УДК 303.732.4

МОДЕЛИРОВАНИЕ ОЦЕНКИ РИСКОВ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ИТ-СЕРВИСОВ

Разумников С.В.

ЮТИ ТПУ «Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета», Юрга, e-mail: demolove7@inbox.ru

Хотя за последние несколько лет «облачные» сервисы приобрели огромную популярность у предприятий за свои многочисленные выгоды, они не лишены рисков в таких областях, как безопасность, конфиденциальность данных и доступность данных. Стало очевидно, что необходимо единое мнение о методах оценки рисков облачных вычислений, но этого трудно добиться, поскольку в отрасли отсутствует единая, стандартная, структурированная платформа, которая могла бы помочь предприятиям в оценке и снижении рисков «облачных» вычислений. Существуют методы, позволяющие сделать систему безопасной изначально, вместо того чтобы полагаться на аттестаты безопасности, которые предлагает поставщик услуг облачных вычислений. В работе предложена функциональная SADT-модель оценки рисков облачных ИТ, а также критерий и показатели оценки. На основе предложенных показателей разработана аддитивная модель факторного анализа по оценке рисков применения облачных ИТ-сервисов.

Ключевые слова: методы, модели, оценка, риски, сервисы, облачные вычисления

MODELLING OF THE ASSESSMENT OF RISKS WHEN USING CLOUDY IT SERVICES

Razumnikov S.V.

Yurga Technological Institute (branch) of National research Tomsk Polytechnic University, Yurga, e-mail: demolove7@inbox.ru

Though for the last years «cloudy» services gained huge popularity at the enterprises for the numerous benefits, they aren't deprived of risks in such areas as safety, confidentiality of data and availability of data. It became obvious that the consensus about methods of an assessment of risks of cloud computing is necessary, but it is difficult to achieve it as in branch there is no uniform, standard, structured platform which could help the enterprises with an assessment and decrease in risks of «cloudy» calculations. There are the methods, allowing to make system safe initially instead of relying on safety certificates which are offered by service provider of cloud computing. We propose a functional SADT-risk model of cloud IT, as well as evaluation criteria and indicators. On the basis of the proposed indicators developed additive model of factor analysis to assess the risks of cloud IT services.

Keywords: methods, models, assessment, risks, services, cloud computing

В современном мире нельзя представить себе человека, который смог бы обойтись без использования информационных технологий. На всех уровнях управления имеется желание расширить свои информационные и коммуникационные возможности за счет внедрения современных информационных технологий. Преимущества, которыми обладают облачные вычисления – огромны, но только если удастся верно рассчитать риски при переходе к облачной модели, которые должны учитывать пользователи и поставщики. Сегодня все больше руководителей ИТ выбирают облачные вычисления. Суть облачных вычислений – в переходе к высоко стандартизированным наборам удобных сервисов и программного обеспечения, которые вместе составляют основу высокоэффективного использования ресурсов. Отсутствие достаточного количества серьезных исследований вопросов риска облачных вычислений, мешает многим организациям совершить переход к облачной модели [2, 5, 6, 7, 8]. Цель данной статьи – разработать подход к оценке рисков от применения облачных сервисов. Для достижения поставленной цели необходимо исследовать особенности применения облачных сервисов и проанализировать риски, которые могут возникнуть при переходе к ним.

Безопасность должна быть частью облачной системы, а не ее надстройкой. Необходимо рассматривать вопросы безопасности в самом начале развертывания облачной системы – на этапе планирования. Использование облачной структуры предполагает деление ее с большим числом людей, при этом имеется очень немного инструментов, делающих возможность контролировать то, как люди будут использовать этот общественный ресурс [1].

На сегодняшний момент существует несколько методик для оценки рисков от внедрения информационных технологий и созданные на основе их программные продукты. К ним относятся: риск-модель Octave, Cramm, Risk Watch. В случае использования частного облака эти модели могут быть использованы для управления риском с внесением ряда поправок. Однако если частное облако находится в собственности организации и физически существует внутри ее юрисдикции, то возможно абстрагироваться от идеи облака и считать

что фирма его не использует. При использовании частного облака, можно считать клиентом работников организации, а ее саму провайдером услуг [3]. Также они могут служить базисом для создания новой модели, способной удовлетворить возникшую потребность. Важно отметить, что ни одна из существующих моделей по оценке рисков информационных технологий полностью не подходит для случая облачных вычислений, т.к. ни в одной из них не учитываются специфика модели взаимодействия, присущая облачным средам. Эта специфика заключается в возможности удалённого доступа к предоставляемым сервисам. В связи с этим появляется необходимость рассматривать следующие возможные риски:

- неблагоприятные последствия неправильного управления данными;
- неоправданные расходы на обслуживание;
- финансовые или юридические проблемы поставщика;
- эксплуатационные проблемы или простои поставщика;
- проблемы восстановления данных и конфиденциальности;
- общие проблемы безопасности;
- атаки на систему извне.

Автором предлагается следующая аддитивная модель по оценке рисков применения облачных ИТ-сервисов на основе факторного анализа. Прежде чем приступить к выполнению расчета по модели оценки риска, необходимо выполнить следующие несколько шагов [1].

Шаг 1. Сегментация данных, исходя из их важности. Лаборатория реактивного движения (ЛРД) НАСА (NASA'S Jet Propulsion) Lab недавно начала собственные исследования облачных вычислений. Исследования проводились в сфере навигации среди данных с различным уровнем доступа и защищенности. Их команда отобразила исследования облачных систем в виде диаграммы, на которой нанесены различные наборы данных в соответствии с требованиями безопасности для каждого среза. Затем команда ЛРД начинала работать с информацией в соответствии с диаграммой – от общедоступных данных до секретных.

Шаг 2. Определить, как много информации необходимо защищать посредством аутсорсинга. Если изначально определить, какую часть данных мы хотим оставить на ресурсах хранения и какая их часть уйдет в облачную систему, процесс организации сохранности данных будет организован значительно лучше, чем у других. Разумеется, в этом случае часть ответственности за уровень безопасности данных ложится на сотрудников, которые непосредственно работают с этими ресурсами.

Если в фирме есть продвинутая команда по обеспечению безопасности – отлично, если нет – легко отдать эту задачу на аутсорсинг. Это деньги, которые действительно будут потрачены не зря. Оптимальным будет объединить эти два метода, включить в этот процесс сторонний аудит и ревизию кода. Поставщики облачных сервисов начинают осознавать, что наличие надежной системы безопасности – это хороший способ отличиться от прочих поставщиков, поскольку большинство из них и не задумываются о том, чтобы действительно защищать информацию, размещенную на их сервисах, от неавторизованного доступа. Для разрешения подобных ситуаций необходимо наладить диалог и понимание между поставщиком облачных услуг и отделом фирмы, который отвечает за управление рисками.

Шаг 3. Составить короткий список облачных поставщиков для оценки. Стоит оценивать поставщиков, исходя из общей точки зрения на их возможности, с оговоркой, что чем глубже отдел управления рисками попытается узнать инфраструктуру проверяемого поставщика, тем большую ответственность он может взять на себя перед организацией. И в то же время, если облачный поставщик не сможет предоставить соразмерного с потребностями фирмы уровня масштабирования, проблемы с безопасностью информации возникнут вне зависимости от изначальных обещаний поставщика.

Шаг 4. Написать подробную характеристику провайдера. Вот четыре основных критерия, характеризующие поставщиков:

1) безопасность: уверенность, что поставщик и субподрядчики будут соблюдать все применимые законы;

2) компенсация: как поставщик и его субподрядчики возместят фирме урон в случае утечек информации;

3) ответственность: ответственность поставщика в том, чтобы уведомить компанию об утечке информации и покрыть расходы по обозримым утечкам, согласно соответствующим законам, включая возможные претензии третьих сторон, возникающие вследствие утечки;

4) аудит: поставщикам, услуги которых относятся к наиболее подверженным рискам, необходимо проводить и оплачивать сторонние аудиторские проверки.

С помощью этого процесса можно опознать поставщиков услуги, которые создают слишком много рисков.

Шаг 5. Согласование контракта и особых условий. Язык стандартного контракта

и согласований об уровне обслуживания должен быть конкретным при описании ваших требований к безопасности. Имеет смысл научиться гнуть свою линию в переговорах с поставщиками, когда речь заходит о праве на собственность информации вплоть до того, что при разрыве отношений с поставщиком фирма получает все свои данные назад, даже если эти данные потребуется доставлять на дисках.

Шаг 6. Отслеживать показатели программы управления рисками поставщика и наблюдать за результатами аудитов фирм, поддерживающих его. Ряд фирм создали процесс, посвященный текущей оценке поставщиков. Они (фирмы) также должны заключать контракты со сторонними аудиторами, чтобы воспользоваться их услугами, как только потребуется.

Шаг 7. Запустить прототип с образами данных. Безопасность неразрывно связана с доступностью и надежностью. Функции безопасности, такие как сканирование, могут сами по себе снижать производительность – необходимо убедиться в том, что все системы безопасности на месте и работают во время тестов. Система должна пережить плохую производительность в любой момент, когда некий процесс может вызвать ее сбой или зависание. Необходимо обладать возможностью выхода системы из этих ошибок. Но выход из них может вызвать появление проблем в системе безопасности.

Хотя риск взлома присутствует всегда, реальный риск при передаче любой функции на аутсорсинг – будь то облачный сервис или нет – заключается в понимании уровня контроля, который был потерян, и к каким это может привести последствиям.

Шаг 8. Выполнение тестирования на проникновение. На этой заключительной стадии организация задействует своих внутренних экспертов или информационных консультантов, чтобы они произвели взлом системы, используя общедоступные инструменты. Эти консультанты также могут быть полезны в области устранения системных уязвимостей, которые они найдут [1].

На рис. 1 представлена спроектированная функциональная SADT-модель средствами BPwin. Эта модель представляет систему по оценке рисков в виде простейшей компоненты – один блок и дуги, которые изображают интерфейсы с функциями вне системы.

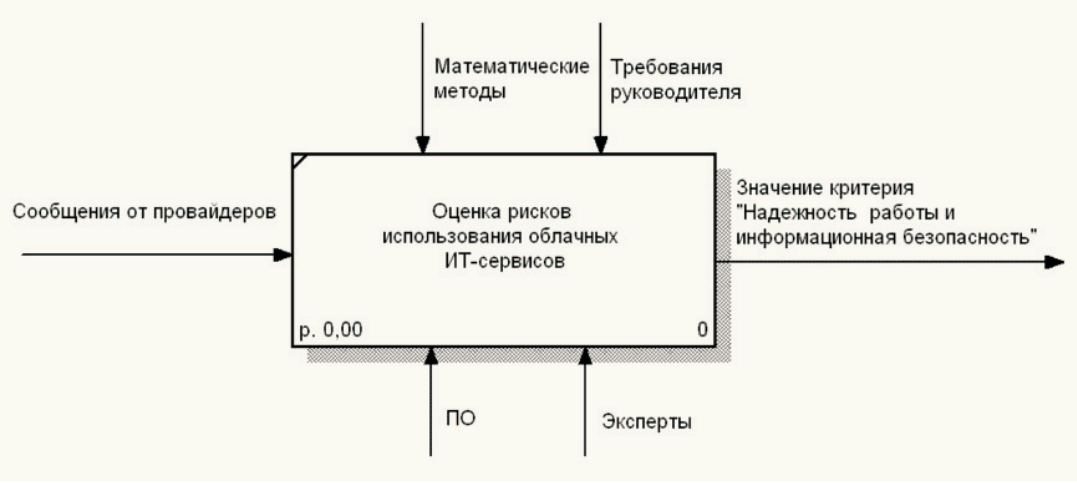

Рис. 1. Функциональная модель оценки рисков использования облачных ИТ-сервисов

На рис. 2 представлена декомпозиция блока «Оценка рисков использования облачных ИТ-сервисов».

Для более детального представления блока «Оценка и расчет показателей риска» декомпозируем его следующим образом (рис. 3).

Для построения аддитивной модели предлагается использовать 6 показателей, представленных в таблице. Расчет критерия «Надежность работы и информационная безопасность» проводится по формуле (1). Для обеспечения соответствия характеристикам показатели имеют ранг (коэффициенты весомости). Определение ранга показателей для эксперта является непростой задачей, т.к. при назначении весов он должен принимать во внимание среднестатистические балльные оценки показателей, диапазон шкалы критерия [4].

$$\text{Иб} = a_1 \cdot \text{Сд} + a_2 \cdot \text{Зп} + a_3 \cdot \text{Ау} + a_4 \cdot \text{Ип} + a_5 \cdot \text{Нпв} + a_6 \cdot \text{Рп}, \quad (1)$$

где Сд – относительный показатель сохранности хранимых данных; Зп – показатель защиты данных при передаче; Ау – показатель аутентификации; Ип – относительный показатель изоляции пользователей; Нпв – коэффициент использования нормативно-правовых вопросов; Рп – относительный показатель реакции на происшествия; a_1, a_2, a_3, a_4, a_5, a_6 – коэффициенты степени влияния.

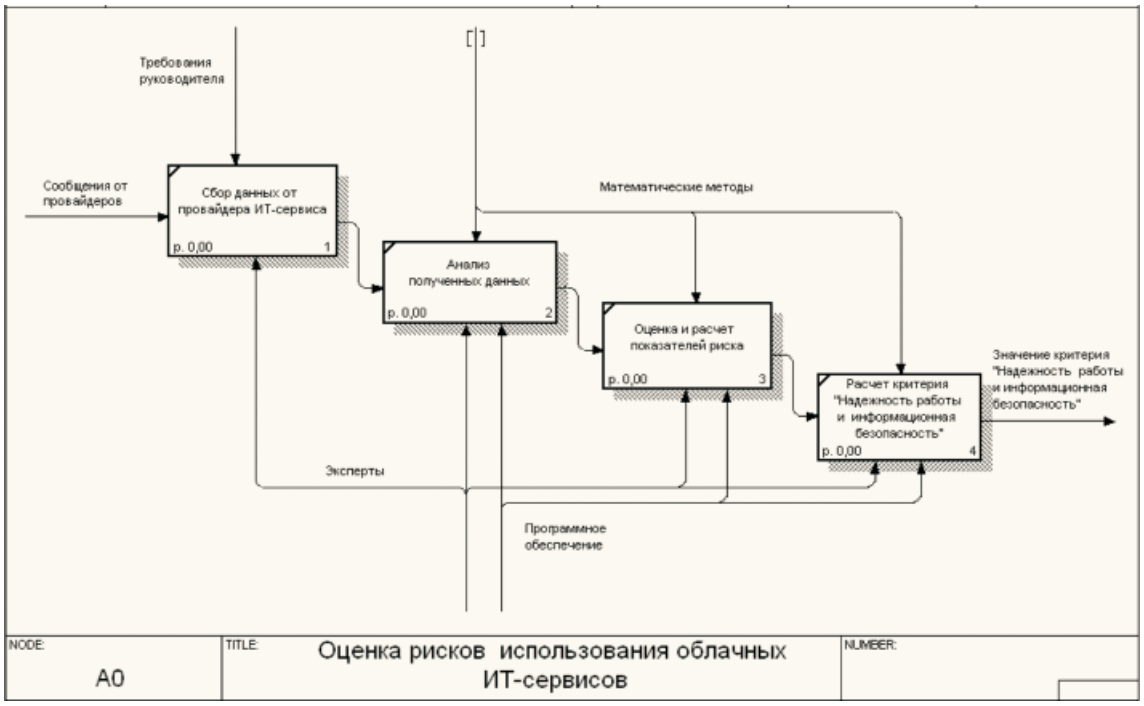

Рис. 2. Декомпозиция модели «Оценки рисков»

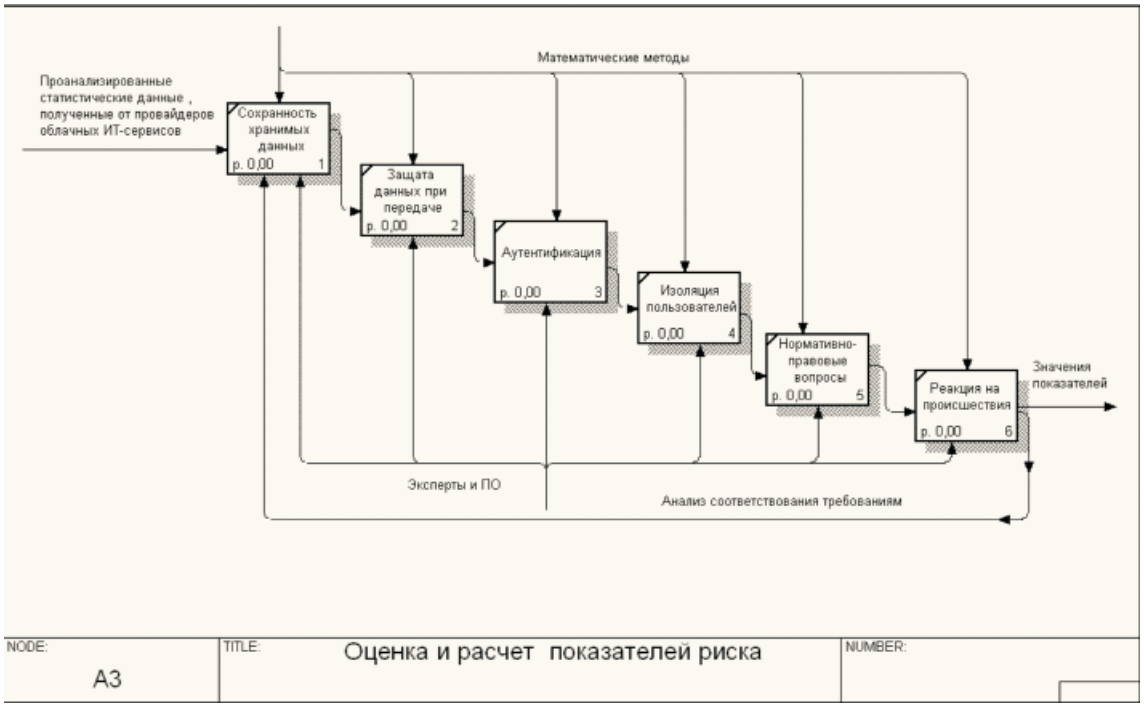

Рис. 3. Декомпозиция блока «Оценка и расчет показателей риска»

Классификация показателей оценки рисков применения облачных ИТ-сервисов

Показатели оценки рисков	Роль показателя в оценке	Правило расчета показателя
Критерий надежности работы и информационной безопасности		
Сохранность хранимых данных	Работа сервиса-провайдера по обеспечению сохранности хранимых данных	Алгоритм расчета показателей Критерия «Надежность работы и информационная безопасность»: 1. Сравнение с требуемыми показателями и стандартами, исходя из ответов провайдеров облачного ИТ-сервиса. 2. Балльная оценка экспертом степени соответствия требованиям безопасности облачных вычислений с использованием теории нечетких множеств (построение функции принадлежности). 3. Представление свернутых значений показателей в соответствии с существующими методическими указаниями.
Защита данных при передаче	Обеспечение сохранности данных провайдером при их передаче (это должно быть как внутри облака, так и на пути от/к облаку)	
Аутентификация	Распознание провайдером подлинности клиента	
Изоляция пользователей	Отделение данных и приложений одного клиента от данных и приложений других клиентов	
Нормативно-правовые вопросы	Степень использования провайдером законов и правил, применимых к сфере облачных вычислений	
Реакция на происшествия	Реагирование провайдера на происшествия, степень вовлечения клиентов в инцидент	

Заключение

Предложенная модель позволяет провести анализ возможных рисков при использовании того или иного облачного ИТ-сервиса, что позволит определить необходимость его приобретения. Расчет критерия «Надёжность работы и информационной безопасности» будет входить в состав интегральной модели оценки эффективности облачных ИТ-сервисов. Разработанная функциональная модель позволит максимально автоматизировать и систематизировать все этапы по разработке программного обеспечения по оценке рисков.

Список литературы

1. 8 шагов к безопасным облачным системам // Information Security / Информационная безопасность. – 2013. – № 1. – С. 28–29.

2. Маслов А.В., Григорьева А.А. Математическое моделирование в экономике и управлении: учебное пособие – Юрга: Изд-во Юргинского технологического института (филиала) Томского политехнического университета, 2007. – 264 с.

3. Москаленко А. Облачно и мобильно: Что может спасти российский ИТ-рынок? // InLine group, 24.01.2013, [Электронный ресурс]. – Режим доступа: http://www.inlinegroup.ru/events/press-releases/5635.php (дата обращения: 08.04.2013).

4. Разумников С.В. Анализ существующих методов оценки эффективности информационных технологий для облачных ИТ-сервисов [Электронный ресурс] // Современные проблемы науки и образования. – 2013 – № 3. – С. 1. – Режим доступа: www.science-education.ru/109-9548.

5. Разумников С.В. Использование метода линейного программирования для оценки эффективности применения облачных ИТ-сервисов // Приволжский научный вестник. – 2013. – № 7(23). – С. 43–45.

References

1. 8 Steps to a secure cloud systems [Journal «Information Security / Computer Security»] 2013, no 1, pp. 28–29.

2. Maslov A.V. *Mathematical modeling in economy and management* [manual / A.V. Maslov, A.A. Grigoriev; Yurginsky institute of technology]. Tomsk, 2012. 269 p.

3. Moskalenko A., *InLine group*, 24.01.2013, available at: http://www.inlinegroup.ru/events/press-releases/5635.php. Address date: 08.04.2013.

4. Razumnikov S.V. Analysis of existing methods of evaluating the effectiveness of information technology for cloud IT services [Modern problems of science and education] 2013, no. 3, available at: www.science-education.ru/109-9548.

5. Razumnikov S.V. Using linear programming method for assessing the effectiveness of cloud IT services [Scientific Bulletin Volga] 2013, no. 7 (23), pp. 43–45.

Рецензенты:

Мицель А.А., д.т.н., профессор кафедры автоматизированных систем управления, Томский государственный университет систем управления и радиоэлектроники, г. Томск;

Сапожков С.Б., д.т.н., профессор, заведующий кафедрой естественно-научного образования, Юргинский технологический институт (филиал) национального исследовательского Томского политехнического университета, г. Юрга.

Работа поступила в редакцию 26.02.2014.