции облачного сервера. Надежный монитор может предоставить подтверждение соответствия владельцу данных, гарантируя, что определенные политики доступа не были нарушены. Для обеспечения целостности монитора, доверенные вычисления также позволяют выполнять безопасную загрузку этого монитора рядом (и надежно изолированы) от операционной системы и приложений. Монитор может применять политики контроля доступа и выполнять задачи мониторинга или аудита. Для подтверждения соответствия подписывается код монитора и заявление о соответствии, выданное монитором. Когда владелец данных получает это подтверждение соответствия, он может проверить, что выполняется правильный код монитора и что облачный сервер выполнил политики контроля доступа.

– Бизнес-аналитика с улучшенной конфиденциальностью – другой подход для сохранения контроля над данными, который заключается в необходимости шифрования всех облачных данных. Проблема в этом подходе заключается в том, что шифрование ограничивает использование данных. В частности, поиск и индексация данных становится проблематичным, 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 шифрования, хотя существуют универсальные схемы шифрования, которые позволяют выполнять операции и вычисления на зашифрованных текстах.

– Бастионные хосты – это виртуальные машины, которые находятся в общедоступной подсети клиента и обычно доступны с использованием SSH или RDP. Как только удаленное соединение установлено с хостом-бастионом, оно действует как «скачкообразный» сервер, позволяя клиентам использовать SSH или RDP для входа в другие виртуальные машины (в пределах частных подсетей) глубже в пользовательском виртуальном приватном облаке (VPC). При правильной настройке с использованием групп

безопасности и сетевых списков ACL (NACL) бастион по сути действует как мост к пользовательским частным виртуальным машинам через Интернет [17].

Однако, главным принципом обеспечения безопасности облачных вычислений является следование 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 приложений и систем. Надлежащая проверка должна выполняться в течение всего жизненного цикла приложений и систем, развертываемых в облаке, включая планирование, разработку и развертывание, операции и вывод из эксплуатации. Важно понимать, что как провайдер облака, так и пользователь несут ответственность за безопасность облака. При подписании соглашение с провайдером, должно быть оговорено, за какие аспекты облачной безопасности отвечает пользователь и за какие аспекты будет заботиться провайдер.

Следующий важный момент – это управление доступом. Для управления доступом обычно требуется три возможности: способность идентифицировать и аутентифицировать пользователей, возможность назначать пользователям права доступа и возможность создавать и применять политики контроля доступа к ресурсам. Следует использовать многофакторную аутентификацию, чтобы уменьшить риск компрометации учетных данных. Похищенные учетные данные привилегированного пользователя позволяют злоумышленнику контролировать и настраивать ресурсы потребителя облака. Использование множества факторов требует от злоумышленника приобретения нескольких независимых элементов аутентификации, что снижает вероятность компрометации. Следует запланировать набор ролей для выполнения общих и индивидуальных обязанностей. Эти роли должны гарантировать, что никто не сможет негативно повлиять на весь виртуальный центр обработки данных. Провайдеры предлагают несколько различных типов услуг хранения, таких как виртуальные диски, хранилище больших двоичных объектов и службы доставки контента. Каждая из этих служб может иметь уникальные политики доступа, которые должны быть назначены для защиты данных, которые они хранят. Потребители облачных услуг должны понимать и настраивать эти специфичные для службы политики доступа.

Помимо контроля доступа, защита данных включает три отдельные задачи: защита данных от несанкционированного доступа, обеспечение постоянного доступа к критически важным данным в случае ошибок и сбоев и предотвращение случайного раскрытия данных, которые предположительно были удалены. Важно шифровать данные в состоянии покоя, чтобы защитить их от разглашения из-за несанкционированного доступа. Провайдеры обычно предоставляют возможности шифрования для услуг хранения, которые они предлагают. Также следует правильно управлять связанными ключами шифрования, чтобы обеспечить эффективное шифрование. Провайдеры предлагают потребителям выбор ключей, управляемых ими самими или потребителем.

Провайдеры предоставляют значительные гарантии от потери постоянных данных. Однако, ни одна система не является идеальной, и крупные поставщики облачных услуг могут случайно потерять данные клиентов. В дополнение к ошибкам провайдеров, пользователи облачных сервисов могут также совершать ошибки, которые могут привести к потере данных. Необходимо убедиться, что процессы резервного копирования и восстановления данных соответствуют потребностям организации, использующей облачные сервисы. Провайдеры часто копируют данные, чтобы обеспечить постоянство. В ходе работы системы конфиденциальные данные могут попасть в службы регистрации и мониторинга, резервные копии, службы распространения контента и другие места. Следует проанализировать развертывание облака, чтобы понять, где могут быть скопированы или кэшированы конфиденциальные данные, и определить, что нужно сделать, чтобы эти копии были удалены.

Провайдер отвечает за мониторинг инфраструктуры и услуг, предоставляемых потребителям, но не отвечает за мониторинг систем и приложений, создаваемых пользователями с использованием предоставляемых услуг. Однако они предоставляют потребителю информацию мониторинга, связанную с использованием услуг пользователей. Эта информация может быть использована в качестве первой линии мониторинга для обнаружения несанкционированного доступа к системам и приложениям или их использования, а также неожиданного поведения или использования систем и приложений или их пользователей.

При гибридном облачном развертывании, которое перемещает некоторые ресурсы на хранилища провайдера, но сохраняет много ресурсов на месте, необходимо объединить предоставленную провайдером информацию мониторинга пользователей на основе облака и информацию мониторинга локальных пользователей для создания полной картины положения 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 безопасности войти в свое облачное развертывание.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Многие облачные провайдеры позволят пользователям выполнять тесты на проникновение для поиска этих уязвимостей. Некоторые провайдеры могут выполнить это тестирование самостоятельно. Обеспечение того, чтобы эти тесты выполнялись на регулярной основе, позволяет искать любые уязвимости, которые появились в системе пользователя облачных сервисов.

2. Много-облачные вычисления

2.1. Введение в много-облачную стратегию

Много-облачная стратегия – это использование двух или более сервисов различных провайдеров облачных вычислений, а также использование различных моделей предоставления сервисов [21]. Первоначально многие организации придерживались стратегии использования нескольких облаков, потому что они не были уверены в надежности облака. Много-облачные вычисления по-прежнему рассматриваются как способ предотвратить потерю данных или избежать простоев из-за сбоя локализованного компонента в облаке. Возможность избежать привязки к конкретным провайдерам также была важным стимулом на раннем этапе внедрения нескольких облаков.

Несмотря на то, что проблемы избыточности и привязки к провайдерам по-прежнему являются движущей силой многих развертываний в много-облачных средах, они также в значительной степени обусловлены более широкими деловыми или техническими целями предприятия. Эти цели могут включать использование более конкурентоспособных по цене облачных услуг или использование преимуществ скорости, емкости или функций, предлагаемых конкретным поставщиком облачных услуг в конкретной географии.

Кроме того, некоторые организации используют много-облачные стратегии по причинам суверенитета данных. Некоторые законы, правила и корпоративные политики требуют, чтобы корпоративные данные физически находились в определенных местах. Много-облачные вычисления могут помочь организациям удовлетворить эти требования, поскольку они могут выбирать из нескольких центров обработки данных или зон доступности нескольких провайдеров сервисов модели IaaS. Такая гибкость в размещении облачных данных также позволяет организациям размещать вычислительные ресурсы как можно ближе к конечным пользователям для достижения оптимальной производительности и минимальной 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 прибегать к консультациям провайдера. Рабочая нагрузка или управление приложениями в много-облачных средах также может быть проблемой, поскольку информация перемещается с одной облачной платформы на другую.

Также важно понимать разницу с гибридной моделью развертывания. Много-облачные и гибридные облачные вычисления похожи, но отличаются в целях и задач применения. В целом, гибридное облако относится к среде облачных вычислений, в которой используется сочетание локального приватного облака и стороннего публичного облака с согласованием между ними. Предприятие часто применяет гибридное облако для решения конкретной задачи, такой 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 нескольких провайдеров публичных облаков и представляют собой более общий подход к управлению и оплате облачных услуг таким образом, который кажется наилучшим для данной организации. Хотя, необходимо отметить, что использование нескольких облаков не исключает возможности использования гибридного облака, и оно может быть частью развертывания нескольких облаков. Две модели не являются взаимоисключающими, их использование просто зависит от того, чего пользователь облачных вычислений надеется достичь.

2.2. Анализ производительности облачных вычислений

Важным фактором при планировании использования много-облачной стратегии является производительность облачных сервисов. Данная тема рассматривается во многих работах, таких как «Exploring Uncertainty of Delays as a Factor in End-to-End Cloud Response Time» [22] и «Dependability of Service-Oriented Computing: Time-Probabilistic Failure Modelling» [23]. Для получения последних результатов в этой области можно обратиться к интересному докладу «ThousandEyes Cloud-Performance Benchmark 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 производительность 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 соединений, устраняя зависимость от сторонних интернет провайдеров для много-облачной связи. Эти три облачных провайдера имеют обширные сети и хорошо связаны между собой несколькими популярными средствами размещения. Основываясь на протестированных ими комбинациях, IBM продемонстрировал тесную связь с GCP и Azure, но имел неравномерную связь с AWS и Alibaba Cloud. Касательно Alibaba Cloud, они заметили сильное взаимодействие с Azure и GCP в хорошо связанных географических регионах, таких как Восток США, Запад и Лондон, но не в Азии. Облачные сервисы Alibaba Cloud и AWS по большей части не имели прямого пиринга независимо от географии. Следовательно, важно учитывать фактор пиринга и прямого подключения к облачному провайдеру, повышающий производительность по сравнению с подключением через Интернет-провайдера, при выборе областей размещения облачных сервисов для проектирования архитектуры много-облачных приложений. На рис. 1 [24] представлены результаты измерений средней задержки в зоне доступности на протяжении 4 недель для крупнейших облачных провайдеров.

3. Обеспечение безопасности облачных ресурсов основанный на принципе диверсности

Диверсность является широко используемым принципом обеспечения безопасности и надежности критично важных систем, базирующимся на создании избыточности не за счет резервирования системы, 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 повышения 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 сохранить критичные данные или избежать простоя системы.

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-

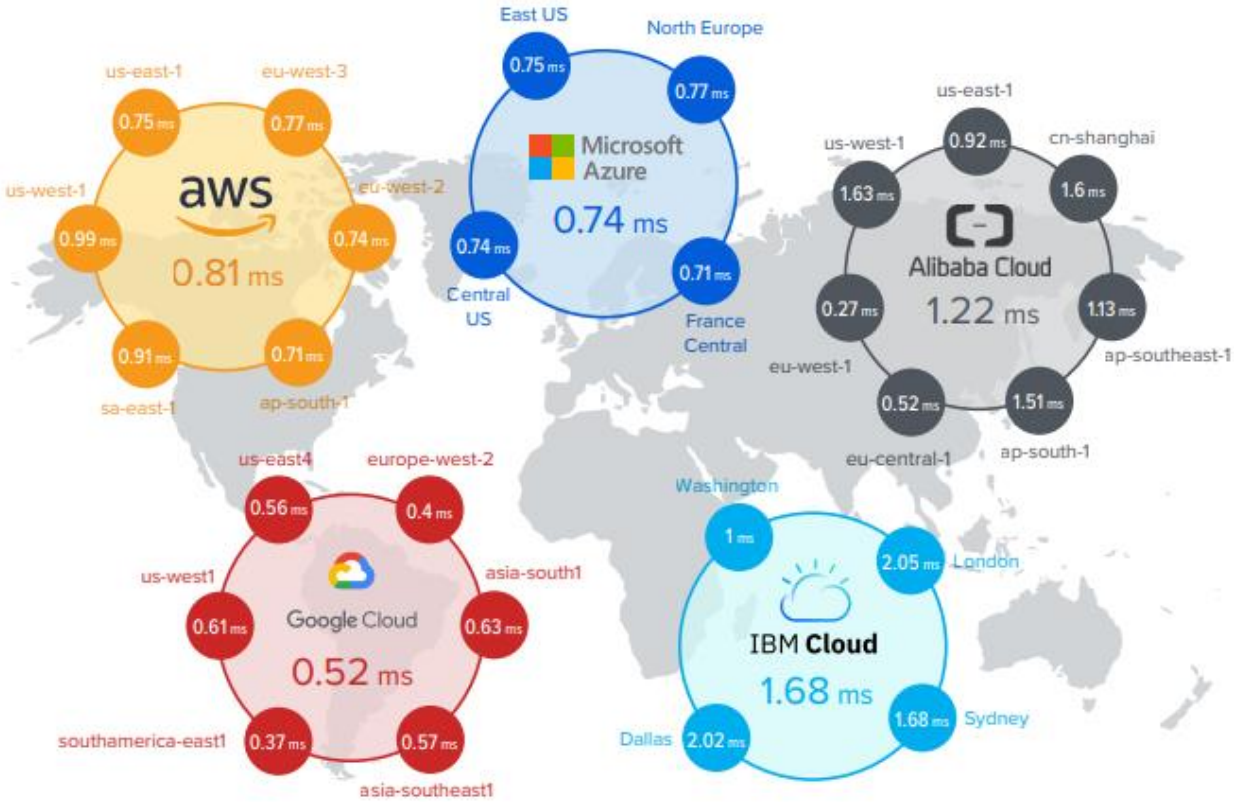

Рис. 1. Результаты измерения средней задержки в зоне доступности

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

нии системы. Который в свою очередь делиться на N-версионное программирование, Само-проверяющееся программирование и Блоки восстановления [25]. В N-версионном программировании обычно используют различные языки программирования, операционные 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 случаев такая стратегия не призвана повысить безопасность, а скорее снижает издержки на поддержание облачных вычислений. Таким образом, близкие по реализации, но различные по целям много-облачная стратегия и диверсность могут применяться одновременно, при этом важно находить баланс между безопасностью и производительностью и стоимостью облачных ресурсов.

Исходя из вышесказанного, можно предложить реализацию принципа диверсности для использования облачных ресурсов. Как показано на рис. 2, предлагается использовать одновременно трех облачных провайдеров, для каждого из которых применять три модели предоставления облачных сервисов и размещать их в различных регионах. Также возможно использовать как публичное, так и приватное развертывание облачных ресурсов.

Особое внимание стоит уделить диверсности облачных сервисов, поскольку, помимо различных моделей представления, сервисы могут отличаться используемыми технологиями, языками программирования, 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-ориентированной архитектурой, а значит могут применять принцип диверсности с помощью использования различных готовых сервисов. Одним из самых популярных видов сервисов для этой модели являются сервисы, предоставляющие базы данных, для них тоже можно применить принцип диверсности, например, использовать MySQL, PostgreSQL и SQL Server системы 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 сервисов модели SaaS, предоставляемых различными компаниями, что приводит к естественному появлению диверсности, вызванное рыночной конкуренцией. Одним из примеров реализации принципа диверсности сервисов данной модели является использование различных облачных хранилищ данных.

Например, большое количество людей пользуется Google Drive, OneDrive или Dropbox для хранения, как своей личной, так и коммерческой информации. Одновременное использование различных хранилищ позволяет повысить количество информации, которое можно бесплатно там размещать. Однако это также можно использовать с целью повышения надежности хранимой там

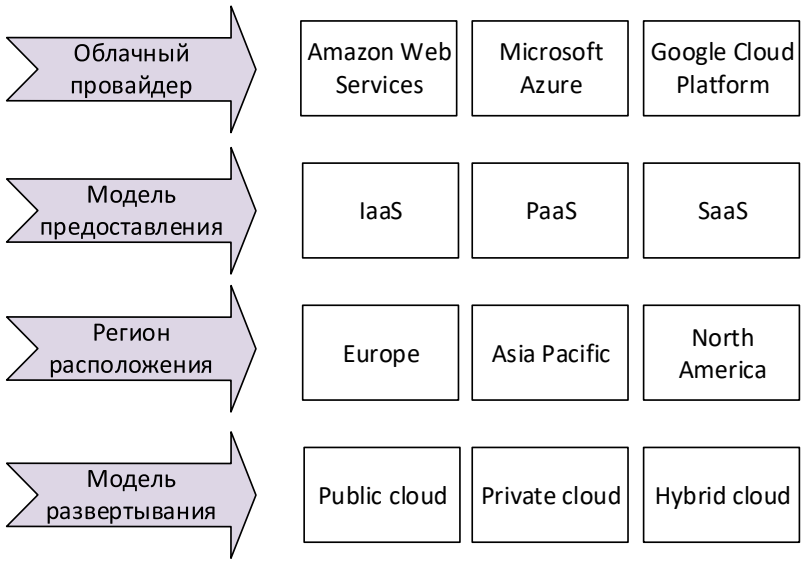

Рис. 2. Схема диверсности для облачных вычислений

информации, размещая одну и ту же критичную информацию в различных облачных хранилищах данных.

Одним из наиболее перспективным направлением в облачных сервисах является модель FaaS, которая позволяет пользователям загружать только свой программный код, а весь процесс по обслуживанию и поддержанию программы и необходимой для нее инфраструктуры переложить на облачного провайдера. Таким образом масштабирование приложения осуществляется на уровне конкретной функции, которая вызывается в ответ на запрос пользователя. В такой ситуации разработчики должны лишь выбрать на каком языке будет их приложение и загружать 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 учитывать при использовании нескольких облаков одновременно. Схема диверсности облачных сервисов для различных моделей представления дана на рис. 3.

Заключение

Обеспечение безопасности облачных сервисов во многом делегируется самому провайдеру облачных вычислений, однако несмотря на это, он не отвечает за то, как пользуются его сервисами. Поэтому необходимо тщательно следить за уязвимостями и снижать вероятность угроз, исходящих из особенностей облачных вычислений, так и традиционных для информационного пространства. Слабым местом любых облачных вычислений являются люди, которые их используют, и среда доступа от облака до конечных пользователей. Использование гибридной модели развертывания, комбинируя с много-облачной стратегией в связке с принципом диверсности позволит минимизировать риски нарушения информационной безопасности. При этом не стоит забывать про баланс между расходами на безопасность и поддержанием высокой производительности для максимально эффективного использования преимуществ облаков.

Существует ряд подходов к обеспечению безопасности облачных ресурсов, большинство из которых направлены на повышения осознанности происходящего в облаке, либо на безопасный доступ к облачным сервисам. В остальном, все подходы схожи с традиционными, для информационных ресурсов, мерами безопасности. При этом основные правила, позволяющие снизить риски потери своих данных или их компрометации, описаны в рекомендациях по обеспечению безопасности от самих провайдеров облачных вычислений. Диверсность способна увеличить надежность и безопасность сервисов по большей части как подстраховка от угроз исходящих от провайдера, как случайных так и преднамеренных. Однако недостаточно качественное обучение персонала по безопасной работе с облаками может перечеркнуть все остальные меры обеспечения безопасности облачных сервисов.

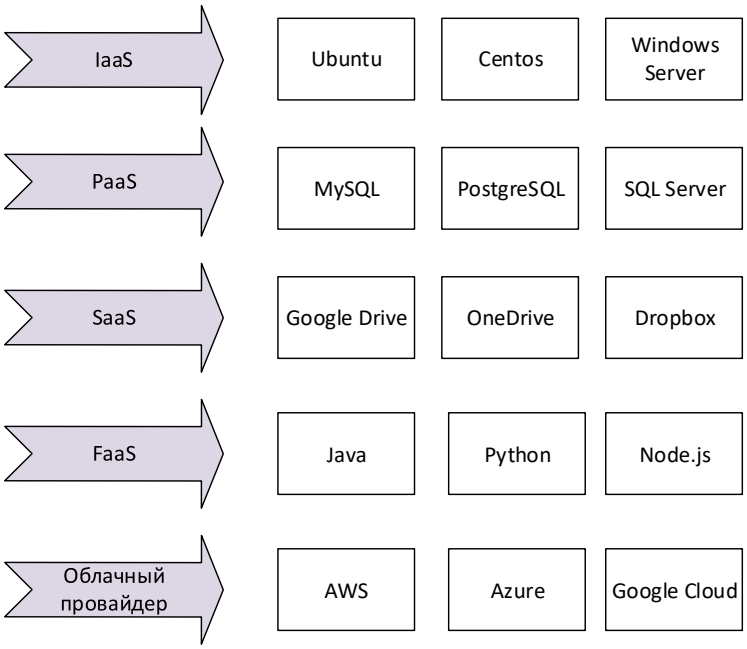

Рис. 3. Диверсность облачных сервисов

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

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

Литература

1. Diversity strategies for nuclear power instrumentation and control systems (NUREG/CR-7007, ORNL/TM-2009/302) [Text] / R. T. Wood, R. J. Belles, M. S. Cetiner, D. E. Holcomb et al. – U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC, 2010. – 225 p. DOI: 10.2172/1000417.

2. Yastrebenetsky, M. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security [Text] / M. Yastrebenetsky, V. Kharchenko. – IGI Global, USA, 2014. – 450 p.

3. Sen, J. Security and Privacy Issues in Cloud Computing [Electronic resource] / J. Sen. – Access mode: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf – 10.06.2019.

4. Cloud Computing Use Cases White Paper. Version 4.0. 2010. Cloud Computing. Use Case Discussion Group [Electronic resource]. – Access mode: http://www.cloud-council.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf. – 10.06.2019.

5. ENISA – Cloud computing: benefits, risks and recommendations for information security [Electronic resource]. – Access mode: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ENISA%20Cloud%20Computing%20Security%20Risk%20Assessment.pdf. – 21.12.2019.

6. Cloud Security Alliance (CSA) [Electronic resource]. – Access mode: http://www.cloudsecurityalliance.org/ – 20.12.2019.

7. Kandukuri, B. R. Cloud Security Issues [Text] / B. R. Kandukuri, R. Paturi, A. Rakshit // Proceedings of the 2009 IEEE International Conference on Services Computing, Bangalore, 21-25 September 2009. – P. 517-520.

8. Popovic, K. Cloud computing security issues and challenges [Text] / K. Popovic, Z. Hocenski // The Third International Conference on Advances in Humanoriented and Personalized Mechanisms, Technologies, and Services, 2010. – P. 344-349.

9. On Technical Security Issues in Cloud Computing [Text] / M. Jensen, J. Schwenk, N. Gruschka, L. L. Iacono // IEEE ICCC. – Bangalore, 2009. – P. 109-116.

10. Grobauer, B, Walloschek, T., Stöcker, E. Understanding Cloud Computing Vulnerabilities [Text] / B. Grobauer, T. Walloschek, E. Stöcker // IEEE Security and Privacy. – 2011. – Vol. 9, No. 2. – P. 50-57. DOI: 10.1109/MSP.2010.115.

11. Subashini, S. A survey on security issues in service delivery models of cloud computing [Text] / S. Subashini, V. Kavitha // Journal of Network and Computer Applications. – 2011. – Vol. 34, No. 1. – P. 1-11. DOI: 10.1016/j.jnca.2010.07.006.

12. Organizational cloud security and control: a proactive approach [Text] / K Spanaki., Z. Gürgüç, C. Mulligan, E. Lupu // Information Technology & People. – 2019. – Vol. 32, No. 3. – P. 516-537. DOI: 10.1108/ITP-04-2017-0131.

13. Chen, L. Security, Privacy, and Digital Forensics in the Cloud [Text] / L. Chen, H. Takabi, N.-A. Le-Khac (Eds.). – Higher Education Press, 2019. – 351 p. DOI: 10.1002/9781119053385.

14. Runtime Security Policy Enforcement in Clouds [Text] / S. Majumdar et al. // In: Cloud Security Auditing. Advances in Information Security. – Springer, Cham, 2019. – Vol. 76. – P. 145-156.

15. Wu, Y. Cloud storage security assessment through equilibrium analysis [Text] / Y. Wu, Y. Lyu, Y. Shi // Tsinghua Science and Technology. – 2019. – Vol. 24, No. 6. – P. 738-749. DOI: 10.26599/TST.2018.9010127.

16. Kumar, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey [Text] / R. Kumar, R. Goyal // Computer Science Review. – 2019. – Vol. 33. – P. 1-48. DOI: 10.1016/j.cosrev.2019.05.002.

17. Scott, S. Effective security requires close control over your data and resources. Bastion hosts, NAT instances, and VPC peering can help you secure your AWS infrastructure [Electronic resource] / S. Scott. – Access mode: https://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/ – 22.12.2019.

18. AWS security best practices [Electronic resource]. – Access mode: https://aws.amazon.com/whitepapers/aws-security-best-practices/ – 22.12.2019.

19. Microsoft Azure security best practices [Electronic resource]. – Access mode: https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns – 22.12.2019.

20. Google cloud platform security best practices [Electronic resource]. – Access mode: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations – 22.12.2019.

21. Multi-cloud strategy [Electronic resource]. – Access mode: https://searchcloudcomputing.techtarget.com/definition/multi-cloud-strategy –22.12.2019.

22. Dependability of Service-Oriented Computing: Time-Probabilistic Failure Modelling [Text] / A. Gorbenko, A. Romanovsky, V. Kharchenko, O. Tarasyuk // Software Engineering for Resilient Systems. – SERENE 2012. – Springer, Berlin, Heidelberg, 2012. – Lecture Notes in Computer Science vol. 7527. – P. 121-133. DOI: 10.1007/978-3-642-33176-3_9.

23. Exploring Uncertainty of Delays as a Factor in End-to-End Cloud Response Time [Text] / A. Gorbenko, V. Kharchenko, S. Mamutov, O. Tarasyuk, A. Roma-

novsky // Proceedings - 9th European Dependable Computing Conference, EDCC 2012. DOI: 10.1109/EDCC.2012.10.

24. A Comparative Study of Cloud Performance [Electronic resource]. – Access mode: https://www.thousandeyes.com/resources/cloud-performance-benchmark-report-november-2019 – 22.12.2019.

25. Frolov, V. Classification of Diversity for Dependable and Safe Computing [Electronic resource] / V. Frolov, O. Frolov, V. Kharchenko // COLINS, 2019. – Access mode: http://ceur-ws.org/Vol-2362/paper32.pdf – 22.12.2019.

References

1. Wood, R. T., Belles, R. J., Cetiner, M. S., Holcomb, D. E. et al. *Diversity strategies for nuclear power instrumentation and control systems (NUREG/CR-7007, ORNL/TM-2009/302).* U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC, 2010. – 225 p. DOI: 10.2172/1000417.

2. Yastrebenetsky, M., Kharchenko, V. *Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*. IGI Global, USA, 2014. 450 p.

3. Sen, J. *Security and Privacy Issues in Cloud Computing*. Available at: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf (accessed 10.06.2019).

4. *Cloud Computing Use Cases White Paper. Version 4.0. 2010. Cloud Computing. Use Case Discussion Group*. Available at: http://www.cloud-council.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf (accessed 10.06.2019).

5. *ENISA – Cloud computing: benefits, risks and recommendations for information security*. Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ENISA%20Cloud%20Computing%20Security%20Risk%20Assessment.pdf. (accessed 21.12.2019).

6. *Cloud Security Alliance (CSA).* Available at: http://www.cloudsecurityalliance.org/ (accessed 20.12.2019).

7. Kandukuri, B. R., Paturi, R., Rakshit, A. Cloud Security Issues. *Proceedings of the 2009 IEEE International Conference on Services Computing, Bangalore, 21-25 September 2009*, pp. 517-520.

8. Popovic, K., Hocenski, Z. Cloud computing security issues and challenges. *The Third International Conference on Advances in Humanoriented and Personalized Mechanisms, Technologies, and Services*, 2010, pp. 344-349.

9. Jensen, M., Schwenk, J., Gruschka, N., Iacono, L. L. On Technical Security Issues in Cloud Computing. *IEEE ICCC*, Bangalore, 2009, pp. 109-116.

10. Grobauer, B, Walloschek, T., Stöcker, E. Understanding CloudComputing Vulnerabilities. *IEEE Security and Privacy*, 2011, vol. 9, no. 2, pp. 50-57. DOI: 10.1109/MSP.2010.115.

11. Subashini, S., Kavitha, V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 2011, vol. 34, no. 1, pp. 1-11. DOI: 10.1016/j.jnca.2010.07.006.

12. Spanaki, K., Gürgüç, Z., Mulligan, C., Lupu, E. Organizational cloud security and control: a proactive approach. *Information Technology & People*, 2019, vol. 32, no. 3, pp. 516-537. DOI: 10.1108/ITP-04-2017-0131.

13. Chen, L., Takabi, H., Le-Khac, N.-A. (Eds.). *Security, Privacy, and Digital Forensics in the Cloud*, 2019, Higher Education Press Publ., DOI: 10.1002/9781119053385.

14. Majumdar, S. et al. Runtime Security Policy Enforcement in Clouds. *In: Cloud Security Auditing. Advances in Information Security*, Springer, Cham, 2019, vol. 76, pp. 145-156.

15. Wu, Y., Lyu, Y., Shi, Y. Cloud storage security assessment through equilibrium analysis. *Tsinghua Science and Technology*, 2019, vol. 24, no. 6, pp. 738-749. DOI: 10.26599/TST.2018.9010127.

16. Kumar, R., Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 2019, vol. 33, pp. 1-48. DOI: 10.1016/j.cosrev.2019.05.002.

17. Scott, S. *Effective security requires close control over your data and resources. Bastion hosts, NAT instances, and VPC peering can help you secure your AWS infrastructure*. Available at: https://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/ (accessed 22.12.2019).

18. *AWS security best practices*. Available at: https://aws.amazon.com/whitepapers/aws-security-best-practices/ (accessed 22.12.2019).

19. *Microsoft Azure security best practices.* Available at: https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns (accessed 22.12.2019).

20. *Google cloud platform security best practices*. Available at: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations (accessed 22.12.2019).

21. *Multi-cloud strategy.* Available at: https://searchcloudcomputing.techtarget.com/definition/multi-cloud-strategy (accessed 22.12.2019).

22. Gorbenko, A., Romanovsky, A., Kharchenko, V., Tarasyuk, O. Dependability of Service-Oriented Computing: Time-Probabilistic Failure Modelling. In: *Software Engineering for Resilient Systems. SERENE 2012*, Springer, Berlin, Heidelberg, 2019, Lecture Notes in Computer Science, vol 7527, pp. 121-133. DOI: 10.1007/978-3-642-33176-3_9.

23. Gorbenko, A., Kharchenko, V., Mamutov, S., Tarasyuk, O., Romanovsky, A. Exploring Uncertainty of Delays as a Factor in End-to-End Cloud Response Time. *Proceedings - 9th European Dependable Computing Conference, EDCC 2012*. DOI: 10.1109/EDCC.2012.10.

24. *A Comparative Study of Cloud Performance*. Available at: https://www.thousandeyes.com/resources/cloud-performance-benchmark-report-november-2019 (accessed 22.12.2019).

25. Frolov, V., Frolov O., Kharchenko V. Classification of Diversity for Dependable and Safe Computing. *COLINS, 2019*. Available at: http://ceur-ws.org/Vol-2362/paper32.pdf (accessed 22.12.2019).

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Поступила в редакцию 9.12.2020, рассмотрена на редколлегии 20.01.2020.

АНАЛІЗ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

В. В. Фролов

Стаття присвячена аналізу сучасних підходів, що забезпечують безпеку хмарних сервісів. Оскільки хмарні обчислення є однією з найбільш швидко зростаючих областей серед інформаційних технологій, вкрай важливо гарантувати безпеку і надійність процесів, які відбуваються у хмарах і убезпечити взаємодію між клієнтом і постачальником хмарних сервісів. З огляду на те, що побоювання з приводу втрати даних і їх компрометація є однією з головних причин того, що деякі компанії не переміщують свої обчислення в хмари. Об'єктом дослідження і аналізу даної роботи є хмарні сервіси, які надаються різними провайдерами хмарних сервісів. Метою дослідження даної роботи є порівняння існуючі підходів, що забезпечують інформаційну безпеку хмарних сервісів, а також пропозиція нового підходу, заснованого на принципі диверсності. Існує безліч підходів, які забезпечують їх безпеку, використовуючи як традиційні, так і специфічні для хмарних середовищ техніки. Багато-хмарний підхід є одним із найбільш перспективних стратегій підвищення надійності за рахунок резервування хмарних ресурсів на серверах різних провайдерів хмарних сервісів. Показано, що необхідно використовувати диверсність для забезпечення надійності і безпеки критичних компонентів систем. Принцип диверсності полягає у використанні унікальної версії кожного ресурсу завдяки особливій комбінації провайдера хмарних обчислень, географічного розташування центрів обробки даних, моделей надання хмарних сервісів і моделей розгортання хмарної інфраструктури. Детально йдеться про відмінності між хмарними провайдерами і про те, які комбінації послуг краще ніж інші з точки зору продуктивності. Крім того, розглядаються передові практики по забезпеченню безпеки хмарних ресурсів. Як результат, в даній роботі робиться висновок про те, що існує проблема недостатньої безпеки і надійності хмарних обчислень і того, як можна зменшити загрози, щоб уникнути відмови з загальної причини і як наслідок - втрати конфіденційних даних або простою системи, використовуючи диверсність хмарних сервісів

Ключові слова: хмарні сервіси; багато-хмарна стратегія; підхід до забезпечення хмарної безпеки; диверсність; хмарні провайдери; модель надання хмарних сервісів; модель розгортання хмарної інфраструктури; відмова з загальної причини; загрози безпеці хмарних обчислень.

ANALYSIS OF APPROACHES PROVIDING SECURITY OF CLOUD SEVICES

V. V. Frolov

The article is devoted to the analysis of modern approaches that ensure the security of cloud services. Since cloud computing is one of the fastest growing areas among information technology, it is extremely important to ensure the safety and reliability of processes occurring in the clouds and to secure the interaction between the client and the provider of cloud services. Given that fears about data loss and their compromise are one of the main reasons that some companies do not transfer their calculations to the clouds. The object of research and analysis of this work are cloud services, which are provided by various cloud service providers. The aim of the study of this work is to compare existing approaches that provide information security for cloud services, as well as offer a new approach based on the principle of diversity. There are many approaches that ensure their safety, using both traditional and cloud-specific. The multi-cloud approach is one of the most promising strategies for improving reliability by reserving cloud resources on the servers of various cloud service providers. It is shown that it is necessary to use diversity to ensure the reliability and safety of critical system components. The principle of diversity is to use a unique version of each resource thanks to a special combination of a cloud computing provider, the geographical location of data centers, cloud service presentation models, and cloud infrastructure deployment models. The differences between cloud providers and which combination of services are preferable to others in terms of productivity are discussed in detail. In addition, best practices for securing cloud resources are reviewed. As a result, this paper concludes that there is a problem of insufficient security and reliability of cloud computing and how to reduce threats in order to avoid a common cause failure and, as a result, loss of confidential data or system downtime using diversity of cloud services.

Keywords: cloud services; multi-cloud strategy; cloud security approach; diversity; cloud providers; cloud service delivery model; cloud deployment model; common cause failure; cloud security threats.

Фролов Вячеслав Вікторович – аспірант, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Frolov Viacheslav Viktorovich – PhD student, assistant lecturer of Computer Systems, Networks and Cybersecurity department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: v.frolov@csn.khai.edu, ORCID Author ID: 0000-0002-5860-7193.