Лекция 9. Облачная безопасность

План лекции

1. Виды облачных вычислений
2. Достоинства облачных вычислений
3. Недостатки облачных вычислений
4. Распределенные вычисления
5. Облачная безопасность

Глоссарий

- **Облачные вычисления** – технология обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис.
- **Инфраструктура как сервис** - это предоставление компьютерной инфраструктуры как услуги на основе концепции облачных вычислений.
- **Платформа как сервис** - это предоставление интегрированной платформы для разработки, тестирования, развертывания и поддержки веб-приложений как услуги.
- **Программное обеспечение как сервис** - модель развертывания приложения, которая подразумевает предоставление приложения конечному пользователю как услуги по требованию. Доступ к такому приложению осуществляется посредством сети, а чаще всего посредством Интернет-браузера.
- **Частное облако** - это вариант локальной реализации "облачной концепции", когда компания создает ее для себя самой, в рамках одной организации.
- **Публичное облако** – используется облачными провайдерами для предоставления сервисов внешним заказчикам.
- **Распределенные вычисления** – Технология когда большая ресурсоёмкая вычислительная задача распределяется для выполнения между множеством компьютеров, объединённых в мощный вычислительный кластер сетью или интернетом.

Сервисы облачного хранения данных

1. Концепция облачных вычислений

Первые идеи об использовании облачных вычислений (Cloud Computing) как публичной услуги были предложены еще в 1960-х известным ученым в области информационных технологий, изобретателем языка Lisp, профессором MIT и Стэнфордского университета Джоном Маккарти (John McCarthy). Понятие облака (cloud) уже давно ассоциируется с метафорическим изображением Интернета, с помощью которого доступны некоторые сервисы. Облачные вычисления – это практическая реализация данной идеи. Облачные вычисления основаны на масштабированных и виртуализованных ресурсах (данных и программах), которые доступны пользователям через Интернет и реализуются на базе мощных центров обработки данных (data centers).

С пользовательской точки зрения, имеются доступные "облака", предоставляемые различными компаниями, которые можно использовать для доступа к мощным вычислительным ресурсам, отсутствующим у пользователя (который может работать, например, на нетбуке). Пользователь платит абонентскую плату за использование облачных сервисов какой-либо фирмы.

Появление концепции облачных вычислений предопределили три ключевых тенденции - консолидация и виртуализация ИТ-инфраструктуры, а также понятие Software as a Service (SaaS).

Появление концепции облачных вычислений предопределили три ключевых тенденции - консолидация и виртуализация ИТ-инфраструктуры, а также понятие Software as a Service (SaaS).

Реализация первого реального проекта приписывается компании Salesforce.com, основанной в 1999 году. Именно тогда и появилось первое предложение нового вида b2b продукта "Программное обеспечение как сервис« (SaaS). Определенный успех Salesforce в этой области возбудил интерес у гигантов ИТ индустрии, которые спешно сообщили о своих исследованиях в области облачных технологий.

Первое бизнес-решение под названием "Amazon Web Services" было запущено в 2005 году компанией Amazon.com, которая активно занималась модернизацией своих датацентров. Следующим свою технологию постепенно ввела Google, начав с 2006 года b2b предложение SaaS сервисов под названием "Google Apps". И, наконец, свое предложение анонсировала компания Microsoft, презентовав ее на конференции PDC 2008 под названием "Azure Services Platform".

Сам факт высокой заинтересованности крупнейших игроков рынка ИТ демонстрирует определенный статус облачных вычислений как тренда 2009-2010 годов. Кроме того, с релизом Microsoft Azure Service Platform множество экспертов связывает новый виток развития веб-технологий и выход всей сферы облачных вычислений на новый уровень.

Напомним, что под облачными вычислениями мы понимаем программно-аппаратное обеспечение, доступное пользователю через Интернет или локальную сеть в виде сервиса, позволяющего использовать удобный интерфейс для удаленного доступа к выделенным ресурсам (вычислительным ресурсам, программам и данным).

На данный момент большинство облачных инфраструктур развернуто на серверах датацентров, используя технологии виртуализации, что фактически позволяет любому пользовательскому приложению использовать вычислительные мощности, совершенно не задумываясь о технологических аспектах. Тогда можно понимать "облако" как единый доступ к вычислениям со стороны пользователя.

2. Виды облачных вычислений

С понятием облачных вычислений часто связывают такие сервис-предоставляющие технологии, как:

- **"Инфраструктура как сервис"** ("Infrastructure as a Service" или "IaaS")
- **"Платформа как сервис"** ("Platform as a Service", "PaaS")
- **"Программное обеспечение как сервис"** ("Software as a Service" или "SaaS").

Рассмотрим каждую из этих технологий подробнее.

2.1. Инфраструктура как сервис (IaaS)

IaaS - это предоставление компьютерной инфраструктуры как услуги на основе концепции облачных вычислений.

IaaS состоит из трех основных компонентов:

- **Аппаратные средства (серверы, системы хранения данных, клиентские системы, сетевое оборудование)**
- **Операционные системы и системное ПО (средства виртуализации, автоматизации, основные средства управления ресурсами)**
- **Связующее ПО (например, для управления системами).**

IaaS основана на технологии виртуализации, позволяющей пользователю оборудования делить его на части, которые соответствуют текущим потребностям бизнеса, тем самым увеличивая эффективность использования имеющихся вычислительных мощностей. Пользователь (компания или разработчик ПО) должен будет оплачивать всего лишь реально необходимые ему для работы серверное время, дисковое пространство, сетевую пропускную способность и другие ресурсы. Кроме того, IaaS предоставляет в распоряжение клиента весь набор функций управления в одной интегрированной платформе.

IaaS избавляет предприятия от необходимости поддержки сложных инфраструктур центров обработки данных, клиентских и сетевых инфраструктур, а также позволяет уменьшить связанные с этим капитальные затраты и текущие расходы. Кроме того, можно получить дополнительную экономию, при предоставлении услуги в рамках инфраструктуры совместного использования.

Среди других инфра-сервисных компаний можно отметить:

GoGrid имеет очень удобный интерфейс для управления VPS, а также cloud storage с поддержкой протоколов SCP, FTP, SAMBA/CIFS, RSYNC, причем размер хранилища масштабируется на лету. В скором времени разработчики обещают добавить управление посредством API.

Enomaly представляет собой решение для развертывания и управления виртуальными приложениями в облаке, при этом управление услугами осуществляется через браузер. Приятным дополнением является автоматическое масштабирование виртуальных машин под текущую нагрузку, а также автобалансировка нагрузки. Среди поддерживаемых виртуальных архитектур поддерживаются Linux, Windows, Solaris и BSD Guests. Для виртуализации применяют не только Xen, но и KVM, а также VMware.

Eucalyptus представляет собой программный комплекс с открытым кодом для реализации cloud computing на кластерных системах. В настоящее время интерфейс совместим с Amazon EC2, но заявлена поддержка и других.

2.2. Платформа как сервис (PaaS)

PaaS - это предоставление интегрированной платформы для разработки, тестирования, развертывания и поддержки веб-приложений как услуги. Для разворачивания веб-приложений разработчику не нужно приобретать оборудование и программное обеспечение, нет необходимости организовывать их поддержку. Доступ для клиента может быть организован на условиях аренды.

Такой подход имеет следующие достоинства:

- **масштабируемость;**
- **отказоустойчивость;**
- **виртуализация;**
- **безопасность.**

Масштабируемость PaaS предполагает автоматическое выделение и освобождение необходимых ресурсов в зависимости от количества обслуживаемых приложением пользователей.

PaaS как интегрированная платформа для разработки, тестирования, разворачивания и поддержки веб-приложений позволит весь перечень операций по разработке, тестированию и разворачиванию веб-приложений выполнять в одной интегрированной среде, исключая тем самым затраты на поддержку отдельных сред для отдельных этапов.

Способность создавать исходный код и предоставлять его в общий доступ внутри команды разработки значительно повышает производительность по созданию приложений на основе PaaS.

Самым известным примером такой платформы является AppEngine от Google, которая предлагает хостинг для веб-приложений с возможностью покупать дополнительные вычислительные ресурсы (например, для тестирования высоких нагрузок). Для запуска приложений Google AppEngine на виртуальных кластерных системах была разработана платформа AppScale, не имеющая, тем не менее, никакого отношения к Google.

В системах веб-поиска и контекстной рекламы компании Yahoo используется платформа Hadoop, ориентированная на передачу больших объемов данных между сетевыми серверами.

Ну а в центре всей облачной инфраструктуры Microsoft — операционная система Windows Azure. Windows Azure создает единую среду, включающую облачные аналоги серверных продуктов Microsoft (реляционная база данных SQL Azure, являющаяся аналогом SQL

Server, а также Exchange Online, SharePoint Online и Microsoft Dynamics CRM Online) и инструменты разработки (.NET Framework и Visual Studio, оснащенная в версии 2010 года набором Windows Azure Tools). Так, например, программист, создающий сайт в Visual Studio 2010, может не выходя из приложения разместить свой сайт в Windows Azure.

2.3.Программное обеспечение как сервис (SaaS)

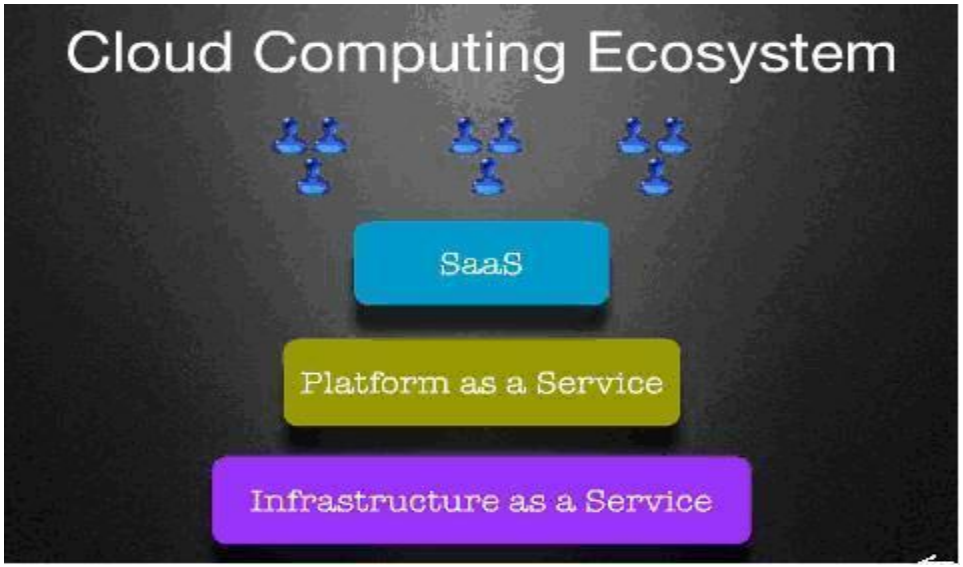

Рис. 1. Вершина айсберга облачных технологий представлена сервисами SaaS

SaaS – модель развертывания приложения, которая подразумевает предоставление приложения конечному пользователю как услуги по требованию (on demand). Доступ к такому приложению осуществляется посредством сети, а чаще всего посредством Интернет-браузера. В данном случае, основное преимущество модели SaaS для клиента состоит в отсутствии затрат, связанных с установкой, обновлением и поддержкой работоспособности оборудования и программного обеспечения, работающего на нём. Целевая аудитория - конечные потребители.

В модели SaaS:

- **приложение приспособлено для удаленного использования;**
- **одним приложением могут пользоваться несколько клиентов;**
- **оплата за услугу взимается либо как ежемесячная абонентская плата, либо на основе суммарного объема транзакций;**
- **поддержка приложения входит уже в состав оплаты;**
- **модернизация приложения может производиться обслуживающим персоналом плавно и прозрачно для клиентов.**

С точки зрения разработчиков программного обеспечения, модель SaaS позволит эффективно бороться с нелицензионным использованием программного обеспечения, благодаря тому, что клиент не может хранить, копировать и устанавливать программное обеспечение.

По-сути, программное обеспечение в рамках SaaS можно рассматривать в качестве более удобной и выгодной альтернативы внутренним информационным системам.

По недавно опубликованным данным SoftCloud спросом пользуются следующие SaaS приложения (в порядке убывания популярности):

- **Почта**
- **Коммуникации (VoIP)**
- **Антиспам и антивирус**
- **Helpdesk**
- **Управление проектами**
- **Дистанционное обучение**
- **CRM**
- **Хранение и резервирование данных.**

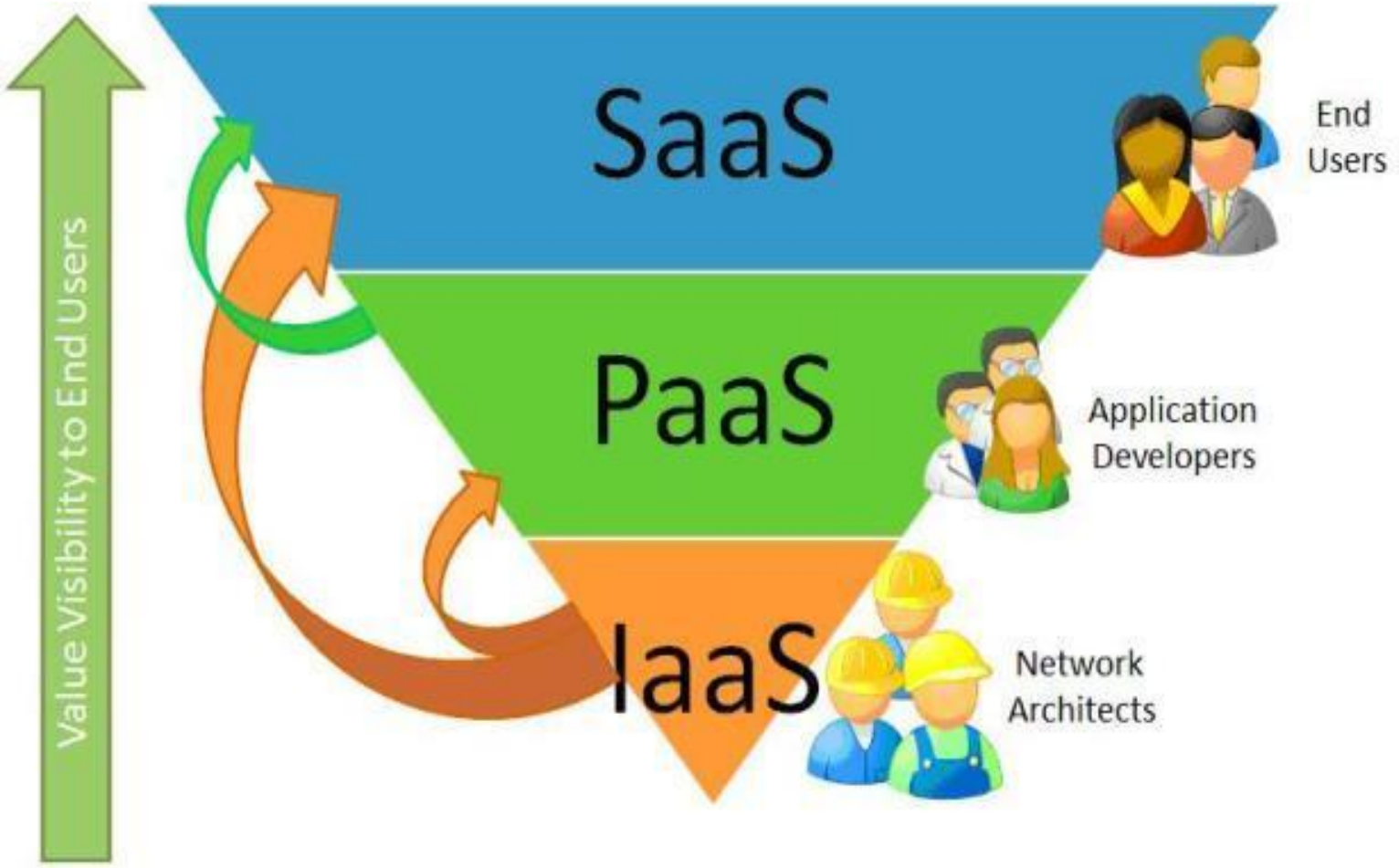

Рис. 2. Сервисы SaaS имеют наибольшую потребительскую базу

Весьма схожими являются продукты MobileMe (Apple), Azure (Microsoft) и LotusLive (IBM). Суть данных сервисов в том, что они предоставляют пользователям доступ к хранению своих данных (контакты, почта, файлы), а также для совместной работы нескольких пользователей с документами.

Вопросами хранения пользовательских данных в Интернет озадачена и компания Google, которая разрабатывает проект GDrive, который будет представлять собой виртуальный жесткий диск, который будет определяться ОС как локальный. Также заявлено, что можно будет хранить неограниченное количество данных, что звучит весьма заманчиво.

Хранение файлов без ограничений также предлагает MediaFire.com. Имеется как полностью бесплатное использование (правда, с некоторыми ограничениями, например, на максимальный размер загружаемого файла), так и покупка премиум-аккаунта, расширяющего возможности (например, шифрование файлов, получение прямых ссылок на скачивание).

Также к SaaS относятся услуги Online backup, или, проще говоря — резервному копированию данных. Пользователь просто платит абонентскую плату, а сервисы сами автоматически в определенное время шифруют данные с компьютера или другого устройства и отправляют их на удаленный сервер, тем самым данные могут быть доступны из любой точки земного шара.

Данную услугу сейчас предоставляют множество компаний, в том числе, такие как Nero и Symantec.

Интересное применение cloud-технологиям нашли и разработчики компьютерных игр: теперь современным компьютерам и игровым приставкам не будут нужны мощные графические адаптеры (видеокарты), ведь вся обработка данных и рендеринг будут производиться cloud-серверами, а игроки будут получать уже обработанное видео. Одним из первых заявил о себе сервис OnLive, и совсем недавно об этом заговорила и компания Sony, которая собирается внедрить данную идею в Playstation 3.

Согласно SaaS-концепции пользователь платит не единовременно, покупая продукт, а как бы берет его в аренду. Причем, использует ровно те функции, которые ему нужны. Например, раз в год вам нужна некая программа. И чаще вы ее использовать не собираетесь. Так зачем же покупать продукт, который будет у вас лежать без дела? И зачем тратить на него место (в квартире, если это коробка с диском, на винчестере, если это файл)?

Конкуренция в облачной сфере привела к появлению бесплатных сервисов. Именно по такому пути пошли два конкурента — Microsoft и Google. Обе компании выпустили наборы сервисов, позволяющих работать с документами. У Google это Google Docs, у Microsoft — Office Web Apps.

При этом, оба сервиса тесно взаимосвязаны с почтой (Gmail в первом случае и Hotmail во втором) и файловыми хранилищами. Таким образом, пользователя как бы переводят из привычной ему оффлайн-среды в онлайн. Важно, что и Google, и Microsoft интегрируют поддержку своих онлайн-сервисов во все программные среды — как настольные, так и мобильные (напомним, что Google создала ОС Android, а Microsoft — Windows Phone 7).

Аналогичную концепцию (но с несколько другими акцентами) продвигает и главный конкурент обеих компаний — Apple. Речь идет об очень любопытном сервисе под названием MobileMe. Сервис включает в себя почтовый клиент, календарь, адресную книгу, файловое хранилище, альбом фотографий и инструмент для обнаружения утерянного iPhone. За возможность пользоваться всем этим Apple берет примерно 65 евро (или 100 долларов) в год. При этом Apple обеспечивает такой уровень взаимодействия своего набора интернет-сервисов и приложений на компьютере (под управлением Mac OS X), телефоне, плеере и iPad, что необходимость в использовании браузера пропадает. Вы пользуетесь привычными программами на своем Mac, iPhone и iPad, однако, все данные хранятся не на них, а в облаке, что позволяет забыть о необходимости синхронизации, а также — о их доступности.

Если Apple интегрирует веб-сервисы в привычные приложения операционной системы, то Google заходит с противоположной стороны: разрабатываемая интернет-гигантом операционная система Chrome OS представляет собой, фактически, один браузер, через который пользователь взаимодействует с разветвленной сетью веб-сервисов. ОС ориентирована на нетбуки, отмечаются очень низкие системные требования и отсутствие необходимости самостоятельной установки программ (так как все программы работают непосредственно в вебе). То есть Google предоставляет преимущества облачной концепции, обычно декламируемые при работе с корпоративными клиентами, обычным пользователям. Вместе с тем, очевидна невозможность использования таких нетбуков в странах с недостаточно широким проникновением широкополосного интернета. Потому что без интернета нетбук на базе Chrome OS будет совершенно бесполезен.

Все три типа облачных сервисов взаимосвязаны, и представляют вложенную структуру.

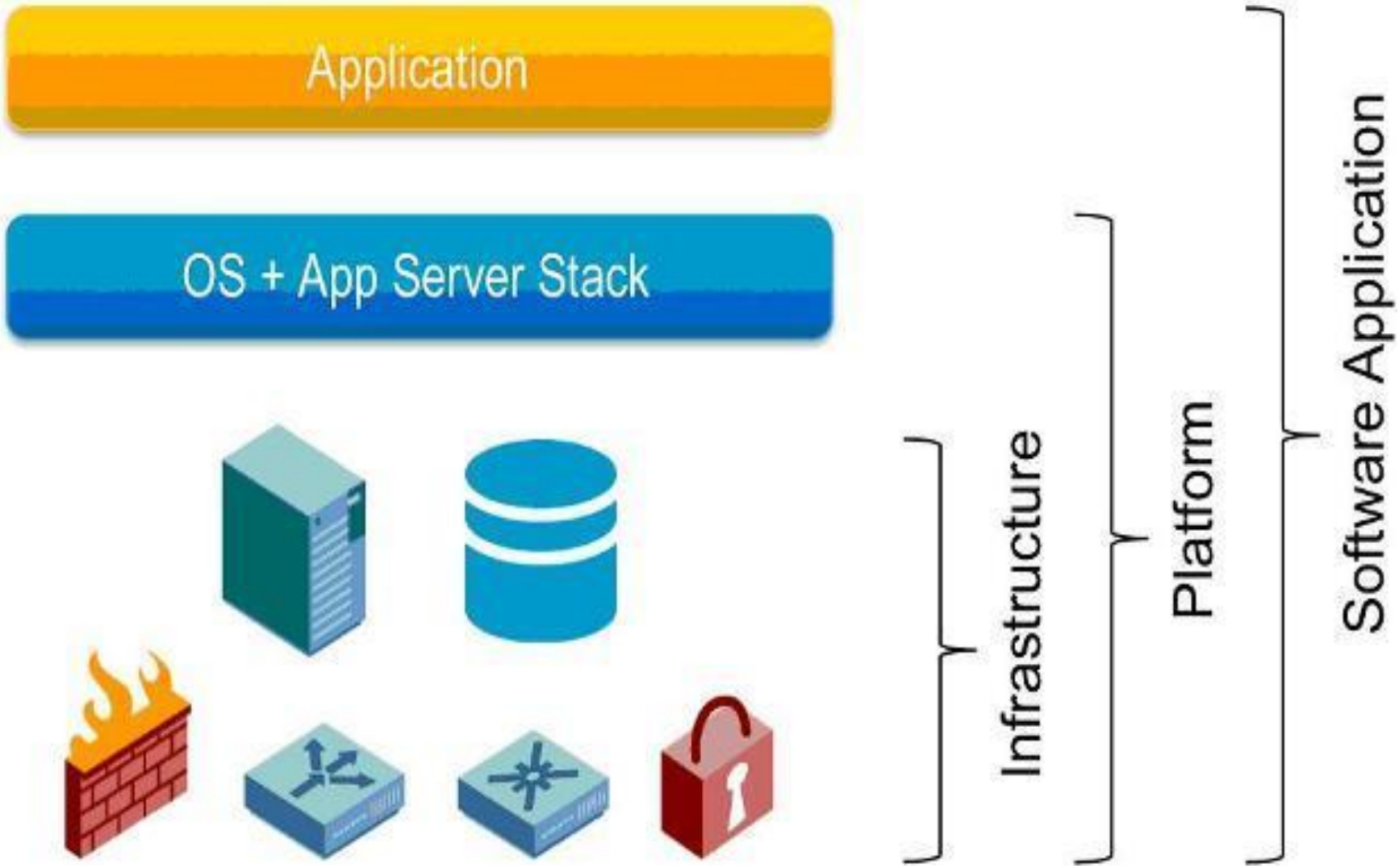

Рис. 3. Взаимосвязь облачных сервисов

Помимо различных способов предоставления сервисов различают несколько вариантов развёртывания облачных систем:

Частное облако (private cloud) - используется для предоставления сервисов внутри одной компании, которая является одновременно и заказчиком и поставщиком услуг. Это вариант реализации "облачной концепции", когда компания создает ее для себя самой, в рамках организации. В первую очередь реализация private cloud снимает один из важных вопросов, который непременно возникает у заказчиков при ознакомлении с этой концепцией – вопрос о защите данных с точки зрения информационной безопасности. Поскольку "облако" ограничено рамками самой компании, этот вопрос решается стандартными существующими методами. Для private cloud характерно снижение стоимости оборудования за счет использования простаивающих или неэффективно используемых ресурсов. А также, снижение затрат на закупки оборудования за счет сокращения логистики (не думаем, какие сервера закупать, в каких конфигурациях, какие производительные мощности, сколько места каждый раз резервировать и т.д.

В сущности, мощность наращивается пропорционально растущей в целом нагрузке, не в зависимости от каждой возникающей задачи – а, так сказать, в среднем. И становится легче и планировать, и закупать и реализовывать — запускать новые задачи в производство.

Публичное облако - **используется облачными провайдерами для предоставления сервисов внешним заказчикам.**

Смешанное (гибридное) облако - **совместное использование двух вышеперечисленных моделей развёртывания**

Вообще одна из ключевых идей Cloud заключается как раз в том, чтобы с технологической точки зрения разницы между внутренними и внешними облаками не было и заказчик мог гибко перемещать свои задания между собственной и арендуемой ИТ-инфраструктурой, не задумываясь, где конкретно они выполняются.

Рис. 4. Взаимосвязь облаков разных типов

Таким образом, эти технологии при совместном использовании позволяют пользователям облачных вычислений воспользоваться вычислительными мощностями и хранилищами данных, которые посредством определенных технологий виртуализации и высокого уровня абстракции предоставляются им как услуги.

2. Достоинства облачных вычислений

Рассмотрим основные преимущества и достоинства технологий облачных вычислений.

1. **Доступность и отказоустойчивость** – всем пользователям, из любой точки где есть Интернет, с любого компьютера, где есть браузер.

***Клиентские компьютеры*. Пользователям нет необходимости покупать дорогие компьютеры, с большим объемом памяти и дисков, чтобы использовать программы через веб-интерфейс. Также нет необходимости в CD и DVD приводах, так как вся информация и программы остаются в "облаке". Пользователи могут перейти с обычных компьютеров и ноутбуков на более компактные и удобные нетбуки.**

***Доступ к документам*. Если документы хранятся в "облаке", они могут быть доступны пользователям в любое время и в любом месте. Больше нет такого понятия как забытые файлы: если есть Интернет - они всегда рядом.**

***Устойчивость к потере данных или краже оборудования*. Если данные хранятся в "облаке", их копии автоматически**

распределяются по нескольким серверам, возможно находящимся на разных континентах. При краже или поломке персональных компьютеров пользователь не теряет ценную информацию, которую он к тому же может получить с любого другого компьютера.

Надежность. **Дата центры управляются профессиональными специалистами, обеспечивающими круглосуточную поддержку функционирования виртуальных машин. И даже если физическая машина "рухнет", благодаря распределению приложения на множество копий оно все равно продолжит свою работу. Это создает определенный высокий уровень надежности и отказоустойчивости функционирования системы.**

2. Экономичность и эффективность - плати столько, сколько используешь, позволь себе дорогие, мощные компьютеры и программы. "Облако" позволяет учитывать и оплачивать только фактически потребленные ресурсы строго по факту их использования.

***Аренда ресурсов*. Обычные сервера средней компании загружены на 10-15%. В одни периоды времени есть потребность в дополнительных вычислительных ресурсах, в других эти дорогостоящие ресурсы простаивают. Используя необходимое количество вычислительных ресурсов в "облаке" в любой момент времени, компании сокращают затраты на оборудование и его обслуживание.**

Это дает возможность заказчику отказаться от закупок дорогостоящих ИТ-активов в пользу их даже не аренды, а операционного потребления по мере надобности, при сокращении затрат на обслуживание своих систем и получении от поставщика гарантий уровня сервиса.

***Аренда ПО*. Вместо приобретения пакетов программ для каждого локального пользователя, компании покупают нужные программы в "облаке". Данные программы будут использоваться только теми пользователями, которым эти программы необходимы в работе. Более того, стоимость программ, ориентированных на доступ через Интернет, значительно ниже, чем их аналогов для персональных компьютеров. Если программы используются не часто, то их можно просто арендовать с почасовой оплатой. Затраты на обновление программ и поддержку в работоспособном состоянии на всех рабочих местах вовсе сведены к нулю.**

Для поставщика ИТ-услуг экономический смысл облака состоит в эффекте масштаба (обслуживать большой однородный центр обработки дешевле, чем множество маленьких разнородных) и сглаживания нагрузки (когда потребителей много, маловероятно, что пиковые мощности понадобятся всем им одновременно.

Разработчики ПО тоже получают выгоду от перехода в облака: теперь им стало проще, быстрее и дешевле разрабатывать, тестировать под нагрузкой и предлагать клиентам свои решения – это можно делать прямо в облаке с минимальными затратами. Кроме того, Облачные вычисления - это эффективный инструмент повышения прибыли и расширения каналов продаж для независимых производителей программного обеспечения в форме SaaS.

Этот подход позволяет организовать динамическое предоставление услуг, когда пользователи могут производить оплату по факту и регулировать объем своих ресурсов в зависимости от реальных потребностей без долгосрочных обязательств.

3. Простота - не требуется покупка и настройка программ и оборудования, их обновление.

Обслуживание. Так как физических серверов с внедрением Cloud Computing становится меньше, их становится легче и быстрее обслуживать. Что касается программного обеспечения, то последнее установлено, настроено и обновляется в "облаке". В любое время, когда пользователь запускает удаленную программу, он может быть уверен, что эта программа имеет последнюю версию - без необходимости что-то переустанавливать или платить за обновления.

Совместная работа. При работе с документами в "облаке" нет необходимости пересылать друг другу их версии или последовательно редактировать их. Теперь пользователи могут быть уверенными, что перед ними последняя версия документа и любое изменение, внесенное одним пользователем, мгновенно отражается у другого.

Открытые интерфейсы. "Облако" как правило, имеет стандартные открытые API (интерфейсы прикладного программирования) для связи с существующими приложениями и разработки новых – специально для облачной архитектуры.

4. **Гибкость и масштабируемость** - неограниченность вычислительных ресурсов (память, процессор, диски). "Облако" масштабируемо и эластично – ресурсы выделяются и освобождаются по мере надобности.

Производительные вычисления. По сравнению с персональным компьютером вычислительная мощь, доступная пользователю "облачных" компьютеров, практически ограничена лишь размером "облака", то есть общим количеством удаленных серверов. Пользователи могут запускать более сложные задачи, с большим количеством необходимой памяти, места для хранения данных, тогда, когда это необходимо. Иными словами, пользователи могут при

желании легко и дешево поработать с суперкомпьютером без каких-либо фактических приобретений. Возможность запуска множества копий приложения на многих виртуальных машинах представляет преимущества масштабируемости: количество экземпляров приложения способно практически мгновенно увеличиваться по требованию, в зависимости от нагрузок.

Хранение данных. По сравнению с доступным местом для хранения информации на персональных компьютерах объем хранилища в "облаке" может гибко и автоматически подстраиваться под нужды пользователя. При хранении информации в "облаке" пользователи могут забыть об ограничениях, накладываемых обычными дисками, - "облачные" размеры исчисляются миллиардами гигабайт доступного места.

5. Инструмент для стартапов. В глазах таких потребителей сервиса облачных вычислений как компании, начинающие свой бизнес, основным преимуществом данной технологии является, отсутствие необходимости закупать все соответствующее оборудование и ПО, а затем поддерживать их работу.

3. Недостатки облачных вычислений

Отметим основные недостатки и трудности использования облачных вычислений.

1. **Постоянное соединение с сетью. Cloud Computing почти всегда требует соединения с сетью (Интернет). Если нет доступа в сеть - нет работы, программ, документов. Многие "облачные" программы требуют хорошего Интернет-соединения с большой пропускной способностью. Соответственно программы могут работать медленнее чем на локальном компьютере. По мнению ведущих российских ИТ-компаний, основным препятствием широкому развитию облаков, является отсутствие широкополосного доступа в Интернет (ШПД) – прежде всего в регионах.**

Безопасность.

Безопасность данных теоретически может быть под угрозой. Не все данные можно доверить стороннему провайдеру в интернете, тем более, не только для хранения, но ещё и для обработки. Все зависит от того, кто предоставляет "облачные" услуги. Если этот кто-то надежно шифрует Ваши данные, постоянно делает их резервные копии, уже не один год работает на рынке подобных

услуг и имеет хорошую репутацию, то угрозы безопасности данных может никогда не случиться. У пользователя "облачных" бизнес приложений могут также возникнуть и юридические проблемы, например связанные с выполнением требований защиты персональных данных.

Государство, на территории которого размещен датацентр, может получить доступ к любой информации, которая в нем хранится. Например, по законам США, где находится самое большое количество датацентров, в этом случае компания-провайдер даже не имеет права разглашать факт передачи конфиденциальной информации кому-либо, кроме своих адвокатов.

Эта проблема является, наверное, одной из самых существенных в вопросе вывода конфиденциальной информации в облако. Путей ее решения может быть несколько. Во-первых, можно шифровать всю информацию, помещаемую на облако. Во-вторых, можно просто ее туда не помещать. Однако, во всяком случае, у компаний, пользующихся облачными вычислениями, это должно быть определенным пунктом в списке вопросов информационной безопасности. Кроме того, сами провайдеры должны улучшать свои технологии, предоставляя некоторые услуги по шифрованию.

2. **Функциональность "облачных" приложений**. **Не все программы или их свойства доступны удаленно. Если сравнивать программы для локального использования и их "облачные"аналоги, последние пока проигрывают в функциональности. Например, таблицы Google Docs или приложения Office web application имеют гораздо меньше функций и возможностей, чем Microsoft Excel.**

Зависимость от "облачного" провайдера

Всегда остаётся риск, что провайдер онлайновых сервисов однажды не сделает резервную копию данных – как раз перед крушением сервера. Риск этот, впрочем, вряд ли превышает опасность того, что пользователь сам упустит свои данные – потеряв или разбив мобильник или ноутбук, не создав на домашнем ПК резервную копию. Кроме того, привязавшись к той или иной услуге, мы в какой-то степени также ограничиваем свою свободу – свободу перехода на старую версию софта, выбора способов обработки информации и так далее.

Некоторые эксперты, например Г. Маклеод (Hugh Macleod) в статье "Самый хорошо охраняемый секрет Облаков", утверждают, что облачные вычисления ведут к созданию огромной, невиданной ранее монополии. Возможно ли это? Конечно, на рынке облачных вычислений для помещения в облако какой-либо информации, в

отношении которой существуют правила информационной безопасности, компании будут скорее использовать таких вендоров, чье имя "на слуху" и кому они доверяют. Таким образом, существует определенная опасность того, что все вычисления и данные будут агрегированы в руках одной сверхмонополии. Однако на данный момент на рынке уже существуют несколько компаний с примерно одинаковым высоким уровнем доверия со стороны клиентов (Microsoft, Google, Amazon), и нет никаких фактов, которые бы указывали на возможность доминирования одной компанией всех остальных. Поэтому в ближайшем будущем появление глобальной сверхкомпании, которая будет координировать и контролировать все вычисления в мире, очень маловероятно, хотя одна лишь возможность такого события отпугивает некоторых клиентов.

4. Препятствия развитию облачных технологий

1. **Недостаточное доверие потребителей облачных услуг. Нередко бизнес относится к облачным услугам несколько настороженно. "Причин же недоверчивого отношения малого и среднего бизнеса к облачным дата-центрам может быть несколько. Скорее всего, это боязнь лишиться контроля над ИТ-ресурсами, опасения насчет гарантии сохранности и защиты переданной информации и представление дата-центра лишь как площадки для размещения оборудования".**
2. **Каналы связи в большинстве регионов страны характеризуются отсутствием SLA по качеству предоставляемого сервиса (QoS), что особенно относится к последним милям. Что толку от того, что ваш основной трафик идет по магистрали с гарантированным QoS (со своими ограничениями), если конечные условия подключены к ней через местного оператора, даже не слышавшего о такой проблеме. При этом стоимость связи для крупных организаций может составлять до 50% от ИТ-бюджета. Соответственно переход к облачной модели существенно влияет на сетевую топологию ваших потоков данных и, скорее всего, QoS будет хуже чем во внутренней сети. Или чтобы получить качество обслуживания на**

приемлемом уровне придется заплатить столько денег, что вся экономия от централизации инфраструктуры или приложений будет перечеркнута ростом коммуникационных затрат.

3. **Безопасность**. Проблема безопасности является серьезным сдерживающим фактором. Нередко Службы Безопасности создают довольно высокий заградительный барьер для идеи вынести какие-либо данные за периметр своей сети. Часто без какой-либо вменяемой аргументации.
4. **Отсутствие надежных ЦОДов**. По поводу центров обработки данных (ЦОД) достаточно вспомнить, что в стране, кажется, еще нет ни одного Tier III ЦОДа по классификации Uptime Institute. Совершенно понятно, что их появление – это вопрос времени. Из-за кризиса большинство строек было заморожено или отложено. Тем не менее, пока достаточной инфраструктуры в стране просто нет.

5. Распределенные вычисления (grid computing)

Отметим в заключение еще одну технологию, которая с одной стороны также оказала влияние на появление концепции облачных вычислений, а с другой стороны имеет ряд существенных отличий. Речь идет о коллективных, или распределённых вычислениях (grid computing) – когда большая ресурсоёмкая вычислительная задача распределяется для выполнения между множеством компьютеров, объединённых в мощный вычислительный кластер сетью в общем случае или интернетом в частности.

Установление общего протокола в сети Интернет непосредственно привело к быстрому росту онлайн - пользователей. Это привело к необходимости выполнять больше изменений в текущих протоколах и к созданию новых. На текущий момент обширно используется протокол Ipv4 (четвёртая версия IP протокола), но ограничение адресного пространства, заданного ipv4, неизбежно приведет к использованию протокола ipv6. В течение долгого времени усовершенствовалось аппаратное и программное обеспечение, в результате чего удалось построить общий интерфейс в Интернет. Использование веб-браузеров привело к использованию модели "Облака", взамен традиционной модели информационного центра.

В начале 1990-ых, Иэн Фостер и Карл Кесселмен представили их понятие Грид-вычислений. Они использовали аналогию с электрической сетью, где пользователи могли подключаться и использовать услугу. Грид-вычисления во многом опираются на методах, используемых в кластерных вычислительных моделях, где многократные независимые группы, действуют, как сеть просто потому, что они не все расположены в пределах той же области.

В частности, развитие Грид-технологий позволило создать так называемые GRID-сети, в которых группа участников могла общими усилиями решать сложные задачи. Так, сотрудники IBM создали интернациональную команду grid-вычислений, позволившую существенно продвинуться в области борьбы с вирусом иммунного дефицита. Целые команды из разных стран присоединяли свои вычислительные мощности и помогли "обсчитать" и смоделировать наиболее перспективные формы для создания лекарства от СПИДа..."

На практике границы между этими (grid и cloud) типами вычислений достаточно размыты. Сегодня с успехом можно встретить "облачные" системы на базе модели распределённых вычислений, и наоборот. Однако будущее облачных вычислений всё же значительно масштабнее распределённых систем, к тому же не каждый "облачный сервис" требует больших вычислительных мощностей с единой управляющей инфраструктурой или централизованным пунктом обработки платежей.

Облачная безопасность

Облачная безопасность — это набор политик, средств контроля и технологий для защиты данных, приложений и инфраструктурных сервисов.

Безопасность облачных вычислений, также называемая облачной безопасностью, — это обобщенный термин, относящийся к технологиям, процессам и элементам контроля, используемым для защиты облачных инфраструктур, служб и приложений, а также данных, хранящихся или обрабатываемых в облаке.

Все эти компоненты работают вместе, помогая обеспечить безопасность данных, инфраструктуры и приложений. Эти меры безопасности защищают среду облачных вычислений от внешних и внутренних угроз и уязвимостей кибербезопасности.

39

В то время как предприятия ускоряют инициативы по цифровой трансформации (DX), энергично переделывают операции и переосмысливают все бизнес-модели с помощью облачных сервисов, такое широкое внедрение также создает новые возможности для совершения кибермошенничества киберпреступниками. Поскольку эти организации переходят к цифровой трансформации своей деятельности очень быстро, думать об эффективных средствах контроля безопасности часто не остается времени. Часто предприятия отказываются от применения проверенных практических рекомендаций, что затрудняет (или даже делает невозможным) точную оценку рисков и управление ими. По мере того как предприятия адаптируются к постоянным изменениям и активно переходят на облачные технологии, возникает потребность объединения разрозненных взглядов и программ действий в целостную стратегию. Организациям, которые рассматривают переход к облаку как возможность активно культивировать стратегию «безопасность превыше всего», придется балансировать между обеспечением возможности использования облачных сервисов и защитой конфиденциальных транзакций и данных.

Что такое облачные вычисления?

- В традиционной среде данных организация владеет и управляет собственным серверным оборудованием и другой инфраструктурой либо на месте, либо в центре обработки данных (называемым «частным облаком»). Это означает, что организация несет ответственность за настройку, обслуживание и обеспечение безопасности всего, включая серверы и другое оборудование.
- В среде облачных вычислений организация фактически «арендует» облачную инфраструктуру у поставщика облачных услуг. Поставщик облачных услуг владеет и управляет центром обработки данных, всеми серверами и другим оборудованием, а также всей базовой инфраструктурой, такой как подводные кабели. Это освобождает организацию от необходимости поддерживать и защищать облачную инфраструктуру и предоставляет множество других преимуществ, таких как простая масштабируемость и модели ценообразования с оплатой по мере использования.

- Облачная безопасность основана на так называемой модели долевой ответственности. В этой модели:
- Поставщик облачных услуг отвечает за безопасность облака, то есть за свой физический центр обработки данных, другие активы, такие как подводные кабели, и логическую облачную инфраструктуру.
- Ваша организация несет ответственность за безопасность в облаке, то есть за приложения, системы и данные, которые вы размещаете в облаке.

Приведем аналогию с арендой ячейки камеры хранения. Вы несете ответственность за сохранность вещей в своей ячейки, для чего вы должны запирать ячейку на ключ и хранить этот ключ в безопасном месте. Компания, владеющая камерой хранения, отвечает за безопасность всего комплекса с помощью средств контроля, таких как видеокамеры, достаточное освещение в местах общего пользования и охранники. Поставщик услуги хранения несет ответственность за безопасность всей камеры хранения, но вы несете ответственность за безопасность в своей ячейке.

Как работает облачная безопасность?

- Говорим ли мы о приложении SaaS, развертывании IaaS (общедоступное облако) или платформе для разработчиков PaaS, облачная безопасность в значительной степени основана на управлении идентификацией и доступом (IAM) и предотвращении потери данных (DLP); другими словами, на предотвращении доступа неавторизованных лиц к вашему облачному сервису и вашим данным.
- Применительно к нашему примеру с камерой хранения: если вы оставляете ключ от своей ячейки без присмотра, а кто-то крадет его и использует для доступа к вашей ячейке, то владелец камеры хранения не виноват, а виноваты вы. Точно так же, если вы используете ненадежный, легко угадываемый пароль для защиты своей учетной записи Gmail или консоли администратора GCP, а злоумышленник скомпрометирует его, ответственность за нарушение безопасности несете вы, а не Google.

Помимо предотвращения несанкционированного доступа и кражи данных, облачная безопасность также направлена на предотвращение случайной потери или повреждения данных в результате человеческой ошибки или небрежности, на обеспечение восстановления данных в случае потери данных и соблюдение законов о конфиденциальности пользователей, таких как HIPAA, запрещающий несанкционированный доступ к личным медицинским записям. Облачная безопасность имеет основополагающее значение для реагирования на инциденты безопасности, аварийного восстановления и планирования непрерывности бизнеса

Общераспространенные меры облачной безопасности:

- Элементы управления IAM, такие как управление доступом на основе ролей (RBAC) и доступ с наименьшими привилегиями, что означает, что сотрудники имеют доступ только к тем приложениям и данным, которые им необходимы для выполнения их работы, и не более
- Инструменты защиты от потери данных, которые идентифицируют конфиденциальные данные, классифицируют их, отслеживают их использование и предотвращают неправомерное использование данных, например не позволяют конечным пользователям делиться конфиденциальной информацией за пределами корпоративных бизнес-сетей.
- Шифрование данных как при передаче, так и при хранении
- Безопасная конфигурация и обслуживание системы

Преимущества облачной безопасности

- Использование искусственного интеллекта (AI) и машинного обучения (ML) для автоматической адаптации к угрозам безопасности и их устранения
- Использование автономных возможностей для масштабирования реагирования, нейтрализации рисков и устранения ошибок в сфере безопасности.
- Проактивная защита данных с помощью средств контроля доступа, управление рисками пользователей и обеспечение прозрачности, а также предоставление инструментов для анализа и классификации.
- Применение модели общей ответственности за безопасность в облаке, чтобы со знанием дела принимать меры по обеспечению безопасности на пути между клиентом и поставщиком облачных услуг
- Встраивание функций безопасности в дизайн архитектуры для реализации подхода «безопасность превыше всего»

Какие основные технологии используются для обеспечения облачной безопасности?

- Облачная безопасность предоставляет организациям подход к решению проблем безопасности и обеспечивает соблюдение нормативных требований. Эффективное обеспечение безопасности облака требует наличия нескольких уровней защиты в рамках стека облачных технологий, в который входят следующие:
- **Средства превентивного контроля**, предназначенные для блокировки авторизованного доступа к конфиденциальным системам и данным.
- **Средства детективного контроля**, предназначенные для выявления несанкционированного доступа к системам и данным и их изменений посредством проведения аудита, мониторинга и отчетности.
- **Средства автоматического контроля**, предназначенные для предотвращения, обнаружения и реагирования на обновления безопасности, как регулярные, так и критически важные.
- **Средства административного контроля**, разработанные для контроля за применением политик, стандартов, практик и процедур безопасности.
- Машинное обучение и искусственный интеллект позволяют дополнить портфель систем облачной безопасности технологиями контекстной осведомленности. Облачная безопасность позволяет предприятиям защищать IaaS, PaaS и SaaS, распространяя защиту на сетевой, аппаратный, операционный, прикладной уровни, уровень кристаллов и уровень хранения данных.

Что такое модель общей ответственности за безопасность облака?

- Облачная безопасность облака — это общая ответственность провайдера облака и клиента за безопасность. Модель общей ответственности за безопасность в облаке — это базовая конструкция для управления безопасностью и рисками в облаке, позволяющая разделить обязанности между поставщиком облачных сервисов и абонентом. Четкое понимание модели общей ответственности за безопасность для всех типов облачных сервисов имеет решающее значение для программ облачной безопасности. К сожалению, можно также сказать, что модель общей ответственности за безопасность является одной из наименее понятных концепций безопасности в облаке. На самом деле, если сравнивать с поставщиком облачных услуг (CSP), только 8 % CISO полностью понимают свою роль в обеспечении безопасности SaaS. Проще говоря, модель общей ответственности за безопасность определяет зону ответственности поставщика облачных услуг по обеспечению безопасности и доступности услуги, а также зону ответственности клиента за обеспечение безопасного пользования услугой, где каждому отводятся свои конкретные обязанности.
- Компании должны понимать свои обязанности. Неспособность адекватно защитить данные может привести к серьезным и дорогостоящим последствиям. Многие организации, которые столкнутся с последствиями взлома, могут оказаться не в состоянии покрыть расходы, даже крупные компании могут ощутить последствия для своих финансовых показателей. Смысл модели общей ответственности за безопасность заключается в обеспечении гибкости с помощью встроенных средств защиты, позволяющих быстро развертывать систему. Поэтому организации должны понимать свои обязанности по обеспечению безопасности в облаке: обычно это называют безопасностью «из» облака и безопасностью «в» облаке.

Какие еще требования важны для обеспечения безопасности облачных данных?

- Сегодня предприятиям предлагается широкий спектр средств защиты облачных сред для обеспечения безопасности при переносе рабочих нагрузок и данных в облако. Однако некоторые из этих инструментов поставляются с индивидуальными инструкциями и предлагаются как отдельные услуги. Пользователи и администраторы облачных решений должны знать, как работают сервисы облачной безопасности, как их правильно настроить и как поддерживать развернутые облачные решения. Хотя сегодня нет недостатка в разных системах обеспечения безопасности, их может быть сложно настраивать и можно легко допустить ошибку в одной области. Кроме того, постоянный риск фишинга и вредоносных программ, растущее кибермошенничество и целый ряд неправильно сконфигурированных облачных сервисов оказывают еще большее давление на программы кибербезопасности, которые уже решают так очень сложные задачи. В результате организации сталкиваются с утечкой данных, а это влечет за собой ущерб бренду, затраты на восстановление и штрафы. Ниже приведены несколько важных требований для обеспечения безопасности данных в облаке:
- **Общая ответственность за безопасность и доверие:** доверие имеет первостепенное значение при выборе партнера по облаку, который будет отвечать за свою часть модели общей безопасности. Организации должны четко понимать свои роли и обязанности, а также иметь доступ к независимым сторонним аудитам и аттестациям систем безопасности.
- **Автоматизация и машинное обучение:** облачные угрозы несутся со скоростью автомобиля, а традиционные корпоративные системы безопасности могут анализировать инциденты и реагировать на них со скоростью человека. Современная система безопасности в облачных средах должна автоматизировать обнаружение угроз и реагирование на них. Для сложных угроз требуются новые современные решения безопасности, которые способны прогнозировать, предотвратить, обнаруживать угрозы и реагировать на них с помощью машинного обучения.

- **Эшелонированная защита:** многоуровневая система безопасности по всему технологическому стеку должна включать средства превентивного, детективного и административного контроля за соответствующими людьми, процессами и технологиями для обеспечения безопасности физических центров обработки данных поставщиков облачных услуг.
- **Управление учетными записями:** по мере того как мобильные устройства, приложения и сведения о пользователях используются все шире, учетные записи становятся новым периметром. Важнейшее значение имеет контроль доступа и привилегий в облаке и локальных системах.
- **Прозрачность:** брокер защиты доступа в облако и решение для управления средствами обеспечения безопасности в облаке увеличивают прозрачность и контроль над всей облачной средой организации.
- **Постоянное соответствие требованиям:** соответствие нормативным требованиям является обязательным, но соответствие и безопасность – это не одно и то же. Организации могут нарушить нормативные требования, не нарушая при этом безопасность, например, в результате изменений и ошибок конфигурации. Для компаний очень важно иметь решение по управлению облачными средами, которое предоставляет полные, своевременные и действенные данные, связанные с соблюдением нормативных требований, по всем облачным средам.

- **Безопасность по умолчанию:** поставщик облачных услуг должен активировать средства контроля безопасности по умолчанию, а не требовать от предприятия помнить о том, что их нужно включать. Не все имеют четкое представление о различных средствах управления безопасностью и о том, как они работают вместе для снижения риска и создания полноценной системы безопасности. Например, шифрование данных должно быть включено по умолчанию. В облаках должны применяться согласованные средства контроля и политики защиты данных.
- **Мониторинг и миграция:** для обеспечения безопасности рабочих нагрузок администраторам политик безопасности следует настроить и обеспечить соблюдение политик безопасности для облачных пользователей и секций. Унифицирование представление всех средств контроля облачной безопасности по всем пользователям облака также необходимо для обнаружения ошибок конфигурации ресурсов и небезопасных действий по всем пользователям, что предоставляет администраторам безопасности возможность отслеживать и решать проблемы безопасности облака.
- **Разделение обязанностей и доступ с минимальными привелегиями:** принципы разделения обязанностей и доступа с минимальными привилегиями – это практические рекомендации по безопасности, которые следует применять в облачных средах. Таким образом Вы сможете гарантировать, что отдельные лица не будут обладать чрезмерными административными правами и не смогут получить доступ к конфиденциальным данным без дополнительной авторизации.

Перспективы развития облачной безопасности

- Поскольку внедрение облачных сред продолжает ускоряться как результат приоритетных целей цифровой трансформации, компании должны предвидеть сложности обеспечения безопасности своих облачных сред и уметь разбираться в них. Очень важно выбрать поставщика облачный услуг, который сможет разработать систему безопасности, автоматически встроенную во весь стек облачных технологий (IaaS, PaaS, SaaS). При рассмотрении перспектив развития облачной безопасности необходимо дополнить учитывать следующие моменты:
- **Безопасность облачной инфраструктуры:** защита рабочих нагрузок с применением подхода «безопасность превыше всего», ориентированного на безопасность вычислений, сетей и систем хранения облачной инфраструктуры, начиная с ее архитектуры. Применение основных служб безопасности для обеспечения необходимого уровня безопасности для самых важных бизнес-нагрузок.
- **Облачная безопасность баз данных:** уменьшение риска утечки данных и ускорение соблюдения нормативных требований в облаке. Внедрение решений по обеспечению безопасности баз данных, включающих шифрование, управление ключами, маскирование данных, контроль доступа привилегированных пользователей, мониторинг активности и аудит.
- **Безопасность облачных приложений:** защита критически важных приложений от мошенничества и неправомерного использования абсолютно необходима для защиты важных бизнес-данных Вашей компании. Детальный контроль доступа, прозрачность и мониторинг являются ключевыми компонентами современной многоуровневой обороны.

- **Корпоративная безопасность и конфиденциальность:** защита конфиденциальности, целостности и доступности данных и систем, размещенных в облаке, независимо от выбранного облачного продукта.
- **Передовое обслуживание клиентов:** при переходе к облачным и мультиоблачным средам группам безопасности приходится сталкиваться с растущей поверхностью атаки, перегрузкой предупреждениями и нехваткой навыков обеспечения кибербезопасности. Для решения этих проблем используйте передовые сервисы от поставщика облачных услуг.
- **Управление учетными записями и доступом (IAM):** контролируйте, кто имеет доступ к Вашим данным, какой тип доступа они имеют и к каким конкретным ресурсам, используя защищенные учетные данные, независимо от того, размещены ли они в облаке или локально.

Существуют ли риски, связанные с облачной безопасностью?

Вот некоторые из самых больших проблем и рисков, связанных с облачной безопасностью.

- Облако создает значительно расширенную поверхность атаки без сетевого периметра. Одна из самых больших ошибок, которую совершают организации при переходе на облачное решение, заключается в том, что они думают, что могут просто перенести все свои текущие инструменты и политики безопасности. Хотя многие аспекты облачной безопасности отражают их локальные аналоги, защита облачной среды сильно отличается от защиты локального оборудования, поскольку облако не имеет определенного сетевого периметра.
- В облаке может отсутствовать видимость, особенно в современных очень сложных средах данных. Редко встречаются организации, использующие только одно общедоступное облако. Большинство организаций используют как минимум два общедоступных облака (называемых многооблачной средой) или объединяют общедоступные облака с локальной инфраструктурой (это называется гибридной облачной средой). К сожалению, каждая облачная среда поставляется со своими собственными инструментами мониторинга, что затрудняет ИТ-администраторам и персоналу DevOps получать общую картину того, что происходит в среде данных.

- Расползание рабочей нагрузки — еще одна проблема отсутствия видимости, даже для организаций, использующих только одно общедоступное облако. Виртуальные машины (ВМ) и контейнеры легко создаются, а это означает, что они могут очень быстро распространяться. Неиспользуемые виртуальные машины и контейнеры не только ставят под угрозу безопасность, но и увеличивают выставляемый вам счет за облачные услуги.
- Теневые ИТ или сотрудники, использующие приложения, не проверенные персоналом службы безопасности, являются еще одной проблемой облачных вычислений.
- Компании могут столкнуться с проблемами совместимости с устаревшими системами и программным обеспечением, особенно с устаревшими бизнес-приложениями, которые невозможно заменить или переделать для облака.
- Неправильные настройки облака также вызывают проблемы, такие как непреднамеренная установка общедоступной облачной папки, содержащей конфиденциальные данные.

Рекомендации по обеспечению безопасности облачных вычислений

- Нужно убедиться в том, что вы полностью понимаете модель долевой ответственности и то, за что ваша организация несет ответственность, а за что нет. Это может показаться очевидным, но выяснить, кто за что отвечает, может быть непросто, особенно в гибридных средах.
- Одним из преимуществ облачных вычислений является возможность доступа к ресурсам в любом месте и с любого устройства. Однако с точки зрения безопасности это означает, что нужно защитить больше конечных точек. Инструменты безопасности конечных точек и управления мобильными устройствами позволят вам применять политики доступа и развертывать решения для проверки доступа, брандмауэры, антивирусы, шифрование дисков и другие инструменты безопасности.

Другие передовые практики облачных вычислений включают в себя:

- Шифрование всех данных, которые вы храните или обрабатываете в облаке, как при передаче, так и при хранении.
- Сканирование своей среды на наличие уязвимостей и максимально быстрое исправление обнаруженных ошибок.
- Регулярное резервное копирование данных на случай атак программ-вымогателей или аварии.
- Регистрация и отслеживание всей пользовательской и сетевой активности во всей своей среде данных.
- Очень тщательная настройка параметров своего облака. Хорошее эмпирическое правило заключается в том, что настройки по умолчанию редко когда являются подходящими или оптимальными для вас, так что вам следует их изменить. Максимально используйте настройки и инструменты безопасности своего поставщика облачных услуг и следите за новыми инструментами и улучшениями.
- Внедрение политики безопасности с нулевым доверием в сочетании с сегментацией сети и надежными инструментами управления идентификацией и доступом (IAM), включая доступ на основе ролей, доступ с наименьшими привилегиями, надежные пароли, одобрение устройств и многофакторную аутентификацию (MFA).

Контрольные вопросы

1. Что такое облачные вычисления?
2. Что понимается в облачных вычислений под "облаком"?
3. Что такое центр обработки данных?
4. Каковы элементы концепции облачных вычислений?
5. Каковы особенности информационной технологии "Инфраструктура как сервис" ("IaaS") ?
6. Каковы особенности информационной технологии "Платформа как сервис" ("PaaS") ?
7. Каковы особенности информационной технологии "Программное обеспечение как сервис" ("SaaS») ?
8. Назовите достоинства облачных вычислений
9. Назовите недостатки облачных вычислений
10. Каковы препятствия развитию облачных технологий?
11. Каков принципы организации распределенных вычислений ?
12. Методы обеспечения безопасности облачных вычислений
13. Риски, связанные с облачной безопасностью

Благодарю за внимание!