УДК 332.87, 004.56

ПРОБЛЕМЫ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ИНФОРМАЦИОННЫХ СЕРВИСОВ ПРИ ФОРМИРОВАНИИ ИННОВАЦИОННОЙ ИТ-ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ ПО УПРАВЛЕНИЮ МНОГОКВАРТИРНЫМИ ДОМАМИ

Попов А. А.

ФГБОУ ВПО «Российский экономический университет имени Г. В. Плеханова», г. Москва, Россия (17997 Российская Федерация, г. Москва, Стремянный пер., 36), E-mail: a1710p@mail.ru

В работе рассматриваются вопросы информационной безопасности при использовании облачных сервисов в организациях по управлению многоквартирными домами. Отмечено, что в России происходит активное внедрение облачных технологий в управление многоквартирными домами. Часть информации, которую предполагается обрабатывать с помощью облачных сервисов, может быть персональной информацией или коммерческой тайной. Уровень информационной безопасности облачных сервисов недостаточен. Рассматриваются факторы, влияющие на информационную безопасность при использовании облачных сервисов. Наличие проблем информационной безопасности может привести к доступу посторонних лиц к персональной информации жильцов многоквартирных домов и к коммерческой информации организации по управлению многоквартирными домами. Приводятся рекомендации организациям по управлению многоквартирными домами по внедрению облачных сервисов и улучшению безопасности информации. Учет рекомендаций может привести к увеличению затрат на внедрение облачных сервисов по сравнению с внедрением существующих информационных систем, не использующих облачные сервисы.

Ключевые слова: информационная система, информационная инфраструктура, управление многоквартирным домом, облачные вычисления, информационная безопасность.

PROBLEMS OF INCREASING INFORMATION SECURITY OF CLOUD SERVICES FOR THE FORMATION OF INNOVATIVE IT INFRASTRUCTURE OF ORGANIZATION FOR APARTMENT BUILDINGS MANAGEMENT

Popov A. A.

Plekhanov Russian Economic University, Moscow, Russia (Stremyanny per. 36, 117997, Moscow), E-mail: a1710p@mail.ru

The paper deals with the issues of information security in the use of cloud services to organizations on management of apartment buildings. It is noted that in Russia there is an active adoption of cloud technology in the management of apartment houses. Some of the information which is supposed to be processed with the help of cloud-based services can be personal or business secrets. The level of security of cloud services is insufficient. Are considered factors are affecting the information security when using cloud services. The presence of information security problems can lead to unauthorized access to personal information of tenants of apartment buildings and commercial information of management organization of apartment buildings. Are given recommendations of the management of apartment buildings to implement cloud services and improve information security. Accounting guidelines may lead to an increase in the costs of implementing cloud computing compared with the implementation of the existing information systems that do not use cloud computing.

Keywords: information system, information infrastructure, the management of the apartment building, cloud computing, information security.

Введение

Использование облачных технологий и технологий виртуализации постоянно расширяется. Независимая исследовательская компании Forrester Research рассчитывает, что к 2020 году объём рынка облачных технологий достигнет $241 млрд. Это почти в 6 раз больше, чем в 2010 году [5]. Кроме этого, по прогнозам компании IDC [2], объем рынка облачных информационных сервисов в России к 2015 году достигнет $ 1,2 млрд.

Использование облачных технологий и технологии виртуализации в организациях по управлению МКД может дать такие ключевые преимущества как мобильность и инновационность. Во многих публикациях по информационной безопасности отмечается, что количество DDoS-атак в ближайшие годы увеличится. Это связано с недостаточным уровнем информационной безопасности появившихся в последнее время программных платформ для реализации облачных сервисов. В таких условиях предприятиям, использующим облачные сервисы, будет нелегко защищать свою деловую информацию и персональные данные абонентов. Кроме этого, в РФ об информационной безопасности зачастую и не задумываются. Информационная безопасность воспринимается как статья расходов, которую либо лучше избежать, либо значительно уменьшить.

Опыт внедрения облачных сервисов в управлении МКД в России

В [8, 9, 10] отмечалось, что в России происходит активное внедрение облачных информационных сервисов в управление жилищно-коммунальным хозяйством (ЖКХ) и, в частности, в управление многоквартирными домами (МКД). В качестве примеров можно привести специальное программное решение «Стек-Облако» программного комплекса «Стек-ЖКХ», 1С, ПАФЭС, универсальную учетную систему «Виртуальный ИРЦ». К абонентам информационных систем по управлению МКД можно отнести: жильцов, ресурсоснабжающие организации, поставляющие в МКД ресурсы, необходимые для оказания коммунальных услуг, организации, осуществляющие предоставление коммунальных услуг в многоквартирных и жилых домах, организации (лица), оказывающие услуги (выполняющие работы) по содержанию и ремонту помещений в многоквартирных домах, органы муниципального (регионального) управления.

Облачное приложение для управления МКД выполняется не на компьютере абонента, а на сервере компании-провайдера. Таким образом, облачные технологии позволяют снизить требования к ИТ-инфраструктуре организации по управлению МКД. Но при этом всё равно необходимо учесть уровень готовности ИТ-инфраструктуры организации по управлению МКД к автоматизации (внедрению облачных сервисов) [9, 10].

Информация, раскрываемая организациями по управлению МКД

Информация, отражающая деятельность организаций по управлению МКД, должна находиться в открытом доступе в соответствии со стандартом раскрытия информации в соответствии с Постановлением Правительства от 23.09.2010 № 731 (в редакции Постановлений Правительства РФ от 10.06.2011 № 459, от 06.02.2012 № 94, от 21.08.2012 № 845). Указанный стандарт предусматривает, что к информации будет иметь доступ широкий круг лиц, причем, независимо от цели ее получения. При изучении стандарта раскрытия информации для товариществ собственников жилья (ТСЖ) и состава электронных

паспортов отмечено, что часть информации (и особенно информация по абонентам-жильцам) может быть отнесена к персональным данным в соответствии с Федеральным законом Российской Федерации от 27 июля 2006г. № 152-ФЗ «О персональных данных». Кроме этого, с 1 марта 2013 года вступило в действие Постановление Правительства от 28 декабря 2012 г. № 1468. В соответствие с данным документом должны быть сформированы электронные паспорта МКД и жилых домов. Часть раскрываемой информации из электронных паспортов (например, размер оплаты за поставленные ресурсы, состояние расчетов с ресурсоснабжающими организациями и т.д.) относится к экономической деятельности организаций по управлению МКД. Также в электронных паспортах необходимо раскрывать сведения о собственниках жилья, а также информацию, непосредственно характеризующую техническое состояние и сведения об инженерной инфраструктуре и конструкции МКД. Перечисленные выше сведения, с некоторой степенью условности, можно классифицировать как сведения, содержащие коммерческую тайну в соответствии с Федеральным законом Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

Раскрытие информации абонентов, участвующих в управлении МКД, в таком концентрированном виде может привлечь внимание недобросовестных абонентов облачных информационных сервисов, а также злоумышленников, не входящих в число абонентов.

Факторы, обуславливающие проблемы информационной безопасности облачных сервисов, предоставляемых для управления МКД

Проблемы информационной безопасности облачных информационных сервисов при управлении МКД обусловлены следующими факторами [3, 4, 5]:

1. Изменяется концепция информационной безопасности. Происходит переход от защиты информации внутри сетевого периметра (защита серверов, бизнес-приложений, баз данных и активного сетевого оборудования предприятия от вирусных атак и других нежелательных воздействий со стороны) к облачной модели защиты приложений, данных и сервисов.
2. Информационные технологии развиваются быстрее, чем совершенствуются законы. Законы и стандарты, регламентирующие деятельность в облачных средах и регламентирующие их взаимодействие с другими системами, практически отсутствуют. Уровень ответственности в отношениях продавца ИТ-услуг (провайдера) и абонента в соответствии с документом SLA (Service Level Agreement) низок. Имеются проблемы лицензирования программного обеспечения в облачных сервисах в случае динамического перераспределения вычислительных ресурсов (не у всех производителей программного обеспечения предусматривается динамическое лицензирование программных продуктов).

3. Недостаточный уровень доверия к облачным информационным сервисам. Большинство компаний-провайдеров не в состоянии предоставить качественные с точки зрения информационной безопасности облачные услуги. Детальный анализ имевших место инцидентов с информационной безопасностью практически отсутствует. Зачастую отсутствует возможность смены провайдера облачных сервисов. Вследствие этого провайдер может навязывать абонентам собственную политику информационной безопасности в предоставляемых облачных сервисах, которая может не обеспечивать должного уровня защиты информации. Также абоненты часто сомневаются в надежности мест хранения информации. В России сложилось такое положение с хранением информации, что хранить данные, представляющие ценность для организации, внутри страны значительно опаснее, чем за ее пределами. Деятельность провайдеров облачных сервисов обычно является «непрозрачной». Провайдер PaaS-услуг не может гарантировать, что абоненты должным образом (с позиции обеспечения информационной безопасности) будут разрабатывать абонентское программное обеспечение на предоставляемой платформе. Провайдер SaaS-услуг не может контролировать корректность организации доступа со стороны абонента.

4. Появление угроз нового вида и неприменимость (ограниченная применимость) большинства существующих методов защиты ИТ-инфраструктуры от инцидентов с информацией. Одной из главных угроз можно считать нарушение безопасного функционирования гипервизора, обеспечивающего независимое функционирование абонентских виртуальных машин и безопасное функционирование системы управления виртуальной инфраструктурой. Атаки злоумышленников (DDoS-атаки на ИТ-инфраструктуру между облачным сервисом и абонентами) производятся в основном на облачные сервисы, которые осуществляют изоляцию между данными абонентов.

Часто данные абонентов изолируются за счет осуществления коррекции программного кода информационного сервиса. Данные абонента в этом случае оказываются «прикреплены» к программному коду. В результате увеличивается уязвимость данных в случае ошибок программного кода. Кроме этого, при предоставлении облачных сервисов слабо рассмотрены вопросы их возможного штатного или несанкционированного взаимодействия друг с другом, а также возможность недостаточного стирания данных на стороне провайдера облачных сервисов после прекращения абонентского сеанса.

5. Возможные злонамеренные действия посторонних лиц (в случае несанкционированного доступа), злонамеренные действия недобросовестных сотрудников организаций по управлению МКД, управляющих организаций и органов власти. Кроме этого, использование облачных сервисов предполагает появление новой категории пользователей

(администраторы облачных сервисов), которые имеют доступ к данным виртуальных машин абонентов.

Рекомендации организациям по управлению МКД по улучшению безопасности информации при внедрении облачных сервисов

ИТ-инфраструктура организации по управлению МКД при внедрении облачных сервисов должна решать задачи, приведенные в [2]. Для повышения безопасности информации следует учесть большое количество рекомендаций, которые могут потребовать от организации по управлению МКД дополнительных финансовых затрат:

1. Перед внедрением частного облака необходимо выяснить потребности всех абонентов, участвующих в управлении многоквартирным домом, в IT-ресурсах, оценить возможность переноса используемых приложений в облачную среду. Требуется определить, какие абонентские данные нуждаются в защите, а также учесть готовность организации по управлению МКД к автоматизации [8, 9, 10]. Также необходимо оценить уровень информационной безопасности провайдера облачных услуг в соответствии с [1].

2. Необходимо предъявлять требования к провайдеру облачных сервисов в соответствии с документами Cloud Computing Information Assurance Framework (ENISA), Security Recommendations for Cloud Computing Providers (BSI) и Security Assessment Provider Requirements and Customer Responsibilities (NIST) [3]. Необходимо предусмотреть заключение соглашение о гарантированном уровне доступности услуг (SLA), соглашение о конфиденциальности, поручения на обработку персональных данных. Помимо этого необходимо знать локальные нормативные требования, которым подчиняется провайдер, проходил ли провайдер внешний аудит соответствия (ISO 27001, PCI DSS, SAS 70) и имеет ли он аттестацию ФСТЭК. Основные меры и процессы информационной безопасности должны быть организованы в соответствии с документами организации Cloud Security Alliance (ассоциация RISSPA – российское отделение Cloud Security Alliance). Также для предоставления абонентам необходимых сведений обо всех основных аспектах информационной безопасности может использоваться опросник [6].

4. В случае использования частных облаков необходимо создать периметр, который обеспечивается идентификацией каждого абонента, допущенного к работе в частном облаке. Необходимо обеспечить многоуровневость периметра с обеспечением различных зон доверия абонентам. Для изоляции абонентов друг от друга каждому из абонентов должна предоставляться индивидуальная виртуальная машина и обеспечиваться применение стандартных протоколов обмена информацией [3]. Построение безопасной инфраструктуры облака необходимо осуществлять с помощью доверенной загрузки любого из серверов, составляющих опорную группировку облака. После этого осуществляется формирование

набора сервисов для поставки абонентам с помощью средств доверенной загрузки виртуальных машин с предопределенными настройками политик безопасности [2].

5. Необходимо применять шифрование (хранение в обезличенном виде) абонентских данных и их резервное копирование при их расположении в хранилище данных. Провайдер должен предусмотреть полное удаление данных абонента, если закончилась необходимость в их дальнейшем использовании. Аутентификация «абонент – данные» должна осуществляться в обоих направлениях (однозначная «привязка» абонентов к выполняемым операциям). Для аутентификации рекомендуется применение сертификатов и токенов [4, 5].

6. Необходимо повысить осведомленность абонентов по вопросам информационной безопасности с учетом рекомендаций, приведенных в [7].

Заключение

Использование облачных сервисов и технологии виртуализации повышает удобство работы абонентов и, в перспективе, снижает затраты организаций по управлению МКД на поддержание ИТ-инфраструктуры. При этом внедрение облачных сервисов и повышение уровня их информационной безопасности в организациях по управлению МКД может потребовать проведения большого количества мероприятий, которые потребуют привлечения дополнительных ресурсов. Таких ресурсов у организаций по управлению МКД может и не быть. Поэтому в настоящее время возможны проблемы с внедрением облачных сервисов.

Массовое внедрение облачных сервисов в управлении МКД следует ожидать в случае улучшения качества, удешевления стоимости услуг, уменьшения количества и сложности мероприятий при их внедрении. До этого момента, очевидно, организации по управлению МКД, вследствие недостатка средств, будут внедрять более дешевые информационные системы без использования облачных сервисов [10].

Список литературы

1. Антонов П. Миграция на облако: стимулы и препятствия. Сайт. – URL: http://www.itsec.ru/articles2/saas/migraciya-na-oblako-stimyli-i-prepyatstviya (дата обращения 29.04.13).

2. Бабанин А. Как построить инфраструктуру безопасного облака. Сайт. – URL: http://www.itsec.ru/articles2/Oborandteh/kak-postroit-infrastrukturu-bezopasnogo-oblaka (дата обращения 29.04.13).

3. Васильев В. Безопасность облачных сред. Сайт. – URL: http://www.pcweek.ru/security/article/ detail.php?ID=139185 (дата обращения 29.04.13).

4. Климов Е. Существующие подходы к защите облачных сервисов. Сайт. – URL: http://www.itsecurityforum.ru/2012/assets/reports/report9.pdf (дата обращения 29.04.13).
5. Облачные вычисления, «дырявые» облака и способы защиты данных. Сайт. – URL: http://4by4.ru/ru/analytics/oblachnye-vychisleniya-dyryavye-oblaka-i-sposoby-zashchity-dannyh (дата обращения 29.04.13).
6. Опросник оценки состояния безопасности облачной среды. Сайт. – URL: http://www.risspa.ru/csa/caiq/ (дата обращения 29.04.13).
7. Писаренко И. Повышение осведомленности пользователей по вопросам ИБ. Сайт. – URL: http://www.itsec.ru/articles2/control/povyshenie-osvedomlennosti-polzovateley-po-voprosam-ib (дата обращения 29.04.13).
8. Попов А. А. Формирование набора параметров для определения готовности ТСЖ региона к автоматизации процессов управления многоквартирными домами// Электронный журнал «Известия Российского экономического университета имени Г.В. Плеханова». – 2012. – №3 (8); Сайт. – URL: http://www.rea.ru/Main.aspx?page=Nomer_3__8__1 (дата обращения: 29.04.13).
9. Попов А. А. Разработка алгоритма для совершенствования информационной инфраструктуры товариществ собственников жилья при управлении объектами недвижимости (многоквартирными домами) // Электронный журнал «Современные проблемы науки и образования». – 2012. – № 6; Сайт. – URL: www.science-education.ru/106-7563 (дата обращения: 29.04.2013).
10. Попов А. А. Определение направлений, форм и способов перспективного развития инновационной инфраструктуры организаций по управлению многоквартирными домами (товариществ собственников жилья). – М.: Изд-во «ИРИСБУК», 2012. – 213 с.

Рецензенты:

Дик Владимир Владимирович, д-р экон. наук, профессор, заведующий кафедрой информационного менеджмента и электронной коммерции, Московский финансово-промышленный университет «Синергия», г. Москва.

Курченков Владимир Викторович, д-р экон. наук, профессор, заведующий кафедрой государственного и муниципального управления, Федеральное государственное образовательное учреждение высшего профессионального образования «Волгоградский государственный университет» (Министерство образования и науки РФ), г. Волгоград.