

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ И ПРОБЛЕМА БЕЗОПАСНОСТИ

Хабло Денис Васильевич

студент, ФГАОУ ВО «Нижегородский государственный университет им. Н.И. Лобачевского»,
РФ, , Нижегородская область, г. Нижний Новгород

Cloud Computing and Security Issue

Denis Khablo

student, FGAOU VO "Nizhny Novgorod State University. N.I. Lobachevsky", Russia, Nizhny Novgorod region, Nizhny Novgorod

Аннотация. В статье рассматриваются базовые понятия облачных вычислений, и прослеживается причинно-следственная связь необходимости совершенствования данной сферы с проблемой информационной безопасности. Ключевая актуальность работы состоит в определении перспектив применения и развития не только самой системы облачных вычислений, но и параметров ее безопасности.

Abstract. The article discusses the basic concepts of cloud computing and traced the cause-effect relationship in this sphere need to improve information security problem. The key relevance of the work is to determine the prospects of application and development of not only the system of cloud computing, but also its security settings.

Ключевые слова: облачные вычисления; информационная безопасность; сервис; технология; инновации.

Keywords: cloud computing; Information Security; service; technology; Innovation.

В последние годы эффективное применение приобретают облачные технологии или облачные вычисления (англ. Cloud computing). В некоторых источниках [4, с. 21] дается определение облачных вычислений как модели обеспечения повсеместного и удобного доступа через сеть к общему пулу вычислительных ресурсов, подлежащих настройке (например, к коммуникационным сетям, серверам, средствам хранения данных, приложений и сервисов), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращением к провайдеру [9, с.112].

К облачным технологиям проявляют интерес как крупные компании, которые пытаются оптимизировать свои расходы на IT-инфраструктуру предприятия, так и малые компании, которые не имеют возможности сразу развернуть свою собственную инфраструктуру. Также заинтересованы обычные пользователи, которые могут получить такие услуги, как хранение данных, использование программ [2, с. 97].

Рост интереса к технологиям облачных вычислений связан с экономическим эффектом от их использования. В ходе их использования потребители могут существенно снизить капитальные затраты на построение центров обработки данных, закупку серверного и сетевого оборудования, аппаратных и программных решений, обеспечения непрерывности и работоспособности, а также при построении и введении в эксплуатацию крупных объектов инфраструктуры информационных технологий. Все эти проблемные вопросы при данных условиях переводятся с пользователей на провайдеров облачных услуг, а пользователь только оплачивает фактически оказанные услуги [2, с. 99]. Также облачные сервисы предоставляют пользователям гибкость в настройке таких параметров, как вычислительная мощность, объем файлового хранилища, состав программного обеспечения и тому подобное.

Однако, несмотря на явные преимущества, при использовании облачных вычислений необходимо решать и ряд проблемных вопросов. Основными из них являются доверие к поставщику сервиса, обеспечение конфиденциальности, целостности, подлинности и безотказности информации на всех этапах ее существования, бесперебойность в работе, защита от несанкционированного доступа (НСД) и сохранения личных данных пользователей, которые передаются и обрабатываются в облаке.

Основными направлениями рисков для безопасности данных считают следующие [8, с. 65]:

- 1) нормативно-правовой (конфликт юрисдикций в части регулирования трансграничной передачи данных и ограничений по их защите)
- 2) технологический (ситуации, когда чрезмерная удаленность сервера может привести к задержкам транспортировки данных и критическим ошибкам в работе программ, а также когда один мощный дата-центр обслуживает большое количество потребителей по всему миру).

В связи с тем, что для облачных технологий стратегическим вопросом является избрание расположения дата-центров, то чаще всего такие центры размещены в оффшорных юрисдикциях или в зонах с определенной географической особенностью, и нередко в странах с несовершенным законодательством в сфере киберзащиты и защиты персональных данных.

Например, дата-центры корпорации Google расположены не только в США, но и во многих странах мира [11]. В 2009 г. корпорация получила патент на дата-центр морского базирования с размещением на судне, которое находится в нейтральных водах. Таким образом, этот объект выведен за пределы юрисдикции какого-либо государства мира, и не надо будет платить налоги. Но стратегически важным является то, что для решения части проблем обеспечения информационной безопасности можно разместить на морской платформе резервный дата-центр на случай стихийного бедствия.

Отметим, что для дата-центров, обслуживающих органы государственной власти США, действует норма, что делает невозможным их размещение вне территории государства [10].

А вот Госдума РФ в июле 2014 приняла изменения в закон о персональных данных, обязывающее зарубежные интернет-компании сохранять личную информацию о российских пользователях только на серверах, расположенных на территории России. Изменения вступили в силу с 01.09.2015 [1].

Главными проблемами, которые требуют дальнейшего детального анализа и решения, являются, с точки зрения автора, такие:

1. Проблема привилегированных пользователей. Наибольшую угрозу для безопасности информации в облаке составляют пользователи, имеющие привилегированный доступ к функциям системы или администраторы облачных сервисов, поэтому для уменьшения риска возможных деструктивных действий с их стороны, целесообразно вести независимый надзор и контроль над их действиями в облаке.
2. Одной из главных проблем, которая тормозит распространение облачных вычислений, является несоответствие законов в сфере обработки, передачи, хранения и защиты

информации различных государств. Решение этой проблемы, по мнению автора, является ключевым фактором для возможности физического размещения серверов поставщика облачных сервисов в разных странах и регионах.

3. Вопрос доверия к поставщику услуг может быть решен только за счет проведения аудита безопасности поставщика облачных услуг и проверки соответствия его системы безопасности международным требованиям к защите информации, сформулированным в международных стандартах.

4. Вопрос общих уязвимостей в облаке практически ничем не отличается от аналогичных в традиционных системах, за исключением того, что найденная одна уязвимость может быть использована для всего облака. И в это время критичность ситуации гораздо большая, потому что данная проблема может с легкостью поразить всех пользователей данного поставщика услуг.

5. Проблемы доступности к сервисам и данным пользователями, восстановление их работы после сбоев, или потери данных должны решаться на административном и правовом уровнях. При заключении договоров с пользователем должны быть четко определены обязанности сторон и мера их ответственности в зависимости от обстоятельств события, приведшего к этим последствиям, а расследование должна проводить третья независимая сторона.

В контексте применения инновационных методов используется концепция облачных вычислений, которая построена на новой конфигурации. Новая конфигурация состоит из разнообразия новых технологий, таких как Hadoop (фреймворк), Hbase (один из видов нереляционных баз данных) семейства Apache, что повышает производительность системы облачных вычислений, но одновременно может привести к риску [5, с. 11]. Среда облачных вычислений дает пользователю возможность «купить» полный доступ к ресурсам, что также увеличивает риск угрозы безопасности.

На сегодня ведущими организациями, которые занимаются вопросами безопасности в облаке, является Альянс безопасности в облаке (Cloud Security Alliance, CSA), который состоит из представителей it-индустрии, а также две государственные организации Европы и США: Европейское агентство сетевой и информационной безопасности (ENISA) и Национальный институт стандартов и технологий (NIST). Каждая из организаций создала соответствующий документ с классификацией всех существующих проблем информационной безопасности (ИБ) в облаке [7, с. 147].

Стоит отметить также требования к безопасности на основе анализа HDFS. HDFS (Hadoop Distributed File System) является известной распространенной технологией облачных вычислений, которая используется в крупномасштабных облачных вычислениях в типовой конфигурации распределенной файловой системы. HDFS похожа на существующую распределенную файловую систему, такую как GFS (Google File System) они имеют идентичные цели, производительность, доступность и стабильность. HDFS сначала использовалась в сетевой поисковой системе Apache Nutch и стала основой проекта Apache Hadoop [11].

Анализируя HDFS, требования безопасности к облачным вычислениям можно разделить на следующие группы:

- Проверка достоверности логина клиента: большинство облачных вычислений проверяют браузер клиента и проводят идентификацию пользователя по запросу программ облачных вычислений для первичной потребности.
- Присутствие единичной ошибки с DNS: если узел имени атакуют или взламывают, это может привести к катастрофическим последствиям в системе. Поэтому эффективность DNS в облачных вычислениях и его действенность - это ключ к успеху в информационной безопасности. Усиление защиты доменного имени является критически важным.
- Быстрое восстановление блоков данных и контроль за правом чтения / записи: узел данных (DataNode) - это узел накопления данных, где возможны проблемы и трудности с доступом к

данным. Также необходимо учитывать и другие возможности, а именно: контроль доступа, шифрование файлов и тому подобное.

Вся процедура защиты данных построена на конфиденциальности, целостности и доступности. Конфиденциальность относится к так называемой скрытой функции фактических данных или информации и является одной из самых жестких требований информационной безопасности. В случае облачных вычислений данные накапливаются в центрах обработки данных, где безопасность и конфиденциальность данных еще важнее. Целостность данных в любом виде не играет значительной роли для гарантии несанкционированного удаления, изменения или повреждения. Доступность данных означает, что пользователи могут использовать данные за счет использования потенциальных возможностей облачных технологий [6, с.97].

По мнению автора, наиболее актуальной и действенной является модель защиты данных, в которой используется трехслойная защитная структура системы, каждый слой которой выполняет свои собственные задачи для обеспечения защиты данных на всех уровнях «облака». Первый слой отвечает за аутентификацию пользователей цифровых сертификатов, выданных соответствующими органами; управляет кодами доступа пользователей. Второй слой ответственный за шифрование данных пользователя, а также защиту конфиденциальности пользователей определенным образом. Третий слой - использование данных пользователя для быстрого восстановления. Защита всей системы – это последний уровень данных.

С помощью трехуровневой структуры аутентификация пользователя обеспечивается целостность данных. Если в системе аутентификации пользователя состоялось нелегальное вмешательство и опасный пользователь входит в систему, шифрование файлов и конфиденциальность могут обеспечить следующий уровень защиты. На этом уровне данные пользователя зашифровываются в случае, если ключ доступа был введен нелегально. Из-за функции защиты конфиденциальности опасный пользователь не сможет получить полный доступ к информации, что очень важно для защиты коммерческих тайн деловых пользователей в среде облачных вычислений.

Наконец, быстрое восстановление слоя файлов с помощью алгоритма восстановления позволяет данным пользователя быстро восстанавливаться даже в случае больших повреждений.

Переход к облачным технологиям требует повышения требований к качеству предоставления услуг доступа в Интернет, которые становятся критически важными. Больше всего в этом вопросе развились американские провайдеры. В американской практике принято публиковать в открытом виде детализированные обязательства по соблюдению качества предоставления услуг, которые прописаны в соглашениях об уровне обслуживания (Service Level Agreements) [11]. В случае, если оператор не выполняет своих обязательств, он несет за это финансовую ответственность.

Вопрос информационной безопасности технологии облачных вычислений требует значительного совершенствования, а во многих аспектах – первоочередных необходимых разработок и наработок. Во всей совокупности преимуществ, которые предоставляет использование облачных вычислений, возникает множество вопросов безопасности, которые на сегодня недостаточно хорошо проанализированы и находятся еще на стадии обсуждения.

Список литературы:

1. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ.
2. Беккер М.Я., Гатчин Ю.А., Кармановский Н.С., Терентьев А.О., Федоров Д.Ю. Информационная безопасность при облачных вычислениях: проблемы и перспективы //

Научно-технический вестник информационных технологий, механики и оптики. – 2011. – № 1 (71). – С. 97–102.

3. Белов Е. Б. Основы информационной безопасности: учеб. пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия-Телеком, 2006. – 544 с.

4. Климентьев И. П. Введение в Облачные вычисления / И. Климентьев, В. Устинов. – М.: УГУ, 2009. – 233 с.

5. Куликов Р.Д. Методы повышения информационной безопасности в системах облачных вычислений // Современное состояние естественных и технических наук. – 2016. – № 23. – С. 9–12.

6. Митрошина Е.В. Исследование угроз безопасности облачных вычислений // E-Scio. – 2017. – № 1 (4). – С. 96–99.

7. Николаев Д.Д., Гатчин Ю.А. Модель безопасности процесса обработки данных в среде облачных вычислений // Национальная Ассоциация Ученых. – 2015. – № 4-2 (9). – С. 146–148.

8. Чемёркин Ю.С. Разработка нормативного подхода к управлению безопасностью сред облачных вычислений // Т-Comm: Телекоммуникации и транспорт. – 2014. – Т. 8, № 5. – С. 63–68.

9. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ФОРУМ, 2013. – 416 с.

10. Харатишвили Д. Дата-центры в цифрах и фактах // КомпьютерПресс – [Электронный ресурс] – Режим доступа: <http://compress.ru/article.aspx?id=20687> (Дата обращения: 17.06.17).

11. Mell P. The NIST Definition of Cloud Computing (Special Publication 800-145): Recommendations of the National Institute of Standards and Technology. – September 2011. – 7 p. – [Электронный ресурс] – Режим доступа: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (Дата обращения: 17.06.17).