# УГРОЗЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ И МЕТОДЫ ИХ ЗАЩИТЫ

**Арзамасов Евгений Владимирович**

студент, Воронежский государственный университет инженерных технологий, РФ, г. Воронеж

**Чурикова Анастасия Алексеевна**

студент, Воронежский государственный университет инженерных технологий, РФ, г. Воронеж

**Денисенко Владимир Владимирович**

научный руководитель, старший преподаватель, Воронежский государственный университет инженерных технологий, РФ, г. Воронеж

Для начала следует разобраться, что же такое центр обработки данных и зачем он нужен (ЦОД) - это отказоустойчивая сопряженная централизованная система, которая обеспечивает автоматизирование бизнес-процессов с большим уровнем продуктивности и качеством выделяемых сервисов.

Проще говоря, ЦОД- это несколько серверов, которые размещаются на общей площадке с целью увеличения защиты и результативности работы. Защита центра обработки данных – это предоставление сетевой физической защиты, подача электричества, отказоустойчивость.

В наши дни существует множество вариантов охраны серверов ЦОД от множества разных угроз. Всех их соединяет то, что они все направлены на небольшой круг решаемых задач.

Несмотря на это, с приходом новых виртуальных платформ спектр задач расширился. К главным видам угроз, таким как: атака сети, вредоносное ПО, небезупречные операционные системы, прибавились трудности с контролированием среды, трафика между гостевыми машинами и различными границами прав доступа.

Для множества отраслей работа ЦОД нуждается в закрытии тех. проблем и решении ряда вопросов, которые касаются безопасности. Для финансовых институтов, таких как банки, у которых есть свои стандарты, и выполнения которых лежит на тех. составляющей. Количество таких компаний, в которых платформы виртуализации проникают все глубже, плотно задумались над вопросами их безопасности. С каждым днем все тяжелее и тяжелее становится создать защиту необходимых для бизнеса программ [1].

Из-за виртуализации многие системы перешли на виртуальные машины, и в связи с этим встает задача о безопасности этих систем. Для большинства угроз безопасности систем уже разработали защиту, но также их необходимо приспособить для того, чтобы использовать в облаке.

## Рассмотрим основные виды угроз:

1. Динамика виртуальных машин.

Виртуальные машины по сути динамичны. В любой момент  имеется возможность ввести в использование новейшую машину, прекратить работу машины или возобновить. Виртуальные машины очень легко клонируются и также легко могут быть перемещены из одного физ.

сервера в другой. Такие изменения делают сложным создание единой системы безопасности, так как обычная модель подразумевает четкую устойчивость ИТ- инфраструктуры. Уязвимые места в ОС или приложений в виртуальных средах могут распространяться свободно, которые будут видны после некоторого момента времени. Следовательно, встает вопрос о необходимости безошибочно зафиксировать защитное состояние системы, в независимости от места.

2. Уязвимые места изнутри виртуальной среды.

Локальные серверы и серверы расчета в облаке пользуются одними и теми же утилитами и ОС. У облачных систем высокий уровень угрозы удаленного хакинга, а также заражением вирусами. Не менее большой риск и для виртуальных систем. Так называемые параллельные виртуальные машины повышают площадь заражения ПО. В идеале, система поиска вирусов и система фиксирования вмешательства на сервер должна обнаруживать такую активность на уровне виртуальных машин, независимо от того, где эти машины находятся в облаке.

3. Сложности во время переноса серверов в вычис-ое облако

Условия к защищенности облачных вычислений никак не различаются с условий защищенности к центрам обрабатывания данных. Но процесс создания программного представления центра обработки данных и переключение к облаку может послужить причиной возникновения опасностей. Допуск посредством Сети интернет к регулированию вычислит. мощностью – самая главная характеристика облачных вычислений. В основной массе классических центров обработки данных, допуск инженеров к серверам проверяется на физ. уровне, в облачных окружениях они работают посредством Сети интернет. Разделение контролирования допуска и обеспечение прозрачности модификаций на системном уровне считаются одними из важнейших критериев защиты.

4. Защита границ и разделение сети.

Во время использования облачных вычислений граница сети становится расплывчатой либо пропадает вовсе. Как следствие, охрана наиболее незащищенной части сети устанавливает единую степень безопасности. Для разобщения участков с различными степенями доверенности в облаке виртуальным машинам необходимо снабжать себя защитой, транспортировать сетевую границу к самой виртуальной машине (Рисун. 1). Корпоративный firewal – главный элемент для введения IT-защиты и безопасности и разделения частей сети – не способен оказать действие на серверы, которые располагаются в облаке.

5. Защита “спящих” (находящиеся без действия) виртуальных машин

Если виртуальная машина бездействует, то она становится жертвой инфицирования вирусами. Допуска к хранилищу образов виртуальных машин посредством сети вполне хватает. В неработающей виртуальной машине совершенно нельзя привести в действие защитное ПО. В этом случае обязана быть выполнена охрана изнутри всех виртуальных машин, а также охрана на уровне гипервизора [3].


***Рис. 1. Представление работы конструкции разделения доступа***

**Атаки на облака и варианты решения для их предотвращения**

• Обычные  атаки на программное обеспечение

Уязвимые места в операционных системах, различных модулях, протоколов сети — стандартные (типичные) угрозы, от которых можно защититься установкой брандмауэра, файервола(firewal), антивирусного ПО, или других компонентов, которые решают текущую задачу.

При этом немаловажно, чтобы эти ресурсы защиты результативно функционировали в условиях виртуализации.

• DDoS налеты на пользователя

Большая часть юзеров подсоединяются к облаку, применяя интернет-браузер.В следствие чего , хаккеры пользуются такими виды атаки на пользователей, как Cros Site Scripting, похищение паролей, перехватывание сессий в беспроводных сетях, «атака посредника » и большое изобилие различных атак.

Существует один способ защиты от атак таких типов: верная аутентификация и применение специального соединения (SSL) с двухсторонней аутентификацией. Опять-таки, перечисленные способы защиты не совсем пригодны и являются далеко неэкономичным для разработчиков облаков. И поэтому, в текущей области ИТ безопасности существует много задач, которые необходимо решить.

• Функциональные атаки на части облака

Функциональные атаки соединены с многослойностью облака, совместным правилом безопасности.

В заметке об угрозе облаков было представлено соответствующее разрешение:

С целью обороны от многофункциональных атак с целью любой составляющей облака следует применять последующие ресурсы защиты: для прокси-серверов – успешную защиту от DoS-атак, для интернет-сервера — контролирование цельности страниц, для сервера приложений — дисплей уровня приложений, для СУБД — охрану от SQL-внедрений, для системы сохранения сведений – верные backup (дополнительное дублирование), разделение допуска.

В раздельности любые из этих защитных элементов сейчас сформированы, однако они никак не сосредоточены совместно с целью цельной защиты облака.  По этой причине, проблему введения их в совместную конструкцию требуется регулировать в промежуток формирования облака.

· Атаки на системы управления

Для большинства машин, которые используются в облаке, необходим такой компонент, как система управления,  которая может следить за изготовлением, переносом и переработкой (утиль) виртуальных машин.

Вмешательство со стороны в такую систему  послужит причиной выхода виртуальных машин, так называемых “машины-невидимки”, которые способны заблокировать или же подставлять другие виртуальные машины.

# Способы защиты облачных вычислений.

1. Шифрование данных.

Шифрование – это один самых надежных способов для  защиты информации в облаке. Провайдер, который предоставляет данные, обязан шифровать инф-ию пользователя. Информация  находится в ЦОД, а если нет необходимости предоставлять ее, то нужно удалять ее. Таким образом, облако всегда имеет дело только с зашифрованным контентом. Выделим плюсы шифрования данных:

· Владелец облака не сможет получить доступ к файлам пользователя.

· Никакой элемент на пути следования трафика не получит доступ к данным пользователя. К примеру:  владелец wi-fi точки какого-либо заведения.

Главным условием с целью предоставления защищенности подобного решения считается

отдельное использование облачного сервера и сервера управления ключами (см. Рис 2) [4].

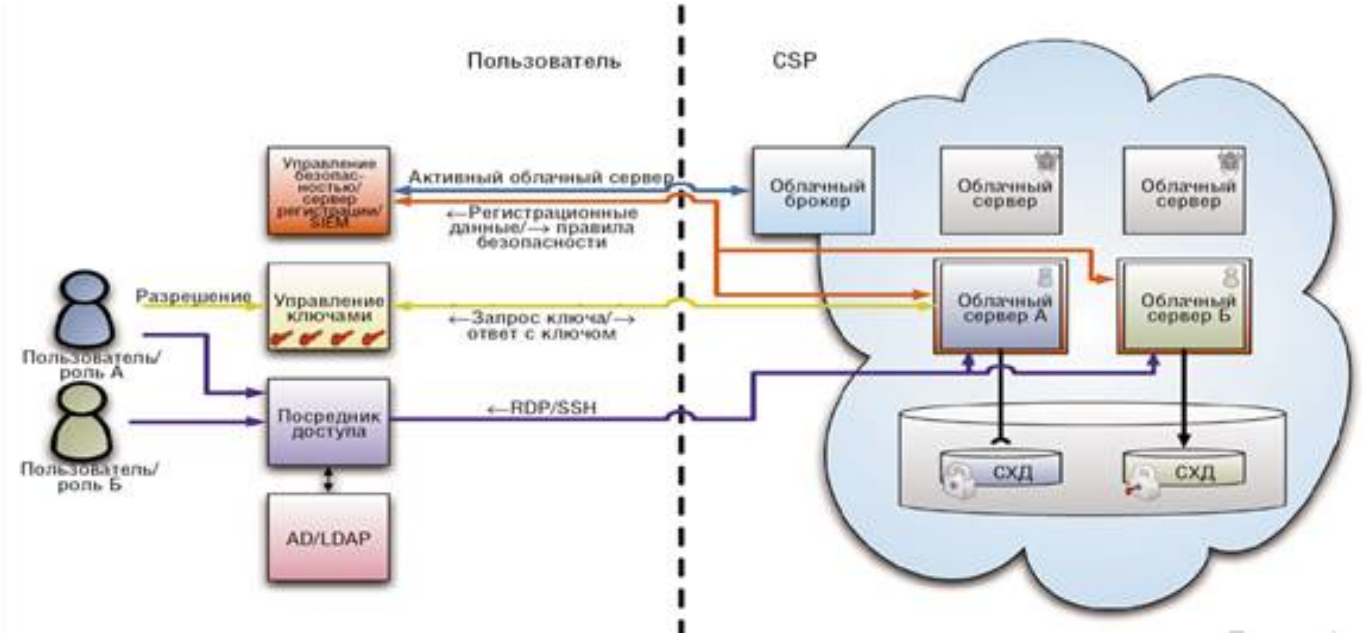


***Рисунок. 2 (Схема взаимодействия пользователя, сервера управления ключами и облачного сервера)***

2. Аутентификация

Аутентификация — это процесс проверки подлинности чего-либо. Проще говоря, это защита с помощью пароля. В случае если внедренные сведения оказываются точными, то пользователь приобретает допуск к некоторым составляющим инфраструктуры. Существуют различные виды аутентификации. Надежным видом является двухфакторная аутентификация. Например, после ввода логина и пароля , необходимо подтвердить ваш вход при помощи одноразового когда, который приходит SMS сообщением на телефон.

3. Защита данных при передаче

Доступ к данным, которые  передаются должны быть доступны только после аутентификации. Никому и никак не получится изменить или прочитать информацию, которая передается, несмотря на надежные узлы передачи. Как правило, для публичного облака используется VPN-туннель в целях защиты данных пользователя.VPN-туннель основан на двухфакторной аутентификации.

# Заключение.

Все перечисленные методы защиты были использованы в различных проектах построения облаков. Они существенно снизили процент случившихся взломов и различных инцидентов. Несмотря на это, существует еще множество проблем, которые связаны с защитой и безопасностью облачных систем.

**Список литературы:**

1. Джордж Риз: Cloud Application Architectures (Облачные вычисления).  БХВ-Петербург , 2013- 288с.

2. Клементьев И.П. Устинов В.А. Введение в Облачные вычисления. УГУ, 2013 -233с.

3. Короткова Е.Е. Использование облаков и облачных вычислений в коммерческой

деятельности / Короткова Е.Е., Денисенко В.В. – Научные тенденции: Вопросы точных и технических наук, 2017.

4. Никольский А.В. Защита облачных вычислений от атак на средства виртуализации. СПБ, 2013-210с.