

# КАЧЕСТВО И ИННОВАЦИИ ОБРАЗОВАНИЕ

№6  
2013

ISSN 1999-513X  
  
9 771999 513000



КАЧЕСТВО и ИПИ (CALS)-технологии

w w w . q u a l i t y - j o u r n a l . r u



А.В. Нижегородов, А.С. Кабанов, В.Н. Азаров

# ОБЛАЧНЫЕ ТЕХНОЛОГИИ И ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В статье рассмотрены вопросы доступности информационных ресурсов при использовании облачных технологий. Проведен анализ проблем использования облачных технологий. Отражены основные особенности использования облачных технологий в государственном секторе.

**Ключевые слова:** облачные технологии, доступность информационных ресурсов, информационная безопасность

**Ш**ирокое внедрение облачных технологий наблюдается относительно недавно. При этом большая часть технологий, используемых в облачных сервисах, таких как WEB, распределенная обработка данных и др. существуют уже несколько десятков лет. Облачным вычислениям свойственны практически все угрозы безопасности, характерные для используемых ими технологий. Следует отметить, что зависимость от атак, в том числе и через Интернет, растет с каждым днем, а вместе с этим увеличиваются потенциальные возможности мошенников и преступников. Ежедневно выявляются около 260000 фрагментов вредоносных кодов, причем за три года были раскрыты только 50000 таких преступлений [1]. При этом информация становится одним из наиболее важных ресурсов, необходимых для анализа, прогнозирования и принятия решений. Доступность информации легитимным пользователям является одним из ключевых факторов, она является одной из трех главных составляющих информационной безопасности (ИБ), помимо ее конфиденциальности и целостности. Обеспечение доступности в условиях техносферных воздействий приобретает большое значение, особенно при использовании облачных технологий [2]. Ниже приведен краткий обзор облачных технологий с точки зрения ИБ.

Помимо таких достоинств, как отказоустойчивость, экономичность и гибкость, данные технологии открывают новый пласт проблем, связанных с ИБ. Доступность позиционируется организациями, оказывающими услуги по предоставлению облачных сервисов, как одно из главных достоинств данных систем. Следует отметить, что данный тезис спорен. Причин этому достаточно, начиная с того, как следует понимать указанный термин:

- как экономическую составляющую доступности (например, низкая стоимость);
  - как доступность информации легитимным пользователям (составляющая ИБ) и др.

Многие организации оценивают экономическую эффективность перехода на облачные технологии как очень 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 по предоставлению 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 РФ соглашения об уровне предоставления услуг и качества обслуживания являются нерешенными вопросами, что определяет ряд соответствующих проблем. Из этих проблем можно выделить: пропускную способность беспроводных каналов, вопрос последней мили на пути от клиента к облаку, использование шифровальных средств, включая криптографические средства обеспечения подлинности информации и др.

Кроме этого, дополнительно необходим анализ центров обработки данных (ЦОД), сетевых устройств, подключаемых к облачным сервисам, нормативно-правовой базы по применению облачных технологий и др. [3, 4]. По мнению ряда экспертов, отсутствие надежных ЦОД является одним из решающих факторов отказа от использования облачных технологий. Касательно вопросов защиты информации в ЦОД, помимо программного обеспечения, важной составляющей является человеческий фактор. Персонал, обслуживающий ЦОД, должен иметь соответствующий уровень подготовки по вопросам ИБ, 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 ИБ облачных технологий, но необходимость разработки унифицированных стандартов в этой области является ключевым моментом. Это связано с тем, что данные технологии составляют новое направление развития в IT-индустрии, и существует множество компаний-разработчиков, которые используют

различные подходы к обеспечению ИБ.

Важным является вопрос использования облачных технологий в государственных инфраструктурах РФ. В настоящее время касательно этого 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 этого, немаловажен факт территориального расположения удаленных облачных сервисов, на которых происходит обработка и хранение данных. На сегодняшний день мировые лидеры по предоставлению облачных сервисов, такие как Amazon, CitrixSystems, Google, Microsoft и др. используют данные центры, расположенные на территории США и Западной Европы. Спецслужбы США могут получить доступ к информации, расположенной в данных центрах, в соответствии с законодательной базой [5]. Все это приводит к невозможности использования облачных сервисов зарубежных компаний из соображений национальной безопасности.

Второе мнение, к которому присоединяются авторы, базируется на том, что в ближайшее время внедрение облачных технологий коснется и государственных инфраструктур РФ. Здесь можно провести аналогию с использованием сети Интернет: достоинств от ее использования больше, чем недостатков, таких как возможность нарушения ИБ и др. В настоящее время большинство государственных структур не имеют межведомственного электронного взаимодействия, используемое оборудование устарело, не имеется единой базы данных документов. Одним из направлений решения накопившихся проблем, согласно [6], является планирование, создание и использование информационно-коммуникационных технологий в деятельности государственных органов, а также внедрение систем электронного документооборота и организация архивов. При этом, цель не столько в оптимизации внутренней работы ведомств, сколько в удовлетворении требований, предъявляемых к системам в рамках межведомственного электронного документооборота и систем межведомственного электронного взаимодействия [7].

Вескими аргументами использования облачных технологий в госсекторе РФ 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 СИО 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 госучреждениям

провести оценку альтернативных вариантов облачных вычислений по основным инвестициям в информационные технологии. В 2013 году все инвестиции в информационные технологии в постоянном режиме должны анализироваться с точки зрения облачных вычислений [8].

На наш взгляд, решением проблемы безопасного внедрения облачных технологий в государственных инфраструктурах РФ является создание частных облаков (privatecloud). 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. Таким образом, необходимость развития систем защиты информации при использовании облачных технологий является актуальной проблемой. Её решение имеет большое значение для общества, правительства, силовых структур, промышленности и научных кругов РФ.

#### **Литература:**

- 1.JemesLyne. Frontline. - Режим доступа: <http://www.ru.euronews.com/2013/01/16/fighting-cybercrime-in-europe>.
- 2.Стародубцев Ю.И., Бухарин В.В., Семенов С.С. Техносферная война // Воен. мысль. 2012. № 7.
- 3.Облачные сервисы. Взгляд из России / Под ред. Е. Гребнева. - М.: CNews, 2011.
- 4.Сюруков И. Что мешает активному переходу заказчиков в России к "облачным" технологиям? Портал iBusiness. - Режим доступа: <http://i-business.ru/blogs/11529>.
- 5.Thompson B. Storm warning for cloud computing. - Режим доступа: <http://www.news.bbc.co.uk/2/hi/technology/7421099.stm>.
- 6.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>.
- 7.Смирнов Н. Директор информационной службы. №10, 2012. - Режим доступа: [http://www.mfpa.ru/general/upload/contents\\_jurnal/direktor\\_informacion noi\\_slujby.doc](http://www.mfpa.ru/general/upload/contents_jurnal/direktor_informacion noi_slujby.doc).
- 8.Харламов А. Облачные вычисления для государственного и муниципального управления: решения от корпорации NEC. - Режим доступа: <http://www.iis.ru/docs/harlamov.pdf>.

**Нижегородов Антон Валентинович,**  
канд. техн. наук, докторант Военной академии  
связи им. С.М. Буденного.

**Кабанов Артём Сергеевич,**  
канд. техн. наук, доцент кафедры  
"Компьютерная безопасность" МИЭМ НИУ ВШЭ.  
e-mail: kabanov\_as@mail.ru

**Азаров Владимир Николаевич,**  
д.т.н., профессор,  
заместитель директора МИЭМ НИУ ВШЭ.

A.V. Nishegorodov, A.S. Kabanov, V.N. Azarov

## CLOUD TECHNOLOGIES AND ENSURING THE ACCESSIBILITY OF INFORMATION RESOURCES

The article considers the issues of accessibility when using cloud technologies. The analysis of the problems in using cloud technologies. Reflects the main features of use in the public sector.

**Keywords:** cloud technology, the availability of information resources, information security

### References:

- 1.JemesLyne. Frontline. - Mode of access: <http://www.ru.euronews.com/2013/01/16/fighting-cybercrime-in-europe>.
- 2.Starodubtsev Y.L., Bukharin V.V., Semenov S.S. Technosphere war // The Military thought. 2012. № 7.
- 3.Cloud based services. View from Russia / ed. E. Grebneva. - M.: CNews, 2011.
- 4.Coats And. What hinders the active transition of customers in Russia to the "cloud" technologies? Portal iBusiness. - Mode of access: <http://i-business.ru/blogs/11529>.
- 5.Thompson B. Storm warning for cloud computing. - Mode of access: <http://www.news.bbc.co.uk/2/hi/technology/7421099.stm>.
- 6.The decree of the Government of the Russian Federation dated April 25, 2012. № 394 // the Russian newspaper. - Mode of access: <http://www.rg.ru/2012/05/08/gosorgany-site-dok.html>.

7. Smirnov N. The Director of the information service. 2012. №10. - Mode of access: [http://www.mfpa.ru/general/upload/contents\\_journal/direktor\\_informacion noi\\_slujby.doc](http://www.mfpa.ru/general/upload/contents_journal/direktor_informacion noi_slujby.doc).

8.Kharlamov A. Cloud computing for the state and municipal management: solutions from NEC Corporation. - Mode of access: <http://www.iis.ru/docs/harlamov.pdf>.

**Nishegorodov Anton Valentinovich,**  
cand. of techn. science, doctoral student  
of the Military Academy of Communication.

**Kabanov Artem Sergeevich,**  
cand. of techn. sciences, associate Professor  
of the Department "Computer security"  
Higher School of Economics.  
e-mail: kabanov\_as@mail.ru

**Azarov Vladimir Nikolaevich,**  
dr.sci.tech., professor,  
deputy director of MIEM HSE.