ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

КАЧЕСТВО ИННОВАЦИИ ОБРАЗОВАНИЕ

№6 (109)
ИЮНЬ 2014

АДРЕС РЕДАКЦИИ И ИЗДАТЕЛЯ
105118, Москва, ул. Буракова, д. 8
Тел.: +7 (495) 916-89-29
Факс: +7 (495) 916-81-54
E-mail: quality@eqc.org.ru (для статей)
hg@eqc.org.ru (по общим вопросам)
www.quality-journal.ru; www.quality21.ru

ИЗДАТЕЛЬ
Европейский центр по качеству

НАУЧНЫЙ РЕДАКТОР
Гудков Ю.И.
ygudkov@hse.ru

ХУДОЖЕСТВЕННЫЙ РЕДАКТОР
Гуревич А.А. (ООО "Экспресс 24")

ЛИТЕРАТУРНЫЙ РЕДАКТОР
Савин Е.С.

ОТВЕТСТВЕННЫЙ СЕКРЕТАРЬ
Мартюкова Е.С.
ne@eqc.org.ru

ЖУРНАЛ ЗАРЕГИСТРИРОВАН
в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций. Свидетельство о регистрации ПИ №77-9092

ПОДПИСНОЙ ИНДЕКС
в каталоге агентства «Роспечать» 80620, 80621
в каталоге агентства "Урал-Пресс" 14490
на сайте НЭБ eLIBRARY.RU 80620

ОТПЕЧАТАНО
ФГУП Издательство «Известия» УД ПРФ
127254, г. Москва, ул. Добролюбова, д. 6

Журнал входит в перечень ВАК РФ

Статьи рецензируются

СОДЕРЖАНИЕ

Сведения о членах редколлегии и об авторах статей можно найти на сайте www.quality-journal.ru

А.С. Кабанов, А.Б. Лось

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ГОСУДАРСТВЕННОМ СЕКТОРЕ

В статье рассматриваются вопросы использования облачных технологий в современных условиях. Дана общая характеристика указанных технологий и рассмотрено одно из направлений, связанное с удаленным хранением и обработкой данных. Приведены примеры существующих решений и отмечены основные проблемы с точки зрения обеспечения информационной безопасности. Обсуждаются различные точки зрения на целесообразность и перспективы применения облачных технологий в государственном секторе. Отмечено, что, несмотря на все проблемы, облачные технологии являются перспективным направлением, в том числе, и в государственном секторе.

Ключевые слова: облачные технологии, удаленная обработка данных, информационная безопасность

Облачные технологии и информационная безопасность

В условиях быстрого развития информационных технологий и электронного документооборота особую актуальность приобретают вопросы внедрения технологий, связанных с созданием виртуальных файловых систем, предоставляющих доступ к удаленным серверам, и обеспечением их безопасности. Особое распространение в последнее время получили, так называемые, облачные технологии [1, 2, 3].

Облачные (рассеянные) вычисления (англ. cloud computing, также используется термин «Облачная (рассеянная) обработка данных») – технология обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Пользователь имеет доступ к собственным данным, но не может ими управлять и не должен заботиться об инфраструктуре, операционной системе и собственно программном обеспечении, с которым он работает. Термин «Облако» используется как метафора, основанная на изображении Интернета на диаграмме компьютерной сети, или как образ сложной инфраструктуры, за которой скрываются все технические детали.

Облачная обработка данных как концепция включает в себя понятия:

- инфраструктура как услуга;
- платформа как услуга;
- программное обеспечение как услуга;
- данные как услуга;
- рабочее место как услуга;
- другие технологические тенденции, общим в которых является уверенность, что сеть Интернет в состоянии удовлетворить потребности пользователей в обработке данных.

Например, Google Apps обеспечивает приложения для бизнеса в режиме онлайн, доступ к которым происходит с помощью Интернет-браузера, в то время как ПО и данные хранятся на серверах Google.

Следует заметить, что одной из главных проблем удаленных способов хранения и обработки данных является обеспечение их безопасности.

Рассмотрим несколько наиболее известных в данном направлении решений, в том числе, и с точки зрения обеспечения конфиденциальности и целостности информации.

Одной из известных виртуальных файловых систем, предоставляющей доступ к удаленным FTP-серверам, является система CurlFtpFS [7]. Это бесплатная реализация виртуальной файловой системы, осуществляющей доступ к FTP-серверу, работающая с операционными системами на ядре Linux. Данный продукт базируется на популярной библиотеке «libcurl», которая используется для передачи файлов, адресуемых с помощью URL (Uniform Resource Locator – единый указатель ресурсов; последние три буквы в названии библиотеки имеют в виду именно эту аббревиатуру). Что касается обеспечения безопасности информации, то следует заметить, что данная программа не

поддерживает возможности шифрования файлов перед сохранением на удаленном сервере. Она поддерживает протокол SFTP для обеспечения безопасности соединения, однако это не решает проблемы доверенности сервера.

Примером другой виртуальной файловой системы, решающей схожую задачу, является система «Encrypted Virtual File System» [8]. Она также создана для работы с операционными системами, использующими ядро Linux. Данная система поддерживает шифрование файлов, однако хранит шифрованные файлы не на удаленном FTP-сервере, а в указанной директории файловой системы той же операционной системы.

Пользователь может применить эти два решения одновременно, создав шифрующую виртуальную файловую систему поверх другой виртуальной, реализующей доступ к файлам на удаленном FTP-сервере.

Однако и в этом случае система будет иметь ряд существенных недостатков, осложняющих ее применение:

- Установка такой системы не является простой задачей для пользователя, поскольку не существует руководств по установке подобной композиции продуктов.
- Подобная система может оказаться нестабильной, поскольку не было проведено необходимых мероприятий по тестированию подобной композиции.
- Использование двух независимых продуктов с независимыми реализациями может существенно повысить латентность при доступе к данным и, тем самым, осложнить применение данной системы.

В статье не рассматриваются коммерческие продукты с закрытым исходным кодом, поскольку для их использования требуется проведение отдельных мероприятий по выявлению скрытых функционалов и возможных ошибок.

В качестве примера рассмотрим наиболее важные и принципиальные операции над файлами, которые можно совершать при пользовании удаленными хранилищами информации. Необходимо подчеркнуть, что речь идет об операции в широком смысле этого слова, без привязки к конкретной файловой или операционной системе.

Список возможных операций:

- создание файла;
- запись данных в файл;
- чтение данных из файла;
- удаление данных из файла;
- создание директории;
- удаление директории.

Рассмотрим более подробно каждую из операций.

Создание файла

При создании файла в виртуальной файловой системе, файл с тем же именем должен быть создан на удаленном сервере. При этом, на создание файла должен действовать ряд ограничений. Файл не должен быть создан в виртуальной файловой системе, если по какой-то причине его не удалось создать на удаленном сервере.

Основные причины, по которым файл может быть не создан на удаленном сервере:

- Не удалось установить соединение с сервером и выполнить на нем команду для создания файла.
- Сервер отказал в выполнении команды из соображений безопасности или разграничения доступа.
- Сервер отказал в выполнении команды, так как получил ошибку своей файловой системы (например, недопустимое имя).
- На сервере произошел программный или же аппаратный сбой.

Во всех случаях виртуальная файловая система генерирует сообщение об ошибке и невозможности создания файла, что делается для поддержания синхронного состояния между удаленной и виртуальной файловыми системами.

Запись данных в файл

Запись данных в файл можно разделить на следующие этапы:

- запись в локальный файл;
- формирование данных для проверки целостности;
- шифрование;
- загрузка файла на удаленный сервер.

Если исполнение одного из этапов невозможно, то операция записи признается невыполнимой, остальные этапы игнорируются, а пользователю возвращается соответствующая ошибка.

Примеры возможных отказов:

- Запись в локальный нешифрованный файл:

- ошибка или ограничения локальной файловой системы;

- Шифрование:

- отсутствие ключа или сбой механизма шифрования;

- Загрузка файла на удаленный сервер:

- стандартные ошибки исполнения команды на удаленном сервере, аналог которых рассмотрен выше при обсуждении создания файла.

Чтение из файла

Чтение информации из файла можно разделить на следующие этапы:

- получение файла с удаленного сервера;
- расшифровка файла;
- проверка целостности;
- извлечение требуемой области данных из расшифрованного файла.

Если исполнение одного из этапов невозможно, то требуемые данные признаются недоступными, остальные этапы игнорируются, а пользователю возвращается соответствующая ошибка.

Примеры возможных отказов на этапах чтения файла:

- Получение файла с удаленного сервера:

- стандартные ошибки исполнения команды на удаленном сервере, аналог которых рассмотрен выше при обсуждении создания файла;

- Расшифровка файла:

- отсутствуют необходимые данные для расшифровывания файла;

- Проверка целостности:

- не пройдена проверка целостности, что означает, что файл был изменен третьими лицами;

- Извлечение требуемой области данных:

- запрашивается область данных, отсутствующая в файле, например, из-за недостаточной длины.

Удаление файла

Для удаления файла справедливы те же соображения, что и для создания. Файл должен быть удален из виртуальной файловой системы в том и только том случае, если он успешно удален с удаленного сервера.

Создание и удаление директории

Для создания и удаления директории справедливы те же соображения, что и для создания и удаления файла. Директория должна быть удалена из виртуальной файловой системы в том и только том случае, если она успешно удалена с удаленного сервера. Причины, по которым директория может не создаться и не удалиться с удаленного сервера при соответствующей команде от пользователя, совпадают с причинами отказа в создании и удалении файла

Отметим, что одной из главных проблем в использовании большинства продуктов, с точки зрения обеспечения информационной безопасности, является отсутствие поддержки ими российских алгоритмов шифрования. Данное обстоятельство не позволяет сертифицировать данные технологии, что создает сложности при использовании их в государственном секторе.

Перспективы внедрения облачных технологий в государственном секторе

Следует заметить, что многие организации, в том числе и государственные структуры, оценивают экономическую эффективность перехода на облачные технологии как достаточно низкую. Такая оценка определяется тем, что существующие организации, как правило, уже имеют свою собственную построенную инфраструктуру. Необходимые затраты на модификацию данной структуры и переход на облачные технологии могут иметь длительные сроки окупаемости. Кроме того, стоимость каналов связи может составлять до 50% от затрат организации. В результате, для получения необходимого качества обслуживания вышеприведенные затраты превысят экономию от централизации инфраструктуры.

Как правило, при анализе рабочей нагрузки, организации, предоставляющие услуги облачных сервисов, могут показать требуемую степень доступности (например, каналов связи), необходимую для выполнения работы организации заказчика, но это не является достаточным. При использовании облачных технологий важным является качество и соответствующие характеристики каналов связи. В большинстве регионов России соглашения об уровне предоставления услуг и качестве обслуживания являются нерешенными вопросами, что определяет ряд соответствующих проблем. Из этих проблем можно выделить следующие: пропускную способность беспроводных каналов, вопросы последней мили на пути от клиента к облаку, обеспечение информационной безопасности, в частности, использование шифровальных средств, криптографических средств обеспечения подлинности информации и др.

Кроме этого, дополнительно необходим анализ центров обработки данных (далее — ЦОД), сетевых устройств, подключаемых к облачным сервисам, нормативно-правовой базы по применению облачных технологий и др. [1, 2]. По мнению ряда экспертов, отсутствие надежных ЦОД является одним из решающих факторов отказа от использования облачных технологий. В числе вопросов защиты информации в ЦОД, помимо программного обеспечения, важной составляющей является человеческий фактор. Персонал, обслуживающий ЦОД, должен иметь соответствующий уровень подготовки по вопросам информационной безопасности, проходить дополнительные проверки в службах безопасности. Физический доступ персонала к аппаратной части ЦОД должен быть ограничен. Операторы не должны иметь возможности доступа к данным клиентов.

Несомненно, что все вышеперечисленные составляющие являются важными элементами подхода к обеспечению информационной безопасности облачных технологий, но ключевым моментом в этой области является необходимость разработки унифицированных стандартов. Это связано с тем, что данные технологии составляют новое направление развития IT-индустрии, и существует множество компаний-разработчиков, которые используют различ-ные подходы к обеспечению информационной безопасности.

Важным является вопрос использования облачных технологий в государственных инфраструктурах России. В настоящее время по этому поводу существуют два диаметрально противоположных мнения.

Первое заключается в невозможности использования облачных технологий по ряду причин, таких как: отставание технологического развития имеющихся инфраструктур; отсутствие программного обеспечения, разработанного отечественными производителями; высокая возможность утечки данных при размещении на удаленных сервисах и др. Кроме того, немаловажен факт территориального расположения удаленных облачных сервисов, на которых происходит обработка и хранение данных. На сегодняшний день мировые лидеры по предоставлению облачных сервисов, такие компании как Amazon, CitrixSystems, Google, Microsoft и др. используют датацентры, расположенные на территории США и Западной Европы. Спецслужбы США могут получить доступ к информации, расположенной в ЦОДах, в соответствии с законодательной базой [3]. Все это приводит к невозможности использования облачных сервисов зарубежных компаний из-за соображений национальной безопасности.

Второе мнение, которое разделяют и авторы статьи, базируется на том, что в ближайшее время внедрение облачных технологий коснётся и государственных инфраструктур России. Здесь можно провести определенную аналогию с использованием сети Интернет: достоинств от ее использования больше, чем недостатков, таких как возможность нарушения информационной безопасности, утечка конфиденциальной информации и др. В настоящее время большинство государственных инфраструктур не имеют межведомственного электронного взаимодействия,

используемое оборудование устарело, не имеется единой базы данных документов. В связи с этим, одним из направлений решения накопившихся проблем, согласно материалам статьи [4], является планирование, создание и использование информационно-коммуникационных технологий в деятельности государственных органов, а также внедрение систем электронного документооборота и организация архивов. При этом, цель состоит не столько в оптимизации внутренней работы ведомств, сколько в удовлетворении требований, предъявляемых к информационным системам в рамках межведомственного электронного документооборота и систем межведомственного электронного взаимодействия [5].

Весомыми аргументами применения облачных технологий в госсекторе России служат примеры их внедрения в наиболее развитых государствах мира. По данным японской компании Nec, в государственном секторе США активно продвигается внедрение облачных технологий. Так, например, в сентябре 2009 года Федеральный совет CIO под руководством Службы управления и бюджета администрации президента объявил о Федеральной Правительственной Инициативе Облачных Вычислений (Federal Government's Cloud Computing Initiative). Служба управления и бюджета администрации президента США предложила всем государственным учреждениям провести оценку альтернативных вариантов облачных вычислений по основным инвестициям в информационные технологи. В 2013 году все инвестиции в информационные технологии в постоянном режиме должны анализироваться с точки зрения облачных вычислений [6].

Заключение

На наш взгляд, одним из вариантов решения проблемы безопасного внедрения облачных технологий в государственных инфраструктурах России является создание частных облаков (privatecloud) и организаций, в том числе и коммерческих, имеющих соответствующие лицензии на деятельность по обслуживанию государственных структур.

Недостаточное доверие потребителей к облачным услугам связано с множеством причин, основными из которых являются опасения потери контроля над своими информационными ресурсами, а также неуверенность в сохранности и защите своих данных. Но эти проблемы являются далеко не новыми и существуют достаточно хорошо проработанные пути их решения.

Подводя итоги сказанному выше, отметим, что необходимость развития систем защиты информации при использовании облачных технологий является актуальной проблемой, а ее решение имеет большое значение для общества, правительства, силовых структур, промышленности и научных кругов России.

Литература

1. Облачные сервисы. Взгляд из России / Под ред. Е. Гребнева. – М.: CNews, 2011.– 282с.
2. Сюртуков И. Что мешает активному переходу заказчиков в России к «облачным» технологиям? Портал iBusiness. – Режим доступа: http://i-business.ru/blogs/ 11529.
3. Thompson B. Storm warning for cloud computing. – Режим доступа: http: //www.news.bbc. co.uk/2/hi/technology/7421099.stm.
4. Постановление Правительства Российской Федерации от 25 апреля 2012 г. № 394 // Российская газета. – Режим доступа: http://www.rg.ru/2012/05/08/gosorgany-site-dok. html.
5. Смирнов Н. Директор информационной службы. –2012. – №10.– Режим доступа: http://www.mfpa.ru/general/upload/contents_journal/direktor_informacionnoi_slujby .doc.
6. Харламов А. Облачные вычисления для государственного и муниципального управления: решения от корпорации NEC. – Режим доступа: http://www.iis.ru/docs/harlamov.pdf.
7. Домашняя страница CurlFtpFS. Режим доступа: http://curlftpfs.sourceforge .net/.
8. Сообщество SecurityFocus. Режим доступа: http://www.securityfocus.com/tools/3189.

Кабанов Артем Сергеевич,
канд. техн. наук, доцент кафедры
«Компьютерная безопасность» НИУ ВШЭ.
E-mail: kabanov_as@mail.ru

Лось Алексей Борисович,
канд. техн. наук, доцент кафедры
«Компьютерная безопасность» НИУ ВШЭ.
E-mail: alexloss2011@mail.ru

A.S. Kabanov, A.B. Los

PROBLEMS OF MAINTENANCE OF INFORMATION SECURITY IN THE USE OF CLOUD TECHNOLOGIES IN THE PUBLIC SECTOR

The article deals with the use of cloud technologies in modern conditions. Common characteristics of these technologies and considered one of the areas associated with a remote storage and processing of data. The examples of the existing solutions and noted the main problems from the point of view of information security. Discusses the different views on the advisability and prospects of cloud technologies in the public sector. Noted that, despite all problems, cloud computing is a promising direction, including, and in the public sector.

Keywords: cloud computing, remote data processing, information security.

References

1. Cloud services. A view from Russia / Ed. by E. Grebneva. – M: CNews, 2011. – 282 p.
2. The frock coats I. What is preventing the shift of customers in Russia to "cloud" technologies? Portal iBusiness journal. – Mode of access: http://i-business.ru/blogs /11529.
3. Thompson B. Storm warning for cloud computing. – Mode of access: http: //www.news.bbc. co. uk/2/hi/technology/7421099.stm.
4. Resolution of the Government of the Russian Federation on April 25, 2012 № 394 // Russian newspaper. – Mode of access: http://www.rg.ru/2012/05/08/gosorgany-site- dok. html.
5. Smirnov N. Director of information services. – 2012. – №10.– Mode of access: http://www.mfpa.ru/general/upload/contents_journal/direktor_informacionnoi_ slujby .doc.
6. Kharlamov A. Cloud computing for the state and municipal management: solutions from NEC Corporation. — Mode of access: http://www.iis.ru/docs/harlamov. pdf.
7. Home page CurlFtpFS. Mode of access: http://curlftpfs. sourceforge.net/.
8. Community SecurityFocus. Mode of access: http://www.securityfocus.com/tools/ 3189.

Kabanov Artem Sergeevich,
candidate of technical Sciences,
associate Professor of the Department
"Computer security" HSE
E-mail: kabanov_as@mail.ru

Los Alexey Borisovich
candidate of technical Sciences
associate Professor of the Department
"Computer security" HSE
E-mail: alexloss2011@mail.ru