ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

ЗАЩИТА ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ОРГАНИЗАЦИЯХ

Казкеева Гульфарам Бериковна
Магистрант кафедры Вычислительной техники, факультета информационных технологий
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Жумадиллаева А.К.

Облачные (рассеянные) технологии – технологии обработки данных, предоставляющие пользователю компьютерные ресурсы и мощности как интернет-сервис. Пользователь имеет доступ к своим данным, но не может управлять инфраструктурой, операционной системой и собственно программным обеспечением, с которым работает. Для поддержки облачных вычислительных сред используются технологии виртуализации. В бизнесе применяется несколько видов виртуализации:

- виртуализация серверов – перенос физических серверов в виртуальные машины (ВМ) одного физического сервера (хостовой системы), оснащенного средством виртуализации (гипервизором);
- виртуализация рабочих мест пользователей – централизованное хранение рабочих мест (виртуальных десктопов) в виде ВМ на сервере (хостовой системе) с предоставлением доступа по сети с физических рабочих мест (тонких клиентов);
- виртуализация терминалов – для пользователя терминала создается собственный сеанс работы в ОС.

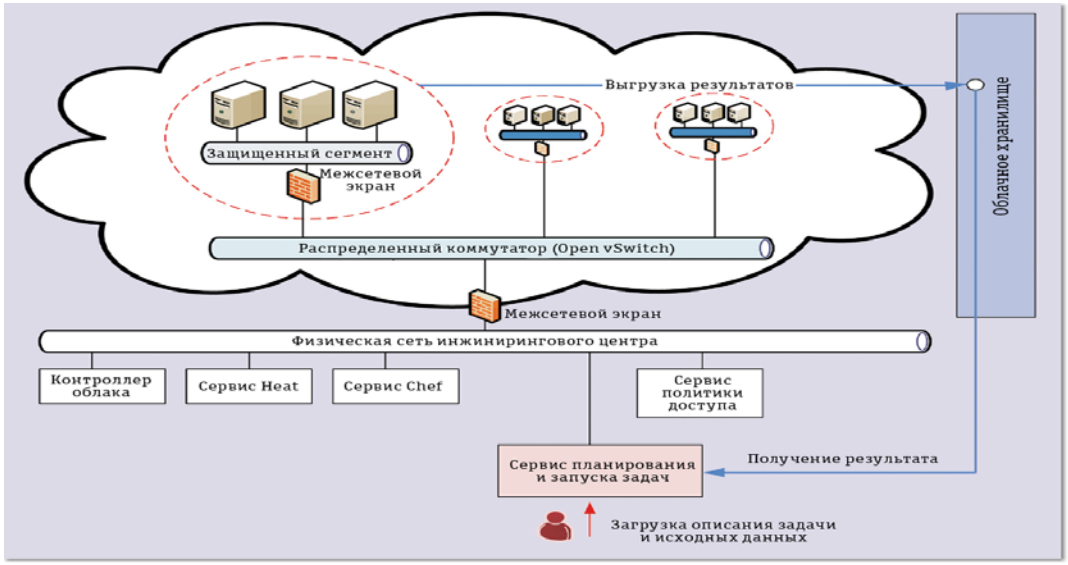


Рисунок 1 - Угрозы безопасности облачных технологий и виртуализации

Приведем наиболее актуальные угрозы для виртуально-облачной среды. Среди угроз, направленных на АРМ конечных пользователей, можно выделить компрометацию клиентских устройств доступа в облако и атаки на клиентские браузеры. Эти угрозы актуальны вследствие слабой защиты АРМ конечных пользователей и отсутствия контроля политики информационной безопасности (ИБ) на АРМ пользователей при доступе в облака. Через гипервизор реализуется такая угроза виртуальной инфраструктуре, как несанкционированный доступ (НСД) к среде виртуализации. Он возможен вследствие нарушения изоляции среды, предоставленной клиенту в рамках облачной услуги. Например, может использоваться уязвимость в реализации инструкции SYSRET всех процессоров Intel архитектуры x86-64. Также НСД возможен вследствие плохой очистки клиентской информации на стороне провайдера облачных услуг. Кроме того, вследствие некорректных

настроек гипервизора возможен несанкционированный доступ к ресурсам ВМ из реальной или виртуальной среды. В рамках виртуальной среды НСД возможен вследствие программных закладок или ошибок в ПО гипервизора. Вследствие эксплуатации уязвимостей гипервизора возможны атаки на сервер с гипервизором из сетевой среды типа "переполнение буфера" и "отказ в обслуживании".

Так какие же безопасные способы использования облачных технологий существуют? Предлагаем рассмотреть один из подходов к защите облачных технологий. Для защиты от несанкционированного доступа рабочих мест пользователей, хостовой системы и системы хранения данных предлагается использовать традиционные сертифицированные средства защиты от НСД, такие как Dallas Lock компании "Конфидент" и Secret Net компании "Код безопасности". Для антивирусной защиты ВМ предлагается использовать новаторский безагентный подход, обеспечивающий комплексную безопасность без установки агентского модуля в защищаемой системе. К примеру, безагентный режим использует решение Deep Security компании Trend Micro. В виртуальную среду внедряется виртуальное устройство – шлюз безопасности, который берет на себя функции антивируса для всех ВМ. Для шифрования трафика, усиленной аутентификации, аудита и межсетевого экранирования ВМ совместно с Deep Security предлагается использовать Secure Cloud компании Trend Micro. Необходимо использовать системы обнаружения вторжений и межсетевого экранирования. С появлением виртуальных сред появилась новая проблема – неконтролируемое сетевое взаимодействие между ВМ. Общая рекомендация такова: контролировать внешние подключения к среде виртуализации следует с помощью аппаратных решений, а внутренние – с помощью программных решений, реализуя таким образом комбинированный подход. Для контроля трафика как между ВМ внутри хоста, так и со стороны каждой ВМ в отдельности предлагается использовать решение Deep Security компании Trend Micro. Обеспечить эффективную защиту от сетевых угроз позволяет семейство продуктов StoneGate Virtual Security компании Stonesoft, включающее в себя виртуальный межсетевой экран StoneGate Virtual Firewall/VPN и систему предотвращения вторжений StoneGate Virtual IPS, а так же StoneGate Virtual SSL VPN. Дополнительный плюс в том, что продукты Virtual Firewall/VPN и Virtual IPS сертифицированы ФСТЭК и ФСБ для платформ VMware ESX/ vSphere и поддерживают технологию VMsafe

Еще одним средством защиты, заслуживающим внимания, является комплексное решение – VirtualManagementCenter (VMC) компании Reflex, позволяющее контролировать сетевой трафик. В Reflex VMC входят компоненты, которые позволяют повышать эффективность эксплуатации, защиту и расширенный мониторинг:

• vCapacity обеспечивает планирование основных параметров виртуальной среды и динамическое управления конфигурацией;

• vTrust выполняет функции обеспечения сетевой безопасности внутри виртуальной инфраструктуры. vTrust осуществляет мониторинг и контроль трафика между виртуальными машинами, реализует настройку

политики безопасности на уровне виртуальных машин, организует виртуальные зоны доверия, обеспечивает динамическое управление сетью вне зависимости от физического расположения виртуальных ресурсов;

• vWatch позволяет администратору получить

всесторонний обзор состояния виртуальной среды на любой момент времени и оценить влияние изменения конфигурации на работу системы;

• vProfile осуществляет контроль за соблюдением требований внутренних и внешних стандартов, обеспечивает единую конфигурацию всей виртуальной инфраструктуры. Например, контроль соответствия политике безопасности позволяет в блокировать сетевое взаимодействие виртуальных машин, контроль основных настроек гипервизора позволяет быстро привести виртуальную среду в соответствие с рекомендациями производителя или отраслевыми стандартами (например, PCI DSS). Решение vSecurity компании Catbird реализует расширенные функции аудита, инвентаризацию объектов и программного

обеспечения виртуальной инфраструктуры (включая ПО, установленное на сами ВМ), сетевой контроль и защиту гипервизора от сетевых атак, а также управление конфигурациями. Решение гарантирует соблюдение заданных с точки зрения ИБ параметров и позволяет управлять изменениями и уязвимостями.

Список использованных источников

1. Toby Velte; Anthony Velte; Robert Elsenpeter; Robert C. Elsenpeter: Cloud computing, 2009
2. http://www.computerra.ru/95632/oblachnaya-zashhita-tehnologiya-protiv-ideologii/
3. http://www.osp.ru/lan/2013/04/13035155/

ОӘЖ 004.27

ЖОБАНЫҢ ҮШ ДЕҢГЕЙЛІ АРХИТЕКТУРАСЫ

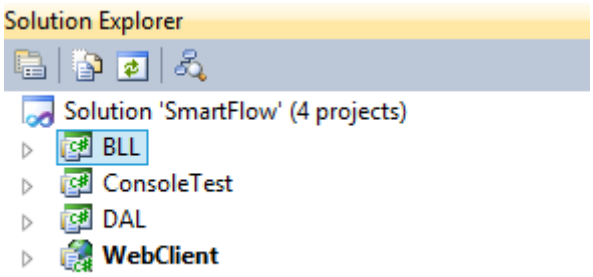
Каракулов Ерлан Махсутович
Л.Н. Гумилев атындағы ЕҰУ, 6М070400 – “Есептеу техникасы және бағдарламалық қамтамасыз ету” мамандығының магистранты
Ғылыми жетекшісі – К.Т. Искаков

Кез келген жобада қандай паттернды қолданса да, кодтың үш деңгейлі архитектура қағидалары сақталуы қажет [1-3]:

Деңгей DAL (Data Access Layer) – ДҚ-мен жұмысқа жауап береді. Яғни, ешқандай есептеулер жүргізбейді. Оның есебі мәліметтермен тек CRUD амалдарын орындаумен шектеледі.(Create, Read, Update, Delete). Сонымен қатар, тракзакциялар орындалуы, ДҚ-на қосылу, sql функцияларын шақыру, процедуралар орындау, яғни, көріп тұрғандарыңыздай, бұл деңгейді біз тікелей СУБД-мен жұмыс жасаймыз.

Деңгей BLL (Business Logic Layer) – жоба құру кезінде қажет болатын барлық есептеулерді қамтиды. Мысалы, менің жобамда тауарды белгілі бір сомаға сату амалы бар (жеңілдіктермен бірге болуы мүмкін), сонда бір транзакцияда ол тауардың сатылуы, қоймадан тауар санының азаюы, компания табысының артуы, т.с.с. амалдар орындалуы тиіс. Байқағаныңыздай, BLL өз ішінде DAL-ды қолданады, керісінше емес.

Деңгей UI (User Interface) – серверден келген мәліметтерді көрсетумен ғана айналысады. Бізде Application server, Database Server бар. Қосымшалар сервері қолданушының жіберген сұранымдарын қабылдап, талдау жасайды. Кейін, сұранысқа сәйкес HTML кодты клиентке жібереді, өз кезегінде Деректер серверіне сұраным жасауы мүмкін. Клиент тек UI көреді, сонымен байланысады, ал, BLL өз кезегінде DAL-мен байланысады.
Деңгейлердің байланысу сызбасы мына түрде болушы еді:
Client <->UI<->BLL<->DAL
Осының бәрін Visual Studio бағдарламалау ортасында көрсетейік:



Сурет 1. Жоба құрылымы