Представлений аналіз поняття довіри в комп'ютерних, і зокрема в хмарних технологіях, як з точки зору клієнта, так і з точки зору постачальника послуг. Дана класифікація ситуацій, які вимагають довіри між клієнтом і постачальником хмарних послуг, та особливості формування довіри для кожної з них. Визначені основні чинники, що мають вплив на рівень довіри

Ключові слова: довіра, рівень довіри, хмара, хмарні технології, хмарні обчислення, сервіси, загрози інформації, сертифікація, безпека мережі, конфіденційність

Представлен анализ понятия доверия в компьютерных, и в частности в облачных технологиях, как с точки зрения клиента, так и с точки зрения поставщика услуг. Дана классификация ситуаций, которые требуют доверия между клиентом и поставщиком облачных услуг, и особенности формирования доверия для каждой из них. Определены основные факторы, оказывающие влияние на уровень доверия

Ключевые слова: доверие, уровень доверия, облако, облачные технологии, облачные вычисления, сервисы, угрозы информации, сертификация, безопасность сети, конфиденциальность

УДК 004.738.5

АНАЛИЗ ПРОБЛЕМ ДОВЕРИЯ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ

Т. Г. Белова
Кандидат технических наук, старший преподаватель*
E-mail: belovatat@bk.ru
И. А. Побеженко
Кандидат технических наук, старший преподаватель*
E-mail: irina_pob@ukr net
В. В. Побеженко
Заведующий лабораторией*
E-mail: vlad1603@mail.ru
*Кафедра информационных технологий
Харьковская государственная академия культуры
Бурсацкий спуск, 4, г. Харьков, Украина, 61000

1. Введение

Облачные технологии направлены на удовлетворение потребностей пользователей, нуждающихся в удаленной обработке данных. В настоящее время множество организаций и учебных заведений задумываются о переводе своих вычислительных мощностей в облака, но основным сдерживаемым фактором при принятии такого рода решения является вопрос доверия провайдеру соответствующих услуг. Эта проблема обсуждается во многих странах, но оптимальное решение до сих пор не найдено.

Согласно исследованиям компании Wisegate, 53% опрошенных специалистов по информационным технологиям, представляющих различные сферы деятельности, охарактеризовали перспективы использования облачных технологий как опасные. Такой большой процент негативного отношения связан с наличием существенных рисков, имеющих место при проведении вычислений в облаке. Защита информации является ключевым вопросом в эффективном ведении бизнеса, поэтому необходимо учитывать потенциальные угрозы информации, а использование облачных технологий влечет за собой целый ряд проблем. Пока не будет создана эффективная схема использования подобных технологий, об их внедрении не может идти и речи.

Всего 16 % опрошенных отметили, что планируют применять облачные технологии, но лишь при условии, что будут заключены соответствующие соглашения и договора с теми, кто эти услуги будет предоставлять. Также некоторые специалисты в ходе исследования отметили, что им запрещается использовать данные решения в соответствии не только с отраслевыми, но и с государственными нормами.

Поэтому вопрос повышения доверия пользователей к облачным технологиям, а в частности, к их провайдерам, является актуальным.

2. Постановка задачи и обзор литературы

Практика использования облачных вычислений показывает ряд проблем, в частности безопасности, правовых и нормативных требований, а также организационных [1, 2, 3, 4]. Наряду с ними встает проблема доверия между поставщиками и потребителями услуг.

Доверие остается решающим фактором при миграции в облако, проблема безопасности требует наиболее пристального внимания. Это связано с тем, что "безопасность есть и чувство, и реальность. И это не одно и тоже."[5]. В реальности безопасность связана с вероятностью различных рисков и показывает, насколько эффективны стратегии по смягчению возможных рисков. Безопасность является чувством, которое основано на психологических реакциях на риски и контрмеры. Поставщикам облачных вычислений необходимо учитывать и чувства потенциальных клиентов, и реальность рисков, с ними связанных, так, чтобы клиенты при использовании облачных вычислений чувствовали себя комфортно и безопасно.

В литературе отмечаются случаи отключения облака, которые приводили к сбоям в работе клиентов, что в свою очередь вело к снижению доверия к облачным технологиям. 13 марта 2009 у компании Microsoft произошел сбой системы, который длился шесть дней

и привел к потерям клиентских данных. Другим примером является сбой Google Gmail 16 октября 2008 года – отключение пострадавшим клиентам Google Apps в результате отказа в доступе приложений, таких как сообщения электронной почты [6]. В 2010 году произошло отключение salesforce.com, когда сервис для всех клиентов (68000 респондентов) был недоступен, но не было никаких сообщений о потере данных [7].

Прежде всего, для обеспечения доверия облачные технологии должны быть в состоянии решать различные задачи, которые возникают при облачных вычислениях. Это означает, что модель доверия должна учитывать многочисленные проблемы, возникающие в любых моделях развертывания и доставки, а также обеспечить оптимальный способ оценки доверия для потребителей и поставщиков услуг. Существует ряд моделей, направленные на укрепление доверия между клиентами и поставщиками облачных услуг, но ни одна из них не получила широкого распространения из-за сложности учета большого числа факторов.

3. Цель и задачи исследования

Цель данного исследования – проанализировать определение доверия и доверия в компьютерных, а в частности в облачных технологиях.

Задачами исследования является анализ понятия доверия, выявление основных сценариев доверительных ситуаций, возникающих между поставщиком услуг и клиентом и возможности возникновения ситуационных рисков, а также раскрытие основных факторов, оказывающих влияние на формирование доверия.

4. Формирование понятия доверия в компьютерных системах

Доверие напрямую зависит от безопасности информационной системы и информации, находящейся в ней. Джон Чемберс, председатель и главный исполнительный директор CISCO Systems, отмечает: " безопасность облачных технологий – это кошмар, который не может быть решен традиционными способами" [8]. Это утверждение перекликается с "чувствами и реальностью безопасности" [5]. Сложность облачных вычислений делает вопрос безопасности первостепенным для потенциальных клиентов и поставщиков услуг. Клиенты думают о безопасности своих данных и приложений в первую очередь так, как понимают их уязвимость от потенциальных атак, ведь облако в действительности является открытым. Вместе с чувством реальности и безопасности поднимают вопрос о конфиденциальности в использовании услуг облачных вычислений.

Оценка уровня доверия – задача сложная и нетривиальная, требующая учета целого ряда факторов, в большинстве своем плохо поддающихся количественной оценке. Уровень доверия зависит от того, как поставщики облачных услуг учитывают чувства потенциального клиента, а также настолько эффективно предотвращают реальность угроз безопасности и решают другие проблемы внедрения облачных вычислений. Организации, доверяя свои данные облачным сервисам, будут обращаться к провайдерам, которые, как они считают, заслуживают доверия.

"Доверие является результатом действий, производимых человеком каждый день на протяжении жизни, однако, термин доверие пострадало от несовершенного понимания (множества определений) и неформального использования в литературе и в повседневной жизни" [9]. В [10] доверие определено как "субъективная вероятность, с помощью которой человек ждет, что другой человек выполняет некое действие, от которого зависит его благополучие". Другое определение дано в [12], авторы определяют доверие как «степень, в которой одна сторона готова зависеть от кого-то или чего-то в данной ситуации с чувством относительной безопасности, несмотря на возможность негативных последствий". Это определение несет в себе понятие рационального принятия решений в вопросе доверия третьему лицу. В [9] автор определяет доверие как "намеренную постановку себя в зависимость от другого лица, и лишь его действия влияют на то, как вы будите себя чувствовать по окончании работы с ним".

Доверие не предназначено, само по себе, гарантировать права и страховую защиту в случае возникновения проблем, но оно также не исключает возможности соглашения [11]. Обзор этих определений и характер облачных вычислений приводит к выводу о концепции доверия, которая раскрывает доверие как готовность клиента зависеть от поставщика услуг с чувством безопасности, учитывая, что поставщик услуг прозрачно раскрывает потенциальные риски и смягчает последствия планов, которые используются для перехода в облака.

5. Ситуации, требующие доверия к облачным вычислениям

Для повышения уровня доверия со стороны потенциальных клиентов к облачным вычислениям следует рассмотреть различные ситуации или случаи, которые могут возникнуть при обращении к соответствующего рода услугам. Как сказано в [13], "решение о доверии основано на многих вещах, таких как склонность доверителя к доверию, его вера и прошлый опыт, связанный с тем, кому доверяют". Таким образом, степень требуемого доверия у каждого клиента зависит от различных ситуаций и может отличаться, но эти различные ситуации являются неотъемлемой частью для построения доверительных отношений при принятии облачных вычислений. Классификация уровней доверия для принятия облачных вычислений включает в себя пять ситуаций [13].

Первая ситуация связана с доступом к ресурсам или «доступ к ресурсу доверителя». Например, когда клиент делегирует администраторам поставщика услуг управление своими ресурсами, размещенными в инфраструктуре облачных услуг. В этом случае доверие оказывается с целью доступа к ресурсам в собственности или под ответственность доверителя, а доверитель позволяет использовать свои ресурсы в полном объеме. Здесь доверие связано с вопросами контроля и управления доступом, которые являются основной темой компьютерной безопасности. Таким образом, доверие является основой для формирования политики авторизации. В облачных вычислениях укрепления доверия имеет решающее зна-

чение, учитывая характер облачной вычислительной среды. Необходимо доказать, что поставщику облачных услуг можно доверять в таких вопросах, как надежность хранения информации и предотвращение возможности инсайдерских атак [14]. Без таких доказательств доверие между поставщиком и клиентом не может быть установлено.

Другим сценарием является предоставление услуг. В [13] такая ситуация называется предоставлением услуг по доверию, а в [11] – обеспечение доверия, в [15] – бизнес-доверие. В этом случае клиент возлагает свое доверие на поставщика услуг. Это предоставление услуг не связано с доступом к ресурсам доверителя [15, 13]. Данные и приложения могут находится в инфраструктуре сервис-провайдера, который поручает доступ администраторам поставщика услуг для достижения оптимальной производительности инфраструктуры. В среде облачных вычислений это доверие относится к требованиям клиента о защите от предполагаемой угрозы и/или нападения. Для того, чтобы предотвратить такие ситуации в облачных вычислениях, поставщики услуг должны поддерживать соглашения об уровне обслуживания (SLA) с клиентами и другими типами контрактов, которые представляют интерес для клиентов. Этот сценарий требует, чтобы клиент доверял вычислительной среде осуществлять облачные вычисления.

Сертификация попечителей [13], или удостоверение доверия [11], или аутентификация доверия [15] – еще один случай, требующий доверия в облачных вычислениях. При таком сценарии клиент должен быть уверен, что сервис-провайдер является именно тем, кем есть на самом деле. Он основан на сертификации третьей стороной, называемой опекуном [13]. Существуют разные системы, которые возникают от доверия на основе тождества [17], такие как PGP и X.509 [16]. С отсутствием сертификации и стандартов, регулирующих облачные вычисления, реализовать этот тип доверия невозможно. Таким образом, провайдерам облачных сервисов необходимо известить клиентов о типе услуг, которые они предлагают, и что они могут предоставить заявленные услуги, а также что они являются теми, за кого себя выдают.

Делегирование доверия возникает, когда клиент делегирует поставщику услуг совершение действий от своего имени. Поставщик услуг принимает решения от имени клиента на ресурсы, какими клиент владеет или контролирует [13]. В облачных вычислениях это означает, что поставщик услуг выполняет аудит безопасности и обнаружение атак от имени клиента. В [13] авторы видят этот тип доверия, как ”доверительное принятие решений службой”. Таким образом, это требует облачных вычислительных услуг по разработке механизмов, обеспечивающих клиентов всем необходимым в таких вопросах, как сбор доказательств в суде. А также соответствие законам о защите данных, другим правилам и стандартам безопасности, юридическое подтверждение способности действовать от имени клиентов.

Последний сценарий требует доверия в случае инфраструктуры доверия. Этот сценарий описывает, в какой степени доверительные стороны считают, что необходимые системы и организации действуют в целях поддержки операций и обеспечения безопасности сети [11]. Такое доверие также известно как контекст доверия [11] и система доверия [12]. Это доверие имеет дело с инфраструктурой, при которой доверителю должны прежде всего доверять [13].

В облачных вычислениях поставщики должны работать вместе с клиентом в направлении создания доверия через сотрудничество в разработке и настройке политики безопасности, договоров и соглашений об уровне обслуживания, в вопросах законодательства и соответствия стандартам.

Доверие как характеристика качества отношений между клиентом и поставщиком требует балансировки между ответственностью и старанием. Оно должно быть нацелено на содействие уверенности, что что-то будет или не будет происходить при обещании со стороны поставщика услуг. В соответствии с рассмотренными выше ситуациями, доверие можно рассматривать как два способа отношений [16], имеющее ряд особенностей и качеств [11, 13].

6. Выводы

Таким образом, для обеспечения конфиденциальности и доверия пользователей к облачным вычислениям необходимо повышение безопасности данных как со стороны клиента, так и со стороны поставщика услуг. Любая из рассмотренных ситуаций требует доверия к поставщику услуг, но, на наш взгляд, из всех выявленных наиболее подверженной риску является ситуация, когда клиент делегирует поставщику услуг принятие решений от своего имени. В этом случае речь идет о стопроцентном доверии поставщику услуг.

Повышение доверия между поставщиками услуг облачных вычислений и их клиентами снижают риски, которые могут возникнуть при нарушениях соглашений. Следует отметить, что существенную роль в безопасности данных в облачных вычислениях играет уровень культуры пользователя и контроль сотрудников компаний, предоставляющих услуги облачных технологий, а также повышение влияния государства на компании, предоставляющие услуги, на законодательном уровне.

Литература

1. Andrei, T. Cloud computing challenges and related security issues [Электронный ресурс] / T. Andrei, 2009.
2. Buyya, R. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities [Электронный ресурс] / R. Buyya, C. S. Yeo, S. Venugopal. // In: Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, Keynote Paper, 2008.
3. Catteddu, D. Cloud Computing Information Assurance Framework [Электронный ресурс] / D. Catteddu, G. Hogben // European Network and Information Security Agency (ENISA), 2008.

4. Khajeh-Hosseini, A. Research challenges for Enterprise Cloud Computing. [Электронный ресурс] / A. Khajeh-Hosseini, I. Sommerville and I. Sriram. 2010.
5. Schneir, B. The Psychology of Security. [Электронный ресурс] / B. Schneir, 2008.
6. Williams, A. Top 5 Cloud Outages of the Past Two Years: Lessons Learned [Электронный ресурс] / A. Williams // Lessons Learned; ReadWriteWeb, 2010.
7. Bigelow, S. J. Pro and Cons of Moving to the Cloud [Электронный ресурс] / S. J. Bigelow // Virtual Data Center, 2010.
8. Greene, T. Cloud security stokes concerns at RSA [Электронный ресурс] / T. Greene // Network World, 2009.
9. Marsh, S. P. Formalising Trust as a Computational Concept [Электронный ресурс] / S.P. Marsh // Computing Science and Mathematics, 1994.
10. Gambetta, D. Can We Trust Trust? [Электронный ресурс] / D. Gambetta, // Trust: Making and Breaking Cooperative Relations, 2000.
11. Audun, J., A survey of trust and reputation systems for online service provision. [Электронный ресурс] / J. Audun, Sang, et al. // Decis. Support Syst, 2007.
12. Mcknight, D. H. The meanings of trust. [Электронный ресурс] / D. H. Mcknight & N. L. Chervany // Trust in CyberSocieties-LNAI, 1996.
13. Grandison, T. A survey of trust in internet applications. [Электронный ресурс] / T. Grandison & M. Sloman // IEEE Communications Surveys and Tutorials, 1996.
14. Santos, N. Towards Trusted Cloud Computing. [Электронный ресурс] / N. Santos, K. P. Gummadi et al. // Max Planc Institute for Software Systems, 2009.
15. Boeyen, S. Liberty Trust Models Guidelines.[Электронный ресурс] / S. Boeyen, G. Ellison et al. // Liberty Alliance Project, 2003.
16. Andert, D. Trust Modeling for Security Architecture. / D. Andert, R. Wakefield, et al. // Santa Clara, CA, Sun Microsystems INC, 2002.

У статті досліджено питання використання найсучасніших технічних та організаційних методів у процесі організації ефективної інформаційної взаємодії вищих навчальних закладів із суспільством за допомогою мережі Інтернет.

Проаналізовано та запропоновано формальний опис видів інформаційної діяльності ВНЗ, який дозволяє систематизувати інформаційну діяльність ВНЗ у глобальному інформаційному просторі, прогнозувати розвиток галузі та освітніх потреб

Ключові слова: Інтернет, соціальні комунікації, вищий навчальний заклад, інформаційна діяльність, моделювання процесів

В статье исследованы вопросы использования современных технических и организационных методов в процессе организации эффективного информационного взаимодействия высших учебных заведений с обществом посредством сети Интернет.

Проанализировано и предложено формальное описание основных видов информационной деятельности ВУЗов для систематизации информационной деятельности ВУЗа в глобальном информационном пространстве и прогнозирования развития отрасли и образовательных нужд

Ключевые слова: Интернет, социальные коммуникации, высшее учебное заведение, информационная деятельность, моделирование процессов

УДК 004.738.5

АНАЛІЗ СУЧАСНИХ ВИДІВ ТА МЕТОДІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВНЗ В ІНТЕРНЕТІ

Р. О. Корж
Кандидат технічних наук, доцент
Кафедра електронних засобів інформаційно-комп'ютерних технологій
Національний університет «Львівська політехніка»
вул. Бандери 12, м. Львів, Україна, 79013
E-mail: korzh@lp.edu.ua

А. М. Пелещишин
Доктор технічних наук, професор
Кафедра соціальних комунікацій та інформаційної діяльності
вул. Бандери 12, м. Львів, Україна, 79013
E-mail: apele@ridne.net

1. Вступ

Ефективність інформаційної діяльності, як однієї з форм взаємодії організації з суспільством, є важливим елементом досягнення цілей, що поставлені перед організацією. Серед інших форм діяльності організації, інформаційна діяльність є найбільш вимогливою до необхідності врахування технічного прогресу та соціальних трендів. Саме тому одним із ключових факторів успішної інформаційної діяльності сьогодні стало