

*Никифорова Анна Андреевна, студентка 3 курса экономического факультета
ФГБОУ ВО МГУ им. Н. П. Огарёва, г. Саранск, Россия*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Аннотация: применение и широкое распространение информационных технологий подразумевает использование сети Интернет, как основного средства манипулирования данными и информацией. С процессом развития и применения информационных технологий в повседневной жизни встал вопрос о применении «облачных вычислений» и их информационной защите.

Ключевые слова: облачные вычисления, облако, информационная безопасность, информационные технологии, системы, хранилище данных, информация, данные.

Annotation: The use and widespread dissemination of information technologies implies the use of the Internet as the main means of manipulating data and information. With the process of development and application of information technologies in everyday life, the question arose about the use of "cloud computing" and their information protection.

Keywords: cloud computing, cloud, information security, information technology, systems, data storage, information, data.

На рынке информационных технологий определение «облачные вычисления» появилось недавно. В 2002 году компания Amazon впервые запустила свой «облачный» сервис, затем компания Google подхватила идею и разработала свое «облако». Сегодня у каждого информационного гиганта

существует «облако»: Mega, Google Диск, Яндекс.Диск, iCloud, Dropbox, OneDrive.

Облачные вычисления (англ. cloud computing) – модель обеспечения удобного сетевого доступа по требованию к некоторому общему фонду конфигурируемых вычислительных ресурсов, которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру. Облако – пространство обращения, являющееся совокупностью аппаратных узлов компьютерной сети. При работе с облаком и облачным вычислением пользователя не интересует «как добраться и воспользоваться данными», потому что технология облачных вычислений не предполагает наличия специализированного программного обеспечения.

Технология облачных вычислений в условиях информатизации общества является услугой. Сегодня выделяют облачные вычисления:

- IaaS (Infrastructure as a Service) – инфраструктура как услуга.
- PaaS (Platform as a Service) – платформа как услуга;
- DaaS (Data as a Service) – данные как услуга;
- SaaS (Software as a Service) – ПО как услуга;
- WaaS (Workplace as a Service) – рабочее место как услуга;
- AaaS (All as a Service) – всё как услуга.

Наибольшую популярность имеют технологии облачных вычислений IaaS, PaaS, SaaS.

IaaS «избавляет предприятия от необходимости поддержки сложных инфраструктур центров обработки данных, клиентских и сетевых инфраструктур, позволяет уменьшить связанные капитальные затраты и текущие расходы. Можно получить дополнительную экономию при предоставлении услуги в рамках инфраструктуры совместного использования» [1, с. 9].

Платформа разработки приложений как услуги является облачным пространством работы с Web-приложениями, обеспечивая безопасность, масштабируемость, универсальность, устойчивость разрабатываемых приложений.

SaaS является услугой предоставления клиенту по его требованию приложение с использованием сети Интернет. При работе с SaaS конечный пользователь имеет дело с «тонким» клиентом.

Направление быстроразвивающегося информационного и цифрового общества ставит под сомнение вопрос безопасности работы с «облачными» вычислениями.

При предоставлении услуг поставщик и конечный пользователь заинтересованы в безопасности передаваемых и получаемых данных. При разграничении доступа к данным, ПО, инфраструктуре поставщик руководствуется классами облаков:

- частное («внутреннее») облако – применяется для отдельных круг лиц, имеющих общую цель в работе с облачными вычислениями. В данном случае серверы, сети, инфраструктуры и данные хранятся в отдельном облаке. «В частном облаке организация создает среду виртуализации на своих собственных серверах, которые расположены в центрах обработки данных, принадлежащих самой этой организации или сервис-провайдеру управляемых услуг» [2, с. 36];

- публичное облако – работать в облаке может клиент, имеющий доступ к сети Интернет по запросу и без;

- гибридное облако – любой из таких «облаков» сочетает программное обеспечение, данные, инфраструктуру, приложения как для ограниченного круга лиц, так и для всех.

Вопросы безопасности работы с облачными вычислениями является разделом компьютерной и информационной безопасности. Ключевыми элементами защиты данных являются: аутентификация, идентификация (IAM), авторизация пользователя, контроль доступа, соблюдение нормативно-правовых требований, а также конфиденциальность, целостность, доступность.

При осуществлении информационной безопасности в облаке применяют способ изолированного доступа к данным (Brokered Cloud Storage Access). Подход подразумевает, что доступ к данным могут получить только люди, прошедшие аутентификацию в качестве клиента сервиса и владельца этих

данных. Здесь необходимо тщательно разграничивать начало и конец правовой ответственности поставщика и клиента.

При работе с информационной защитой «облаков» используют принципы многоуровневой архитектурной безопасности углубленной защиты (Defense-in-Depth) рисунок 1.



Рисунок 1 – Безопасность облачных вычислений

В технологии IaaS информационная безопасность поставщика включает в себя: вычислительные и сетевые ресурсы, а также ресурсы хранения данных. Клиент в таких системах отвечает за приложения и данные, ПО, ОС.

В платформе разработки приложений как услуги независимо от класса облака поставщик координирует сетевые, вычислительные ресурсы, ресурсы хранения данных и часть клиентского наблюдения ПО и ОС. Для клиента остается обеспечение информационной безопасности данных и приложений.

В технологиях SaaS руководствующим лицом по обеспечению санкционированного доступа отвечает только поставщик.

Практическим способам применения информационной безопасности в облаках стоит уделить внимание группе безопасности Amazon EC2. Принцип сервиса – виртуализация облака, технология, создающая уровень абстракции между аппаратной частью компьютеров и выполняемыми на них программами. С помощью такого абстрактного уровня можно поделить один физический компьютер на несколько логических и запустить на последних несколько операционных систем одновременно [1, с. 13].

EC2 как эффективное средство практической реализации информационной безопасности облака обладает преимуществами:

- раздельное использование IP-адресов;
- экземпляры безопасности, находящиеся в одной группе EC2 не имеют возможности взаимодействия друг с другом;
- после запуска элемента невозможно изменить его членство в группе безопасности;
- защита трафика.

Помимо использования существующих методик защиты возможно использовать самостоятельные средства: создание собственных ключей, алгоритмов, протоколов.

При работе с «облаками» важной задачей является использование шифрования. В облачной среде данные, с которыми работает клиент, находятся в виртуальных хранилищах. Доступ к этим данным может быть ограниченным и свободным для всех пользователей сети Интернет. При обеспечении ограниченного доступа узкому или специализированному кругу лиц необходимо осуществлять шифрование Web-трафика и сетевого трафика. Современным способом собственного шифрования онлайн сервиса и облачных вычислений является использование HTTPS протокола и загрузки на него собственных сертификатов безопасности. При таком подходе клиент точно удостоверен, что работает с проверенным хранилищем.

При работе с большими данными и БД также существует необходимость их шифрования алгоритмами. Защита целостности кода с помощью PGP (Pretty

Good Privacy). Использование данного алгоритма может осуществляться возможностями открытого и закрытого ключа. Процесс шифрования репозитория состоит из:

- создание текущего ключа (сеанса);
- шифрование данных с использованием текущего ключа;
- шифрование текущего ключа;
- отправления данных и сеансового ключа.

При использовании алгоритма Pretty Good Privacy необходимо позаботиться о передаче данных при помощи программного кода:

- Anna Nikiforova <anna.nikiforova@example.com> – без указания комментария о ключе;
- Anna Nik (obsolete 1024-bit key) <anna.nik@example.com> – с указанием комментария о зашифрованном ключе.

При использовании методов алгоритмизации, криптографии, информационной защиты данных в облачных вычислениях главным критерием является соответствие нормативно-правовым актам и законодательствам РФ, а также международным законам:

- PCI – закон о защите транзакционных операций в облаках;
- Директива Европейского парламента и Совета Европейского Союза от 15 декабря 1997 года об использовании персональных данных в сети Интернет;
- HIPAA – защита личных медицинских данных;

Таким образом, стоит отметить, что существует большое количество преимуществ работы «облаков» и облачных вычислений. Быстрота доступа к данным, оперативность работы с ними, экономия времени и памяти, возможность использования электронных архивов (хранилищ) данных и разграничение вопросов доступа – эффективные преимущества облаков.

Клиент имеет возможность безопасного использования облаков, посредством использования: публичного, частного или гибридного облака. Вопросы информационной безопасности в «облаках» между клиентами и владельцем остаются основной задачей кибер-защиты.

Среди современных методов обеспечения защиты на практике используются средства компании Amazon EC2. Одним из доступных и стандартных методов является применение шифрования (криптографии), алгоритмов на основе нормативно-правовых актов информационной защиты данных.

Наиболее простыми средствами защиты облаков являются операции по настройке резервного копирования данных, очистке ненужных документов, настройки идентификации доступа пользователям, отслеживание подключенных аккаунтов и IP-адресов клиентов.

Использование подходящих методов шифрования разделяет санкционированный доступ к данным от несанкционированного независимо от того, где располагаются репозитории, не подвергая важные данные риску или сводя этот риск к минимуму.

Библиографический список:

1. Королёва В. А. Инновационные технологии современного офиса (Облачные вычисления) учеб. пособие / В. А. Королёва; Санкт Петербургский филиал Нац. исслед. ун-та «Высшая школа экономики». – СПб.: Отдел оперативной полиграфии НИУ ВШЭ – Санкт-Петербург, 2012. – 88 с.

2. Риз Дж. Облачные вычисления / Дж. Риз: Пер. с англ. – СПб.: БХВ-Петербург, 2011. – 288 с.

3. Сидоров В. Computing уходит в небо, или что такое «облачные вычисления» [электронный ресурс] / В. Сидоров // <http://netler.ru/pc/cloud.htm> (дата обращения 10.05.2014).

4. Топровер О. Десять вопросов об облачных вычислениях / О. Топровер // Открытые системы. 2009. №16. С. 19-20.