Снижение стабильности это не только негативный фактор, но и положительный. Государство уменьшает импорт зарубежной продукции из–за повышения стоимости товаров, это развивает национальную продукцию. Тем самым развивается национальное хозяйство. Снижение стоимости национальной валюты влияет на увеличение экспорта. Национальная продукция становится дешевле, а следовательно более конкурента способной на международном рынке.

Следующий аспект это-влияние на гос. корпорации (ГАСПРОМ, РОСНЕФТЬ, Сбербанк). Представленные гос. корпорации выпускают ценные бумаги, которые является выражением части капитала самой корпорации. Акции о облигации этих компаний располагаются на фондовых рынках. Данные бумаги доступны всем участникам фондовых бирж. Доля от покупки ценных бумаг поступает в бюджет. Этот аспект может оказывать негативное влияние. Из-за покупки ценных бумаг в больших объемах иностранными резидентами, в их руках образуется большая доля корпорации. С одной стороны, это хорошее привлечение новых инвесторов, а с другой это негативное косвенное влияние иностранных резидентов имеющих большую долю акций в этих компаниях. Все это сказывается на экономике страны.

Рассмотренные факторы влияния биржевых торгов на экономику России показали, как положительное, так и отрицательное воздействие. Биржевой рынок создает большие возможности для экономики страны, на пример, США большая часть капитала этой страны постоянно обращается на биржах этой страны и многих других зарубежных стран. У России ещё очень маленький опыт в биржевой истории и при развитии этой части рыночной экономики возможны улучшения и в экономике страны.

Список литературы:

1. Налоговый кодекс Российской Федерации
2. Боровкова Вал. А. Фондовые биржи и механизм их функционирования //учебное пособие. СПБТЭИ-2008.
3. http://onlinebroker.vtb24.ru/services/stock/tax/
4. http://pandia.ru/text/78/345/1404-2.php

БЕЗОПАСНОСТЬ ОБЛАКА И УПРАВЛЕНИЕ ИМ

С.В. Разумников, к.т.н.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел. 8(38451)77764
E-mail: demolove7@inbox.ru

Аннотация. Каждый ответственный ИТ-руководитель в первую очередь интересуется безопасностью приложений и данных в облаке. Безопасность обеспечивается, если применяются соответствующие технологии и средства управления. Обеспечение безопасности – это одна из областей, в которой применяются как технологии, так и управление. Действительно, перенос приложений в облако не сводит на нет множество традиционных функций ИТ, – безопасность, соответствующее управление данными, контроль за расходами и надлежащее управление изменениями остаются ключевыми обязанностями. Но при работе в облаке меняются способы управления на предприятии. В этой статье рассматривается безопасность облака и управление им, а также рекомендации ИТ-руководителям по планированию в этих областях.

Annotation. Every responsible IT leader is primarily interested in the security of applications and data in the cloud. Security is ensured if appropriate technologies and controls are used. Security is one of the areas in which both technology and management are applied. Indeed, migrating applications to the cloud does not negate many of the traditional IT functions — security, proper data management, cost control, and proper change management remain key responsibilities. But when working in the cloud, management methods in the enterprise are changing. This article discusses cloud security and management, as well as recommendations to IT planners in these areas.

Ключевые слова: облачные технологии, управление, безопасность, приложения, стратегия.

Keywords: cloud technologies, management, security, applications, strategy.

Введение. Почти все ИТ-руководители признаются, что они столкнулись с сомнениями при мысли о переносе ИТ-экосистемы в облако. В конце концов, когда все приложения и данные находятся в локальном центре обработки данных, корпоративный ИТ-отдел все контролирует. Это можно сравнить с концепцией банка 150 лет назад. В то время люди держали наличные средства при себе.

Но в итоге все осознали, что безопаснее хранить деньги в банке, где их могут защитить соответствующие специалисты.

Однако безопасность облака существенно отличается от безопасности банка: владелец приложения и данных должен активно участвовать в ее обеспечении [1, 2]. Рассмотрим то, чему следует уделить внимание и для чего выделить ресурсы.

Физическая безопасность

Обеспечение безопасности начинается с физической безопасности, то есть с безопасности помещений, в которых работает облако, – облачных центров обработки данных. Поставщики облачных услуг вкладывают значительные средства в физическую безопасность. Все они обеспечивают круглосуточное видеонаблюдение. Сотрудники в облачных центрах обработки данных должны пройти строгие проверки. Для доступа к зонам работы серверов требуется несколько форм проверки подлинности, включая биометрическую. Все действия контролируются и проверяются.

Обновления программного обеспечения

Напомним, что при развертывании приложения в облаке в качестве виртуальной машины с моделью «инфраструктура как услуга» (IaaS) ваш персонал отвечает за своевременную установку исправлений и обновлений программного обеспечения. При использовании модели «платформа как услуга» (PaaS) поставщик облачных услуг будет поддерживать системное программное обеспечение.

Повсеместное шифрование

Рекомендуется, чтобы в приложении использовалось шифрование везде, где это возможно. Для гибридных облачных соединений (соединения между локальным центром обработки данных и облаком), VPN и Microsoft Azure ExpressRoute в качестве транспортного протокола используйте IPSec и IKE.

Можно рассмотреть возможность использования TLS (Transport Level Security). Это технология обеспечения безопасности с использованием безопасного протокола HTTP (HTTPS) для клиентского доступа к облачным веб-сайтам.

Также следует по возможности шифровать неактивные данные в службе хранилища Microsoft Azure или в базах данных. Например, база данных SQL Azure предлагает прозрачное шифрование данных, чтобы шифровать и расшифровывать данные в реальном времени с использованием сертификата сервера. Реплики в различных географических регионах имеют различные сертификаты, которые сменяются каждые 90 дней (стандартная частота).

Хранилища ключей и аппаратные модули безопасности

При обеспечении безопасности лучше всего отделить ключи шифрования от приложения. С помощью хранилища, например Azure Key Vault, это возможно. Благодаря ему администратор сначала создает хранилище ключей для приложения и помещает в него ключи (рис. 1). Затем Azure Key Vault предоставляет разработчику URL-адреса ключей, которые приложение может использовать во время выполнения для расшифровки произвольных данных, например, в службе хранилища Azure или в другом месте.

Для дополнительной защиты ключи можно хранить в аппаратном модуле безопасности (HSM) – физическом устройстве, которое может хранить и создавать ключи. HSM также может перераспределять нагрузку при криптографической обработке (обычно это ресурсоемкая операция для ЦП), выполняя локальное шифрование и расшифровку.

Антивирусное программное обеспечение

Ничто не может повредить локальное или облачное приложения сильнее, чем умышленное или непреднамеренное распространение вирусов. В приложениях (особенно IaaS) следует использовать антивредоносное ПО, предоставляемое поставщиком облачных услуг (например, антивредоносное ПО Microsoft) или партнером в магазине облачных решений. Регистрируются все события, обнаруживаемые антивредоносным ПО. Администраторам облаков следует периодически проверять соответствующие журналы, чтобы узнать, нужно ли что-то предпринять.

Многофакторная проверка подлинности

Для обеспечения дополнительной безопасности используйте многофакторную проверку подлинности (MFA) при входе пользователей. Для получения доступа к корпоративным ресурсам MFA требует предоставить второй тип удостоверения помимо имени пользователя и пароля. Доступны различные формы MFA, включая биометрические модели, телефонные вызовы и текстовые сообщения. Например, вход пользователя может активировать телефонный вызов на мобильный телефон с возможностью идентификации по отпечатку пальца.

Пользователю запрещается вход до тех пор, пока телефон не вернет действительное значение. При применении еще одного вида MFA каждые несколько секунд на мобильном устройстве изменя-

ется случайное число по определенному алгоритму, при этом для получения доступа пользователь должен ввести число, отображаемое на экране телефона.

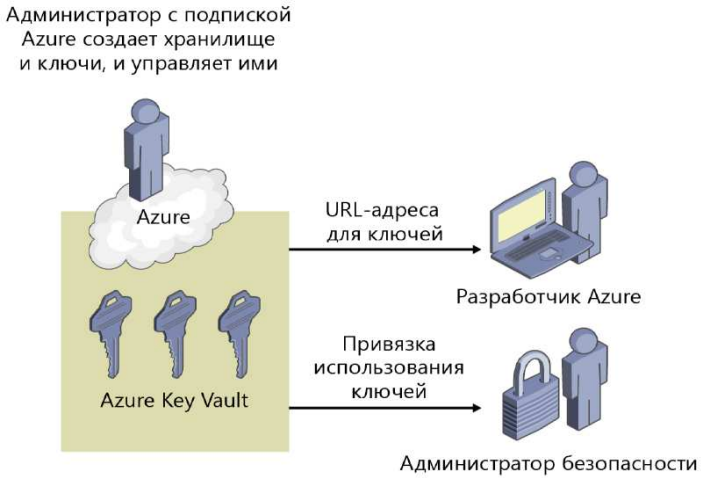

Рис. 1. Azure Key Vault

Безопасный жизненный цикл разработки

Несмотря на то, что облако обеспечивает много преимуществ безопасности, размещение приложения в облаке не освобождает разработчиков приложения и специалистов по безопасности от своих обязанностей полностью. Разработчикам и тестировщикам рекомендуется придерживаться принципов цикла разработки безопасного программного обеспечения (https://www.microsoft.com/sdl/default.aspx), который предоставляет набор шагов для прогнозирования и устранения угроз. При развертывании следует добавить антивирусные и антивредоносные программы.

Мониторинг нарушений системы безопасности

ИТ-руководители должны тщательно следить за нарушениями системы безопасности в облачных приложениях так же, как и для локальных приложений. К счастью, в штате поставщиков облачных услуг состоят обученные специалисты по безопасности, которые непрерывно следят за действиями в облаке [3-5].

Для обеспечения дополнительной безопасности может потребоваться развернуть приложение для предотвращения атак системы безопасности и управления событиями (SIEM). Системы SIEM сканируют приложения на наличие уязвимостей, обеспечивают обнаружение атак и отслеживают поведение пользователей на наличие признаков вредоносных действий.

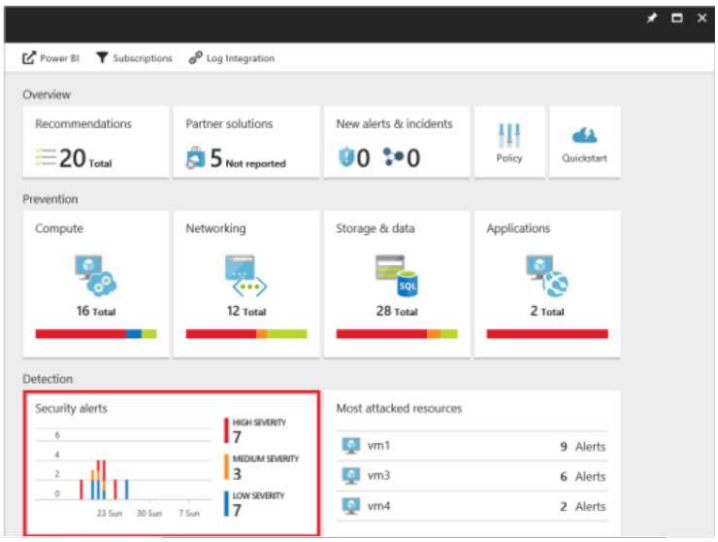

Рис. 2. Центр безопасности Azure

Кроме того, в центре безопасности Azure (рис. 2) специалистам в области безопасности вашей организации доступны широкие возможности, включая предоставление рекомендаций (например, применение исправлений или обновление антивирусного ПО), предупреждений системы безопасности (например, при взаимодействии приложения с известными вредоносными IP-адресами) и настройку политик безопасности для ваших приложений.

Тест на проникновение

Иногда уязвимости можно найти только при попытке реальной атаки приложения. Многие предприятия нанимают команды специалистов в области компьютерной безопасности для выполнения, так называемого, теста на проникновение. Это самый оптимальный подход.

Однако такой тест нужно планировать совместно с поставщиком облачных услуг, поскольку ему будет сложно определить, настоящая ли это атака, без предварительного предупреждения.

Общие сведения о средствах управления безопасностью облака

На рис. 3 показано распределение обязанностей по обеспечению безопасности с учетом модели приложения (локальное, IaaS, PaaS и SaaS).

Рис. 3. Сведения об ответственности за средства контроля безопасности

Заключение. Перенос приложений в облако – важная и серьезная задача, требующая изменения способа работы предприятия и ИТ-инфраструктуры. Одним из главных составляющих переноса является безопасность приложений и данных в облаке. В этой статье была рассмотрена безопасность облака и управление им, а также рекомендации ИТ-руководителям по планированию в этих областях.

Работа выполнена при финансовой поддержке гранта РФФИ № 18-07-00031 «Модели, алгоритмы и программное обеспечение системы поддержки принятия стратегических решений к переходу на облачные технологии».

Список литературы:

1. Разумников С.В. Оценка эффективности и рисков от внедрения облачных ИТ-сервисов // Фундаментальные исследования. - 2014. - Вып. № 11-1. - С. 33-38.
2. Razumnikov S.V. Decision support system of transition IT-applications in the cloud environment // International Siberian conference on control and communications SIBCON 2015 – [Электронный ресурс] – Режим доступа: http://ieee.tpu.ru/musor/sbornik/files/sections.html
3. Разумников С.В. Модель поддержки принятия решений о миграции корпоративных приложений в облачную среду // Научные труды Вольного экономического общества России. - 2015 - Т. 194. - С. 490-502.
4. Razumnikov S.V., Kurmanbay A.K. Models of evaluating efficiency and risks on integration of cloud-base IT-services of the machine-building enterprise: a system approach // IOP Conference Series: Materials Science and Engineering. - 2016 - Vol. 124 - №. 1, Article number 012089. - p. 1-5.

5. Razumnikov S.V. Models of evaluating efficiency and risks on integration of cloud-base IT-services of the machine-building enterprise: a system approach // IOP Conference Series: Materials Science and Engineering. - 2016 - Vol. 124 - №. 1, Article number 012089. - p. 1-5.

ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ МИГРАЦИИ ИТ-ПРИЛОЖЕНИЙ В ОБЛАЧНУЮ СРЕДУ

С.В. Разумников, к.т.н.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел. 8(38451)77764
E-mail: demolove7@inbox.ru

Аннотация. Важным составляющим для обоснования внедрения облачных технологий на уровне виртуальной инфраструктуры являются технико-экономические расчеты. В этой статье рассматриваются модели для расчета экономической эффективности перехода к облачным технологиям на примере IaaS, которые помогут оценить объем вложений и выбрать оптимальный вариант реализации ИТ-инфраструктуры.

Ключевые слова: облачные технологии, управление, безопасность, приложения, стратегия.

Annotation. An important component to justify the introduction of cloud technologies at the level of virtual infrastructure are technical and economic calculations. This article discusses the model for calculating the economic efficiency of the transition to cloud technologies on the example of IaaS, which will help to assess the amount of investments and choose the best option for implementing IT infrastructure.

Keywords: cloud technologies, management, security, applications, strategy.

Введение

Тема экономического обоснования перехода в облака сегодня настолько же актуальна, насколько и слабо освещена в литературе и интернет-СМИ. С одной стороны, модель расчетов экономической эффективности довольно проста и находится как калькуляция эксплуатационных и единовременных затрат. Однако собрать точные входные данные – это непростая задача. А если использовать неточные данные, то и результат будет не в пользу решений по использованию облачных технологий. Поэтому провайдеры облачных услуг стараются избегать грубых расчетов в проектах, а в качестве рекламы используют неполные примерные данные, которые иллюстрируют «эффективность» использования облачных решений [1-5].

В качестве примера облачной услуги приведем сервисы аренды виртуальной инфраструктуры по модели IaaS. Необходимо сделать технико-экономическое обоснование перехода к облачным технологиям. Выполнить такое обоснование требуется в двух случаях: 1) когда назрел вопрос о модернизации существующей инфраструктуры; 2) когда требуются новые ресурсы для проекта, плановое расширение или когда планируется создание ИТ-инфраструктуры с нуля.

Как правило, такие проекты предполагают выполнение технико-экономических расчетов, которые помогут оценить объем вложений и выбрать оптимальный вариант реализации ИТ- инфраструктуры.

В обоих случаях конечной целью расчетов является сравнение нескольких вариантов реализации, но при модернизации существующей ИТ-инфраструктуры мы имеем возможность получить текущие значения затрат на ИТ и текущий уровень качества, используя эти цифры в качестве базовых значений, по отношению к которым будет считаться экономический эффект от внедрения новых технологий.

Основные термины и понятия, необходимые в процессе выбора вариантов реализации ИТ-инфраструктуры.

Оценка экономической эффективности должна основываться на сопоставлении величины затрат на ее внедрение, развертывание и эксплуатацию с получаемыми результатами. Результат оценивают через показатели экономической эффективности, которые должны быть рассчитаны [6, 7].

Годовой экономический эффект (ГЭЭ) – это наиболее удобный показатель оценки экономической эффективности ИТ-проектов, который измеряется в рублях в год.

$$ГЭЭ = Э_{год} - E \times K,$$