Исследование методов защиты информации в облачных сервисах

Research of methods of information security in cloudy services

Гринюк О.Н.
Канд. техн. наук, доцент ФГБОУ ВО «Российский химико-технологический университет имени Д. И. Менделеева», г. Новомосковск

Grinyuk O.N.
Candidate of Technical Sciences, Associate Professor, Novomoskovsk Institute (branch) of the Dmitry Mendeleev University of Chemical Technology of Russia

Сысоев К.А.
Студент, Узловский железнодорожный техникум — филиал ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I», г. Узловая

Sysoyev K.A.
Student, Uzlovsky Railway College, Branch of the Emperor Alexander I Saint- Petersburg State Transport University, Uzlovaya

Шевченко Е.В.
Преподаватель Узловский железнодорожный техникум — филиал ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I», г. Узловая

Shevchenko E.V.
Lecturer, Uzlovsky Railway College, Branch of the Emperor Alexander I Saint- Petersburg State Transport University, Uzlovaya

Аннотация
Дана характеристика существующих моделей обслуживания видов облачных технологий. Сформулированы основные проблемы защиты информации в облачных сервисах. Рассмотрены стратегии обеспечения облачной безопасности для бизнеса разных размеров.
Ключевые слова: облачные технологии, безопасность облачных данных.

Abstract
The characteristic of the cloud technologies models of service is given. The main problems of information security in cloudy services are formulated. Strategy of support of cloudy safety for business of the different size is considered.
Keywords: cloud technologies, safety of cloudy data

Облачные технологии уже стали наиболее активно развивающимся направлением в крупных компаниях с распределенной инфраструктурой, которые стремятся перейти к более эффективному управлению информационными системами. Большинство малых и средних компаний также рассматривают новые технологии, предоставляемые облачными инфраструктурами, как возможность сократить расходы и обеспечить более высокое качество предоставляемых услуг.

Для этого, исходя из специфики решаемых задач и объемов обрабатываемой информации, нужно будет выбрать одну из трех существующих на сегодняшний день моделей обслуживания [1]:

1. SaaS – программное обеспечение как сервис. В данном случае вы используете программное обеспечение, приложения и операционные системы провайдера, который полностью контролирует функционирование облачной инфраструктуры. По большому счету, вы управляете лишь своим аккаунтом (группой аккаунтов) с возможностью вносить незначительные изменения в некоторые настройки приложений. Примером данной услуги могут послужить YahooMail, Google Disk, Office Online и др.
2. PaaS – платформа как сервис. Здесь вы получаете возможность установки собственного программного обеспечения и построения приложений уровня Saas. Тем не менее, контроль операционных систем, серверов, хранилищ данных по-прежнему остается за провайдером. Самым простым примером здесь может послужить хостинг, где вы устанавливаете свою CMS, модули и плагины к ней, а также получаете доступ к MySQL, PHPMyAdmin и др.
3. IaaS – инфраструктура как сервис. Здесь у вас еще больше свободы – провайдер предоставляет лишь физический фундамент вычислительных мощностей (виртуальных машин), на основе которых вы можете развернуть свою облачную инфраструктуру и реализовать собственные решения уровня PaaS и Saas, контролируя устанавливаемые операционные системы и приложения.

Повсеместное использование ЭВМ и на их основе всевозможных организационно-технических («человек-машина») систем, таких как «облачные» вычисления, влечет за собой возникновение проблем информационной безопасности. Еще один немаловажный вопрос – насколько защищенной оказывается информация после ее размещения на облаке. Провайдеры облачных услуг утверждают, что причин для беспокойства нет, поскольку защита информации клиентов для них – вопрос первостепенной важности.

Однако, даже если провайдеру и удастся защитить персональные данные от атаки извне, можно ли быть уверенным, что сотрудники самого облачного сервиса не превысят должностные полномочия и не получат доступ к персональной информации. Даже в том случае, если на облаке предусмотрено шифрование, ключи шифрования также хранятся на облачном сервере, а значит каждый, кто имеет к ним доступ, может получить доступ и к вашим зашифрованным данным.

Фактически задачу защиты облака можно разделить на две составляющие: обеспечение безопасности функционирования оборудования и безопасности данных. Провайдер должен реализовать защиту своего аппаратно-программного комплекса от несанкционированного вторжения, модификации кода, взлома ИТ-системы, чтобы обеспечить защиту данных клиента. Клиент, в свою очередь, при необходимости размещения каких-либо важных и секретных данных, может использовать технологии шифрования для защиты от несанкционированного доступа к ценной информации. Только такой комплекс мер позволит обеспечить безопасность данных в облаке.

Исходя из этого, можно использовать одну из четырех стратегий обеспечения облачной безопасности для бизнеса разных размеров с разными требованиями к конфиденциальности [2].

Стратегия «Минимум ошибок» предполагает максимальное использование лидирующих SaaS-сервисов, не обладающих необходимой экспертизой предприятиями малого бизнеса, поскольку они вряд ли достигнут сравнимого уровня ИБ самостоятельно.

Стратегия «Минимальные усилия» предусматривает максимальное использование лидирующих SaaS-сервисов и дополнительно тщательное изучение и использование доступных встроенных сервисов безопасности, например: двухфакторной аутентификации, защиты паролем загружаемых в Google Drive документов, аккаунта

Google на других сайтах («кустарная» реализация принципа SSO), хранение резервных учетных записей Google и удаление учетных записей сотрудников при их увольнении.

Стратегия «Точечное внимание» заключается в снижении общепризнанных рисков и активном противодействии базовым угрозам. Ключевой посыл – противодействие управляемому количеству угроз, концентрация ресурсов и экспертиз на самых важных направлениях. Как минимум девять указанных угроз ИБ облаков должны быть смягчены, по возможности интегрированы с платформой сервис-провайдера для снижения капитальных и операционных затрат. В случае отсутствия интегрированных мер необходимо внедрение выделенных решений / мер по ИБ облаков. При выборе мер можно использовать как лучшие практики от ENISA, так и описанные ниже продукты ИБ (в том числе, интегрированные с платформами сервис-провайдеров).

Стратегия «Многослойная оборона» предполагает разработку целостной комплексной концепции обеспечения облачной безопасности на основе глубокого анализа рисков, тщательного выбора сервис-провайдера, с учетом вопросов обеспечения ИБ и соответствия требованиям законодательства, а также последующего проектирования и внедрения организационных и технических мероприятий по защите информации. Исходя из значимости и количества чувствительной информации, система защиты по возможности должна быть независима от провайдера облачных сервисов. Все средства защиты информации должны быть переданы в промышленную эксплуатацию и эксплуатироваться командой экспертов. В случае отсутствия внутренних ресурсов – сертифицированных специалистов по облачной безопасности, аудиту и контролю – ИТ желательно привлекать внешних экспертов на постоянной основе – как через открытие новых позиций, так и путем аутсорсинга или аутстаффинга.

Литература

1. Модели сервисов облачных вычислений: Часть 1. Инфраструктура как сервис [Электронный ресурс]/ developerWorks: программе IBM «Глобальный предприниматель»/ 16.03.2012/ URL:http://www.ibm.com/developerworks/ru/library/cl-cloudservices1iaas/

2. Защита облачных сервисов: стратегия информационной безопасности и продукты [Электронный ресурс]/астерос: бизнес-корпорация по предоставлению комплекса IT-услуг/ 29 апреля 2014г./ URL:http://www.asteros.ru/press/press/2477/ /