СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

В настоящее время можно заметить активное развитие одной из концепций сферы информационных технологий, которая имеет название «облачные вычисления». Суть использования данной концепции заключается в том, что пользователю (потребитель облачных вычислений) предоставляется доступ к вычислительным ресурсам провайдера (поставщик облачных вычислений), физически распределённых на многочисленных устройствах, которые в совокупности образуют облако.

Данная технология, безусловно, выгодна для потребителя, так как освобождает его от поддержания работоспособности собственной инфраструктуры.

При использовании технологии облачных вычислений обработка и хранение информации потребителя происходит на серверах провайдера. Исходя из этого можно выделить некоторые проблемы, связанные с информационной безопасностью. Основной проблемой является обеспечение конфиденциальности данных.

Наиболее распространенным и эффективным способом обеспечения конфиденциальности данных является шифрование данных. Проблема заключается в том, что существующие криптографические алгоритмы, не позволяют осуществлять операции с зашифрованными данными. Поэтому, потребителю, для осуществления операций с зашифрованными информацией в облаке, помимо самой зашифрованной информации, необходимо передать и секретный ключ для расшифровки по открытым каналам связи, что значительно повышает возможность компрометации защищаемой информации.

Решение проблемы обеспечения конфиденциальности информации является актуальной, особенно для развития таких бурно развивающихся технологий облачных вычислений.

Объектом исследования является механизм облачных вычислений.

Предметом исследования является безопасность механизма облачных вычислений.

Для достижения цели работы были поставлены следующие задачи:

- изучить концепцию облачных вычислений;
- рассмотреть возможные угрозы безопасности информации при применении облачных технологий;
- рассмотреть существующие способы защиты информации в информационных системах с использованием технологии облачных вычислений;

# 1 Изучение предметной области

## 1.1 Облачные вычисления

Облачные вычисления (Cloud Computing) – это модель предоставления доступа к вычислительным ресурсам, распределённых на многочисленных удаленных устройствах, которые в общей совокупности образуют «облако».

Облако (cloud) – это модель организации инфраструктуры информационной системы, суть которой заключается в конфигурировании информационной системы из совокупности распределенных аппаратных, сетевых и программных ресурсов, находящихся на удаленных дата центрах поставщиков облачных услуг.

Зарождение концепции облачных вычислений произошло в 60-х годах XX века. В это время два американских ученых – Джон Маккарти и Джозеф Ликлайдер высказывали предположения о корпоративном использовании вычислительных ресурсов. Эти предположения уже в те времена отдаленно напоминали то, чем облачные вычисления являются в наше время.

Увеличение вычислительных мощностей, а также повышение пропускной способности сети способствовали активному развитию технологий, в том числе и облачных вычислений. В настоящее время облачные вычисления активно набирают популярность повсюду, крупные IT-компании не отстают от тенденций развития и предлагают свои услуги. Можно выделить некоторые популярные сервисы: Microsoft Azure, Amazon Web Services (AWS), Google Docs.

В современной модели облачных вычислений принято выделять две взаимодействующие стороны: поставщик и потребитель. Под поставщиком подразумевается компания, предоставляющая услуги облачных вычислений, а под потребителем – организация или физическое лицо, которое приобретает эти услуги. На рисунке 1.1 отражена обобщенная модель облачных вычислений.

Средства, которые может предоставлять поставщик можно разделить на три основных типа:

- приложения (Software);
- платформа (Platform);
- инфраструктура (Infrastructure).


Рисунок 1.1 - Обобщенная модель облачных вычислений

### 1.1.1 Модели предоставления облачных услуг

Средства, которые предоставляет поставщик, распространяются как услуги и могут быть использованы вместе и отдельно друг от друга. Исходя из этого можно выделить три основных типа услуг:

- IaaS (Infrastructure-as-a-Service) – инфраструктура как сервис;
- PaaS (Platform-as-a-Service) – платформа как сервис;
- SaaS (Software-as-a-Service – программное обеспечение как сервис).

Рассмотрим указанные выше типы предоставляемых услуг подробней.

IaaS

Данный тип услуги подразумевает предоставление потребителю вычислительной инфраструктуры, которая включает в себя серверы, сетевое оборудование, устройства хранения информации и т.д. Потребители, используя предоставляемую инфраструктуру, могут разворачивать собственные или уже готовые программные решения для достижения определенных задач. Потребитель не имеет возможности влиять на базовую конфигурацию оборудования, но имеет контроль над конфигурацией ПО. Предоставление вычислительной инфраструктуры, как правило, происходит с применением технологии виртуализации.

PaaS

В данном случае потребителю предоставляется возможность использования облачной инфраструктуры для размещения базового программного обеспечения для последующего размещения на нём новых или существующих приложений (собственных, разработанных на заказ или приобретённых тиражируемых приложений). В состав таких платформ входят инструментальные средства создания, тестирования и выполнения прикладного программного обеспечения – системы управления базами данных, связующее программное обеспечение, среды исполнения языков программирования – предоставляемые облачным провайдером.

Потребность в PaaS возникла из-за того, что многие компании используют не стандартный софт (устаревший, специализированный, софт собственной разработки и сделанный под заказ) и им требуются облака, чтобы использовать этот софт внутри компании.

Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем, хранения в случае PaaS осуществляется облачным провайдером, за исключением разработанных или установленных приложений, а также, по возможности, параметров конфигурации среды (платформы).

SaaS

Эта модель доставки программного обеспечения, в которой приложение размещается у провайдера или третьей стороны и становится доступным клиентам по подписке. Клиенты SaaS используют выполняемое в инфраструктуре провайдера ПО на основе оплаты текущих расходов. Вносить предоплату не требуется, поэтому клиент может не заключать какие-либо долгосрочные контракты.

В модели SaaS:

- приложение приспособлено для удаленного использования;
- одним приложением пользуется несколько клиентов (приложение коммунально);
- оплата взимается либо в виде ежемесячной абонентской платы, либо на основе объёма операций;
- техническая поддержка приложения включена в оплату;
- модернизация и обновление приложения происходит оперативно и прозрачно для клиентов.

Данные средства поставщик может предоставить потребителю в качестве услуги (as service) и при необходимости потребителю не обязательно пользоваться услугами только одного поставщика. Разные сервисы могут быть заказаны у нескольких разных поставщиков и настроены на совместное взаимодействие в интересах потребителя, так как потребителю предоставляются возможности контроля и администрирования.

### 1.1.2 Область видимости облачных сервисов

Диапазон применения облаков достаточно велик. Они могут быть использованы как для банального хранения файлов, так и для организации сложнейших вычислений при использовании кластеров. Выбор облака

зависит, также, от аудитории, которой будут видны облачные сервисы: будь то сотрудники организации или же целое интернет-комьюнити.

По области видимости можно выделить несколько классов облачных сервисов:

- private cloud (частное облако). Это модель IT-инфраструктуры, как правило, одного предприятия, при которой приложения и информационные ресурсы распространяются как сервисы. Пользователями такой инфраструктуры является ограниченный круг лиц (сотрудники предприятия). Доступ к такому облаку должен осуществляться только внутри локальной сети предприятия, а также при использовании технологий VPN при территориальной раздельности частей предприятия;
- community cloud (облако для сообщества). Это вид IT-инфраструктуры, предназначенный для использования участниками того или иного сообщества, имеющих общие задачи. При этом сообщество связано с потребителем определенными соглашениями;
- public cloud (публичное облако). Данный вид инфраструктуры предназначен для свободного использования широкой аудиторией. Пользователем данного облака может стать любое лицо, которое имеет возможность сетевого доступа к сервисам облака;
- hybrid cloud (гибридное облако). Данные облака могут быть как сочетанием нескольких типов облаков, приведенных выше (private, public, community), так и сочетанием разных услуг (IaaS, PaaS, SaaS) от одного или разных поставщиков услуг. Сервисы, представленные в данном облаке, могут иметь различную область видимости;
- intercloud. Это инфраструктура, отличительной особенностью которой является то, что она состоит из нескольких, взаимодействующих между собой облаков. Данные облака взаимодействуют между собой посредством сети Интернет.

Исходя из информации, рассмотренной выше можно выделит следующие преимущества облачных вычислений:

- доступность (получение доступа к облачным сервисам можно осуществить из любого места, при этом, необходимо минимальное количество установленного ПО);
- гибкость (можно легко указывать требуемый объем вычислительных ресурсов, которые необходимы потребителю);
- низкая стоимость вычислительных ресурсов, относительно поддержки равной по мощности реальной инфраструктурой;
- надежность (в основном облачные сервисы предлагают крупные компании, которые обеспечивают сохранность пользовательских данных многочисленными способами, например, резервированием).

Также, существуют и некоторые недостатки:

- для получения доступа к облачным сервисам необходимо постоянное подключение к сети Интернет;
- потребитель может выбирать только то программное обеспечение, которое установлено на серверах поставщика облачных услуг;
- несмотря на существующие технологии защиты информации, нет таких облачных сервисов, которые гарантировали бы полную конфиденциальность информации, располагаемой на серверах.

Тем не менее, концепция облачных вычислений подвергалась критике. Из-за того, что обслуживанием серверов занимается третья сторона, появляется целый класс новых проблем, связанных с информационной безопасностью. Наиболее серьезной из них является проблема конфиденциальности данных. Поскольку парк серверов, на которых работает облачный сервис, находится на территории провайдера, организация-потребитель, которая размещает свои данные в облаке, не может контролировать физический доступ к ним. Ситуация осложняется тем, что законодательством многих стран предписываются жесткие требования к

уровню защиты данных определенного класса информации, которые трудно или невозможно обеспечить в случае, когда данные хранятся в облаке.

## 1.2 Безопасность информации в облачных вычислениях

### 1.2.1 Угрозы безопасности информации в облачной информационной системе

Информационные системы, построенные на основе технологии облачных вычислений, в связи с некоторыми особенностями данной технологии, подвержены ряду угроз информационной безопасности. Далее рассмотрим данные особенности подробней, для того чтобы определить основные источники угроз информационной безопасности.

Использование средств виртуализации

Для систем облачных вычислений характерно использование различных технологий виртуализации. Применение данных технологий позволяет обеспечить динамическую масштабируемость вычислительных ресурсов. Также виртуализация позволяет обеспечить возможность самообслуживания потребителей, например, в большинстве облачных сервисов для развертывания виртуальной машины для определенных задач, достаточно совершить пару кликов, как правило, в web-интерфейсе, и через некоторое время пользователю предоставляется, готовая к работе, виртуальная машина.

Уязвимости средств виртуализации бывают нескольких типов:

а) уязвимости, связанные с воздействием на гипервизор:
   1) нарушение работы гипервизора;
   2) нарушение работы виртуальной машины;
   3) DOS-атака на гипервизор;

б) уязвимости, связанные с выходом процесса за пределы виртуальной машины:

1) нарушение изоляции виртуальной машины;
2) внедрение кода в другие виртуальные машины;
3) внедрение кода в гипервизор;
4) запись и чтение данных с устройств, с которыми работает гипервизор;

в) уязвимости, связанные с воздействием на гостевую ОС:
1) нарушение работы гостевой ОС;
2) внедрение кода в гостевую ОС;
3) модификация памяти ОС при миграции виртуальной машины;

г) прочие уязвимости:
1) нарушение работы средств управления средств виртуализации;
2) нарушение работы вспомогательных программ;
3) кража виртуальной машины пользователя.

На рисунке 1.2 представлена краткая схема уязвимостей средств виртуализации.

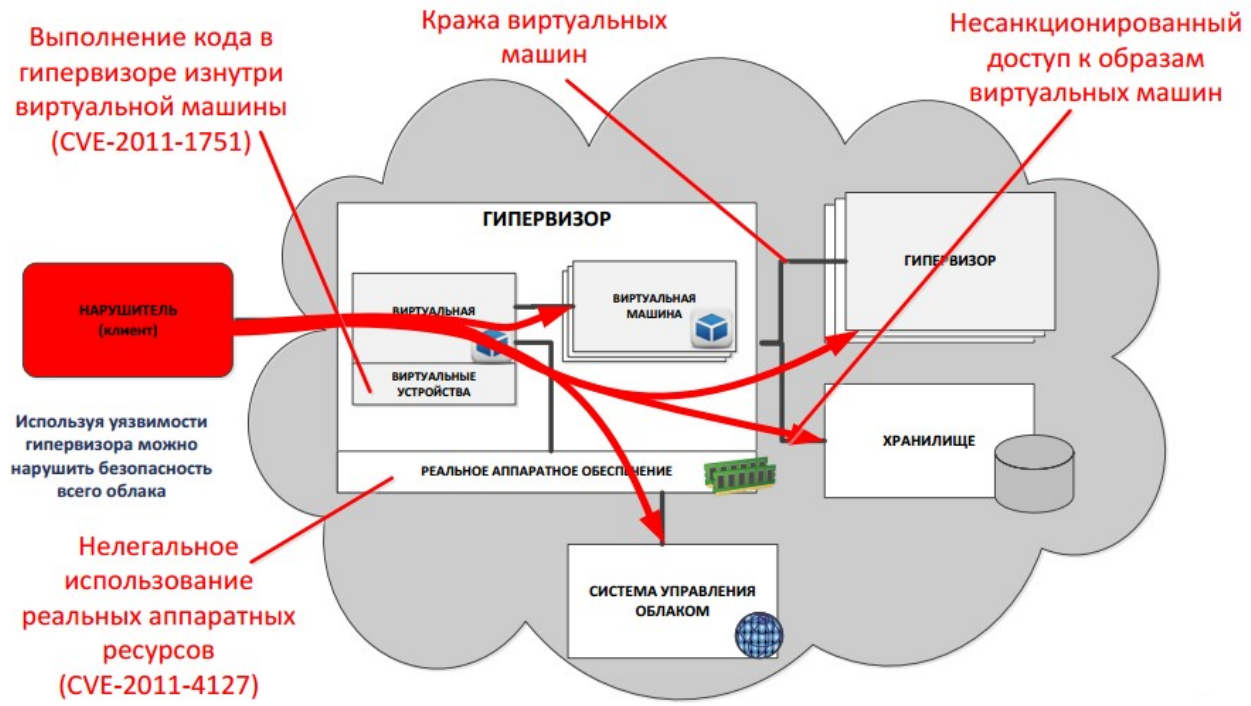


Рисунок 1.2 - Краткая схема уязвимостей средств виртуализации

Сбои в работе средств виртуализации могут негативно повлиять на всю облачную инфраструктуру в целом. Например, потеря обрабатываемой информации может негативно повлиять на доверие клиента сервису, а нарушение изоляции может привести к несанкционированному доступу к вычислительным ресурсам и данным.

Доступ к информационным сервисам по каналам информационно-телекоммуникационных сетей

Использование глобальных сетей передачи данных (Интернет) для обеспечения доступности облачных сервисов значительно увеличивает разнообразие угроз на данную информационную систему. В качестве примера можно привести атаки типа DDoS, MitM и другие. Также следует рассмотреть возможность проведения атаки со стороны оператора связи. Оператор связи предоставляет услуги подключения между провайдером и потребителем. Оператор связи оказывает непосредственное влияние на доступность облачных сервисов со стороны клиента и защиту передаваемых данных. Так как оператор имеет возможность получить доступ ко всей передаваемой информации, недобросовестные действия персонала оператора, могут привести к компрометации передаваемой информации.

Модель предоставления информационных сервисов

Для поддержания аппаратной инфраструктуры облачных сервисов провайдер нанимает определенный персонал. Персонал не является представителем потребителя облачных услуг, следовательно, он находится вне зоны его контроля. Персонал имеет физический доступ к ресурсам облачных сервисов провайдера. Учитывая большую степень консолидации вычислительных ресурсов, данная возможность значительно расширяет количество угроз информационной безопасности со стороны персонала провайдера. Причем данные угрозы могут быть осуществлены не только с

использованием физического доступа, но, также, с использованием определённого программного обеспечения.

После рассмотрения особенностей информационной системы, построенной на технологии облачных вычислений, и после анализа дополнительной информации, можно определить основные источники информационной безопасности в системах облачных вычислений.

Источники угроз:

- технические средства и технологии, сбои в работе которых могут привести к появлению возможности реализации угроз информационной безопасности (технические средства обработки информации, ПО, система электропитания и т.п.);
- средства виртуализации;
- природные явления, стихийные бедствия;
- пользователи информационно-телекоммуникационных сетей (пользователь может реализовать угрозу, используя глобальные сети обмена данными);
- оператор связи (реализация угрозы доступности сервисов, а также перехват передаваемой информации);
- персонал провайдера (ошибочные действия персонала);
- недобросовестный персонал провайдера (намеренные действия по реализации угрозы информационной безопасности);
- потребители системы облачных вычислений (ошибочные действия, несоблюдение требований по защите информации при работе с системой облачных вычислений);
- недобросовестные потребители систем облачных вычислений (намеренные действия по реализации угрозы информационной безопасности).

### 1.2.2 Меры и механизмы защиты облачной информационной системы

В связи с особенностями архитектуры информационной системы, построенной с использованием технологий облачных вычислений, возникает множество угроз информационной безопасности, которые были рассмотрены ранее. Для того чтобы полностью защитить информационную систему от возможных атак, необходимо проделать большую работу по улучшению ИС.

Рассмотрим подробней пять наиболее популярных методов обеспечения безопасности в облачных сервисах.

Сохранность данных. Шифрование

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

Шифрование является одним из самых надежных методов защиты данных. Провайдер облачных услуг, который предоставляет доступ к некоторым услугам, должен шифровать информацию, которая хранится в ЦОД (Центр обработки данных).

Для того, чтобы полностью реализовать весь потенциал шифрования, недостаточно простого введения в систему механизмов шифрования данных. Также необходимо грамотно организовать одну из важнейших процедур – процедуру управления ключами.

Управление ключами состоит из процедур, обеспечивающих:

- включение пользователей в систему;
- выработку, распределение и введение в аппаратуру ключей;
- контроль использования ключей;
- смену и уничтожение ключей;
- архивирование, хранение и восстановление ключей.

Управление ключами преследует цели, связанные с нейтрализацией угроз, связанных с ключами шифрования. Данные угрозы представлены на рисунке 1.3.


Рисунок 1.3 – Угрозы, связанные с ключами шифрования

Для обеспечения конфиденциальности ключей рекомендуется использовать разделение ключей по уровням. При использовании такой системы существуют три уровня ключей шифрования: главный ключ – данный ключ не защищается криптографически, защита ключа происходит посредством физических или электронных средств; ключ для шифрования ключей – данный ключ предназначен для шифрования других ключей при процедуре обмена ключами, эти ключи могут быть также зашифрованы другими ключами; ключи для шифрования данных – ключи, которые используются для защиты данных пользователя.

Одной из важных характеристик системы управления ключами являются сроки действия ключей. Срок действия ключа означает промежуток времени, в течение которого он может быть использован доверенными сторонами.

Сокращение сроков действия ключей необходимо для достижения следующих целей:

- ограничения объёма информации, зашифрованной на данном ключе, которая может быть использована для криптоанализа;
- ограничения размера ущерба при компрометации ключей;

- ограничения объёма машинного времени, которое может быть использовано для криптоанализа.

В дополнение к указанной выше классификации ключей по уровням, может быть введена также следующая классификация:

- ключи с длительным сроком действия. К ним относится главный ключ, часто – ключи для шифрования ключей;
- ключи с коротким сроком действия. К ним относятся ключи для шифрования данных.

Как правило, в телекоммуникационных приложениях используются ключи с коротким сроком действия, а для защиты хранимых данных – с длительным сроком действия. Процедура управления ключами должна проходить на специализированном сервере – сервере управления ключами (Key Management Server, KMS). На рисунке 1.4 показан пример взаимодействия пользователя, сервера управления ключами и облачного сервера. Помимо факторов, связанных с правильной конфигурацией сервера обмена ключами, также следует учитывать расположение данного сервера.

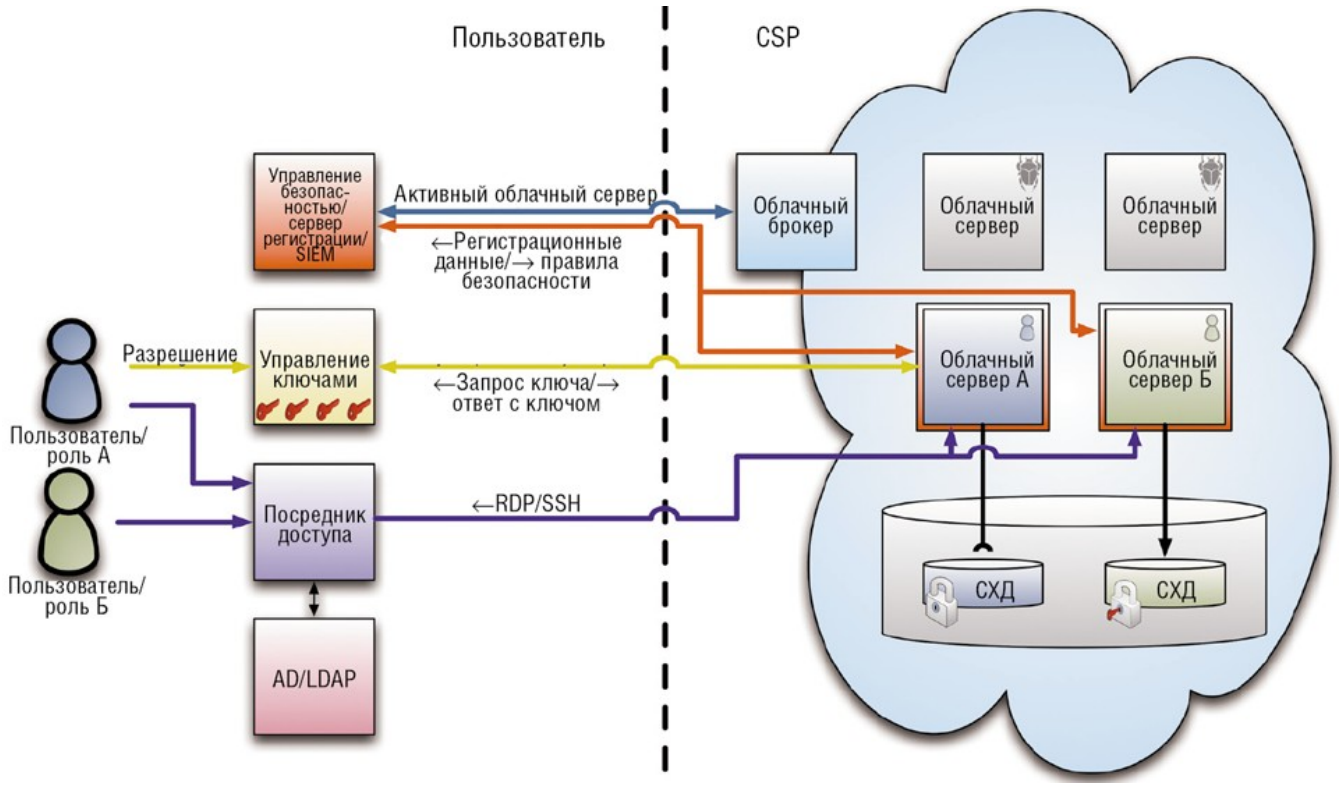


Рисунок 1.4 − Взаимодействие пользователя, сервера управления ключами и облачного сервера

Раздельное использование сервера управления ключами и облачного сервера в разы повысит безопасность ключей, которые хранит KMS, так как у сотрудников облачного сервиса не будет одновременного доступа и к данным пользователей, и к ключам шифрования данных. Но при одновременном размещении облачных серверов и KMS в инфраструктуре одного провайдера тоже может вызывать подозрение о возможной компрометации пользовательской информации. В таком случае можно использовать сервер KMS в качестве внешней услуги у другого доверенного провайдера.

Защита данных при передаче

Передача данных от пользователя поставщику является важнейшей частью архитектуры облачных вычислений. Очень важно обеспечить безопасность передаваемых данных. Для того чтобы решить данную

проблему, можно воспользоваться распространенным решением в данном вопросе – использование протоколов SSL/TLS.

TLS (англ. Transport Layer Security – безопасность транспортного уровня) и SSL (англ. Secure Sockets Layer – уровень защищённых сокетов) – это криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Цифровой сертификат шифрования – это документ, который содержит открытый ключ шифрования, а также некоторый набор атрибутов, принадлежащий владельцу ключа.

Для того чтобы установить безопасное соединение между клиентом и сервером, клиент и сервер должны быть уверены в достоверности использования открытых ключей. Так как прямой безопасный обмен сертификатами не всегда возможен, для проверки достоверности необходимо использовать услуги удостоверяющих центров (УЦ, или CA – Certificate Authority). На рисунке 1.5 представлена схема установки SSL-сессии с использованием УЦ.

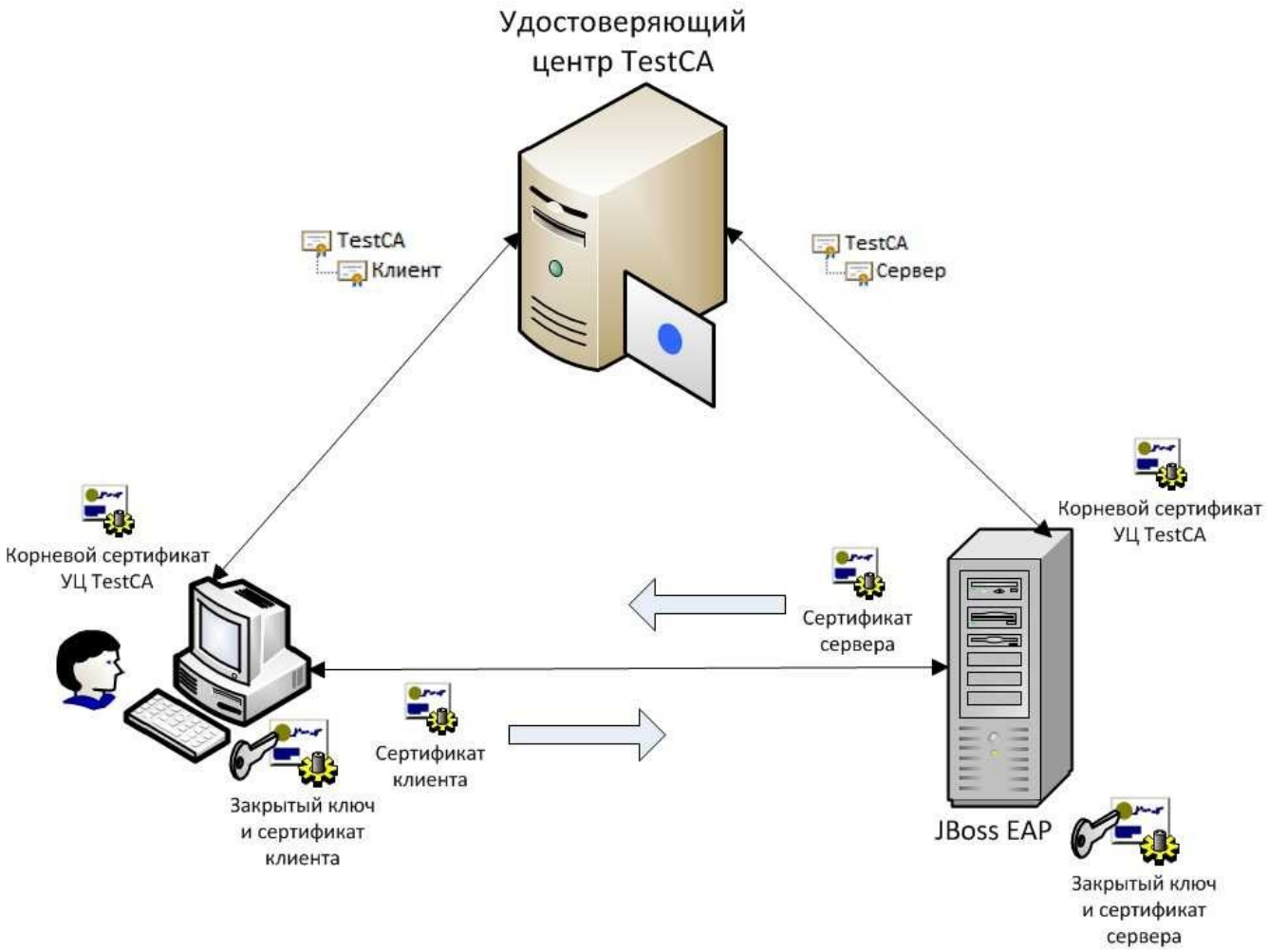


Рисунок 1.5 − Схема установки SSL-сессии с использованием УЦ

Система, которая обеспечивает проверку достоверности сертификатов, называют инфраструктурой открытых ключей (PKI, Public Key Infrastructure). PKI включает в себя все необходимое для выпуска, управления, распространения, проверки достоверности и отзыва цифровых сертификатов.

Для того чтобы использовать цифровые сертификаты каждый участник сессии должен иметь свое локальное хранилище сертификатов (CS, Certificate store), в котором находятся все доверенные сертификаты. Также в этом хранилище располагаются сертификаты данной системы, которые по требованию могут быть предъявлены при установке сетевых соединений. При использовании PKI в хранилище также добавляются сертификаты

центров сертификации, которым доверяет данная система. Такие сертификаты называются корневыми (RC, Root Certificate).

Одним из проверяемых параметров при просмотре сертификата является срок его действия. Следует отметить, что при проверке срока действия используется текущая системная дата и время. Неправильная установка системного времени может служить причиной сбоя в установке защищенного соединения.

Далее рассмотрим использование протоколов SSL/TLS для шифрования передаваемых данных. Шифрование передаваемых данных обеспечивает защиту от прослушивания сетевых соединений и атак типа man-in-the-middle, при которых злоумышленник внедряется в цепочку сетевого соединения в качестве одного из промежуточных узлов.

Очевидно, что для защиты от перечисленных угроз достаточно проверить достоверность сертификата только с одной стороны, после чего ключ шифрования сессии может быть передан безопасным способом.

В этой связи при использовании SSL/TLS в системах облачных вычислений чаще всего ограничиваются проверкой сертификата сервера, что упрощает администрирование и снижает эксплуатационные издержки клиентов, поскольку системы клиент-сервер подразумевают незначительное количество серверов, обслуживающих значительное количество клиентов.

Основным программным обеспечением пользователя систем облачных вычислений является web-браузер. Все популярные на сегодняшний день web-браузеры поддерживают протокол HTTPS (HTTP Secured). Сам по себе протокол HTTPS не является самостоятельным протоколом, а представляет собой режим использования SSL/TLS протоколов для шифрования HTTP-соединения, установленного по протоколу TCP.

Аутентификация

Аутентификацией называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его

подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Для обеспечения более высокой надежности, часто прибегают к таким средствам, как токены (электронный ключ для доступа к чему-либо) и сертификаты. Наиболее простой и достаточно надежный метод аутентификации – это технология одноразовых паролей (One Time password, OTP). Такие пароли могут генерироваться либо специальными программами, либо дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS. Основное отличие облачной инфраструктуры заключается в большой масштабируемости и более широкой географической распределенности. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов, которые сегодня есть практически у каждого. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на страницу доступа к облачному сервису.

Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и язык программирования SAML (Security Assertion Markup Language).

Изоляция пользователей

Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service). Часто провайдеры изолируют данные пользователей друг от друга за счет изменения кода в единой программной среде. Этот подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющем получить доступ к данным. В

случае возможной ошибки в коде пользователь может получить доступ к информации другого пользователя.

Системы обнаружения вторжений и контроль действий пользователя

Защита сети часто включает в свой состав системы обнаружения вторжений из сети (network intrusion detection systems, NIDS), которые осуществляют мониторинг локального трафика с целью выявления всего, что выглядит нестандартным или просто необычным. В качестве примеров нестандартного трафика можно привести:

- попытки сканирования портов (Port scans);
- атаки по типу Denial-of-Service (DoS-атаки);
- попытки использования эксплойтов, эксплуатирующих известные уязвимости.

Обнаружение сетевых вторжений осуществляется либо путем маршрутизации всего трафика через систему, выполняющую его анализ, либо же путем пассивного мониторинга трафика с одного из компьютеров в вашей локальной сети.

Сетевые системы обнаружения вторжений предназначены для того, чтобы предупредить о возможности атак до их начала и, в некоторых случаях, для отражения уже начавшихся атак.

Таким образом, системы обнаружения вторжений позволяют предотвратить атаки, даже те, которые еще находятся на стадии подготовки.

Ознакомившись подробней с технологией облачных вычислений, можно сделать вывод о том, что проблема конфиденциальности информации является, действительно, актуальной на данный момент.

Использование некоторых особенностей технологии облачных вычислений (например, использование средств виртуализации или взаимодействие с клиентом по общедоступным сетям) значительно расширяет спектр атак на облачную инфраструктуру. В такой ситуации наиболее важно обеспечить безопасность информации.

Не смотря на большое количество методов защиты информации, ни один провайдер облачных услуг не может гарантировать абсолютную защиту информации, расположенной на удаленных серверах.

Изучив возможные методы защиты облачной инфраструктуры можно сделать вывод, что единственным эффективным решением проблемы конфиденциальности данных, доступным на данный момент, является шифрование данных, находящихся в облаке. Однако криптографические системы, которые используются в настоящее время, не позволяют осуществлять различные действия без дешифрования информации. В результате, данные приходится расшифровывать, что оставляет только следующие сценарии использования облаков:

- облако хранит зашифрованную информацию. Для доступа к ней данные скачиваются на доверенный компьютер, после чего расшифровываются и обрабатываются. Подобный подход может быть оправдан только в случае, когда необходимо хранить большой объем редко используемой информации, так как для любых манипуляций с ней необходимо их скачать через глобальную сеть, а затем расшифровывать, что значительно ниже скорости доступа к локальному хранилищу;
- облако также хранит зашифрованную информацию, но для её обработки часть данных расшифровывается, а затем зашифровывается прямо на облаке. У такого подхода сразу два недостатка: ключ, которым происходит шифрование, попадает в облако и может быть перехвачен злоумышленником; расшифрованные данные во время обработки находятся в облаке в открытом виде и так же могут быть перехвачены. Таким образом, весь смысл шифрования теряется, особенно в случае частого обращения к данным.

# ЗАКЛЮЧЕНИЕ

На сегодняшний день наибольшее количество пользователей сети Интернет используют технологии облачных вычислений. Данная технология очень сильно прижилась в повседневной жизни людей настолько, что представить взаимодействие в сети без использования этой технологии практически невозможно. Большой интерес к данной технологии порождает огромное количество информации, которое должны обрабатывать облачные провайдера и, конечно же, защищать эту информацию.

В процессе исследования были рассмотрены основные понятия облачных вычислений (модели предоставления облачных услуг, области видимости облачных сервисов), а также механизмы защиты информации, которые применяются в настоящее время при организации облачной инфраструктуры.

# СПИСОК ЛИТЕРАТУРЫ


1. Анисимов, В. В. Проектирование информационных систем: курс лекций : в 2 ч. / В. В. Анисимов. – Хабаровск: Изд-во ДВГУПС, 2007. – Ч. 2; Объектно-ориентированный подход. – 2007. – 100 с.
2. Баранова Е., Бабаш А. – Информационная безопасность и защита. Инфра – М. 2017 – 324 с.
3. Богданов, В. В. Актуальность обеспечения информационной безопасности в системах облачных вычислений, анализ источников угроз / В. В. Богданов, Ю. С. Новоселова. // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1. – С. 78-82.
4. Бостром Н. – Искусственный интеллект Этапы. Угрозы. Стратегии– М.: Издательство « МИФ», 2016 – 760 с.
5. Брэгг, Роберта Безопасность сетей. Полное руководство // Р. Брэгг, М. Родс-Оусли, К. Страссберг; пер. с англ. – М.: Издательство «Эконом», 2018. – 912 с.
6. Волков С.Д. Обзор подходов к построению систем обнаружения компьютерных атак для информационнотелекоммуникационных систем, функционирующих на основе технологии облачных вычислений // Collegium Linguisticum - 2017. Материалы ежегодной конференции студенческого научного общества МГЛУ. 2017. М.: ФГБОУ ВО МГЛУ. С. 442-447.
7. Волков С.Д., Царегородцев А.В. Один из подходов к обеспечению защиты от компьютерных атак при реализации информационной функции государства на внутреннем уровне // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2020. № 36. С. 159-174.

8. Глеске Д.О. Понятие аудита информационной безопасности. / Вестник научных конференций. 2020. №11-4(63). Наука, образование, общество: по материалам международной научно-практической конференции 30 ноября 2020 г. Часть 4. – С. 26-27
9. Глеске Д.О. Программное обеспечение, предусматривающее полный анализ рисков. / Вестник научных конференций. 2020. №11-4(63). Наука, образование, общество: по материалам международной научно- практической конференции 30 ноября 2020 г. Часть 4. – С. 27-28
10. Гребнев Е. Облачные сервисы. Взгляд из России – М.: CNews, 2018. – 282с.
11. Кан К.А. –Нейронные сети. Эволюция – М.: Издательство «ЛитРес» , 2018. – 380 с.
12. Клейнбер Д. – Алгоритмы. Разработка и применение – М.: Издательство «Питер», 2016 – 800 с.
13. Маркелов А. А. - OpenStack. Практическое знакомство с облачной операционной системой – М.: Издательство «ДМК-Пресс, 2.», 2018. – 306 с.
14. Миронова, А.О., Применение методики оценки угроз безопасности информации / А.О. Миронова, Ю.Ю. Гончаренко, А.С. Гоголь, А.Н. Фролова // Энергетические установки и технологии. -2021. - Т. 7. № 4. - С. 71-75.
15. Нестеренко В.Р., Маслова М.А. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними // Научный результат. Информационные технологии. - Т.6, №1, 2021. - С. 48-54.
16. Николенко С – Самообучающиеся системы – М.: Издательство «МЦНМО» , 2015. – 289 с.

17. Ожиганова, М.И. Методы и средства проведения анализа угроз локальной вычислительной сети предприятия / М.И. Ожиганова, А.О. Шейко, Е.М. Исакова, А.О. Миронова // в сборнике: цифровая трансформация науки и образования. Сборник научных трудов II Международной научно-практической конференции. 2021. С. 264-270.
18. Риз, Дж. Облачные вычисления / Дж. Риз ; Пер. с англ. – СПб.: БХВ-Петербург, 2011. – 288 с.
19. Тесленко, И. М. Производственное освещение: учеб. пособие / И. М. Тесленко. – Хабаровск: Изд-во ДВГУПС, 2014. – 103 с.