Бобрышева Г.В., Пудовкина Е.М. Облачная безопасность. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2017. – С. 99-104.

УДК 004.75

ОБЛАЧНАЯ БЕЗОПАСНОСТЬ

Г.В. Бобрышева, Е.М. Пудовкина

CLOUDSAFETY

G.V. Bobrysheva, E.M.Pudovkina

Аннотация. Организации во всем мире активно инвестируют средства в киберзащиту для обеспечения безопасности критических активов компании и приходят к заключению о том, что использование облачных сервисов – один из лучших вариантов для облегчения нагрузки на их внутренние инфраструктуры.

Ключевые слова: облачные вычисления, безопасность, защита данных, инфраструктура как сервис, Data-центр.

Abstract. Organizations around the world are actively investing in cyber defense to ensure the security of critical assets of the company and come to the conclusion that using cloud services is one of the best options to ease the burden on their internal infrastructure.

Keywords: cloud calculations, security, data protection, infrastructure as service, data center.

Облачные сервисы за последние несколько лет проникли во многие сферы жизни и бизнеса – в результате появилось много разновидностей подобных ресурсов. Стек облачных технологий состоит из трех частей, каждая из которых представляет отдельную категорию сервисов:

- SaaS (Software as a Service) – приложения, работающие в облаке, доступ к которым конечные пользователи получают через веб;
- PaaS (Platform as a Service) – набор инструментов и сервисов, облегчающих разработку и развертывание облачных приложений;
- IaaS (Infrastructure as a Service) – вычислительная инфраструктура (серверы, хранилища данных, сети, операционные системы), которая предоставляется клиентам для разворачивания и запуска собственных программных решений [1].

К сожалению, все чаще и чаще крупные корпорации, пользующиеся услугами облачных сервисов, сталкиваются с нарушениями безопасности. Неопределенность, которая окружает облачные вычисления, может обратить процесс обеспечения безопасности в реальную проблему, которая заключается не столько в безопасности облака, сколько в самой политике и технологии обеспечения безопасности облака, а также в контроле над этой технологией. Хотя большинство предприятий знакомы с понятием облака, или, по крайней мере, идеей облачных вычислений, неправильные представления и недоразумения в отношении того, что может предложить технология, являются крайне актуальными. Это в свою очередь, открывает совершенно новые возможности для вирусов и червей, поэтому эксперты советуют заняться вопросами облачной безопасности заранее во избежание дорогостоящих последствий [2].

«Облачные вычисления очень популярны, но крайне непонятны… Безопасность по-прежнему является наиболее распространенной причиной отказа от использования публичного облака», − сказал Джей Хайзер, аналитик и вице-президент по исследованиям Gartner. «Неоднозначность того, что облачные вычисления фактически дают организации, усугубляется множеством реальных и

воображаемых опасений по поводу последствий для систем безопасности и управления различными облачными моделями».

Всегда затруднительно увидеть будущее какой-либо технологии, но Хейзер смог спрогнозировать будущее облачной безопасности. **В течение 2020 года рабочая нагрузка публичных IaaS будет подвергаться атакам по меньшей мере в 60% случаев реже, чем традиционные data-центры.**

Вывод состоит в том, что положение систем безопасности крупных поставщиков облачных вычислений ничуть не хуже, чем в большинстве корпоративных data-центров, следовательно, безопасность больше не должна рассматриваться как основной замедлитель внедрения публичных облачных сервисов. Тем не менее, это не так просто – перенести рабочую нагрузку на облако, поэтому команды безопасности должны обратить внимание на использование программной инфраструктуры общедоступного облачного IaaS. Автоматизация как можно большего количества процессов предотвращает потенциальные человеческие ошибки. Согласно исследованиям IBM 2014 г. именно человеческие ошибки являются причиной 95% всех инцидентов, связанных с нарушением безопасности [3]. Data-центры предприятий также могут быть автоматизированы, но обычно они не предлагают требуемую программную инфраструктуру.

Согласно прогнозам, внедрение и адаптация инфраструктуры IaaS будет проходить медленнее, и не все облачные провайдеры IaaS будут поддерживать общедоступные облачные IaaS. Службы безопасности и управления рисками должны будут использовать возможности провайдера IaaS и интегрировать тестирование безопасности приложений и другие возможности сканирования уязвимостей в цикл развертывания.

К 2018 году 60% предприятий, которые внедрят соответствующие облачные средства обзора и контроля, будут испытывать на треть меньше сбоев в системе безопасности.

При размещении рабочих нагрузок в облаке никаких компромиссных уступок в плане условий безопасности быть не может. Фактически, облачные провайдеры IaaS предлагают функции, обеспечивающие доступ пользователей только к необходимой им информации, а также отслеживают все детали «Кто, Что, Когда и Где?». Предприятия фактически будут выигрывать от системы безопасности, встроенной в облако.

Облачные вычисления снижают общий уровень безопасности, так как требуется, чтобы клиенты управляли некоторым вычислительным стеком в модели с общей ответственностью. Это хорошая возможность для внедрения новых подходов и принятия новых методов защиты информации. Облако же требует иного подхода к безопасности, поэтому традиционные методы осуществления безопасности на местах не будут актуальны для информации, хранящейся в облаке.

Руководителям служб безопасности и управления рисками необходимо консультировать и обучать свои команды особенностям функций управления видимостью, предлагаемых облачными провайдерами. Стоит внимательно приглядеться к облачным инструментам, чтобы усовершенствовать систему безопасности, это, в свою очередь, приведет к тому, что повседневная защита облака будет зависеть уже от служб безопасности, а не от самих разработчиков [4].

Цикл зрелости для технологий обеспечения безопасности в облаке

Устойчивость к атакам большинства провайдеров облачных услуг пока не подвергалась сомнениям, но клиенты этих служб могут и не знать, как правильно,

а главное, безопасно использовать облако. «Цикл зрелости новых технологий может помочь специалистам по кибербезопасности определить наиболее важные новые механизмы, помогающие их организациям осуществлять контролируемое, совместимое и экономичное использование публичного облака», – утверждает Хайзер.

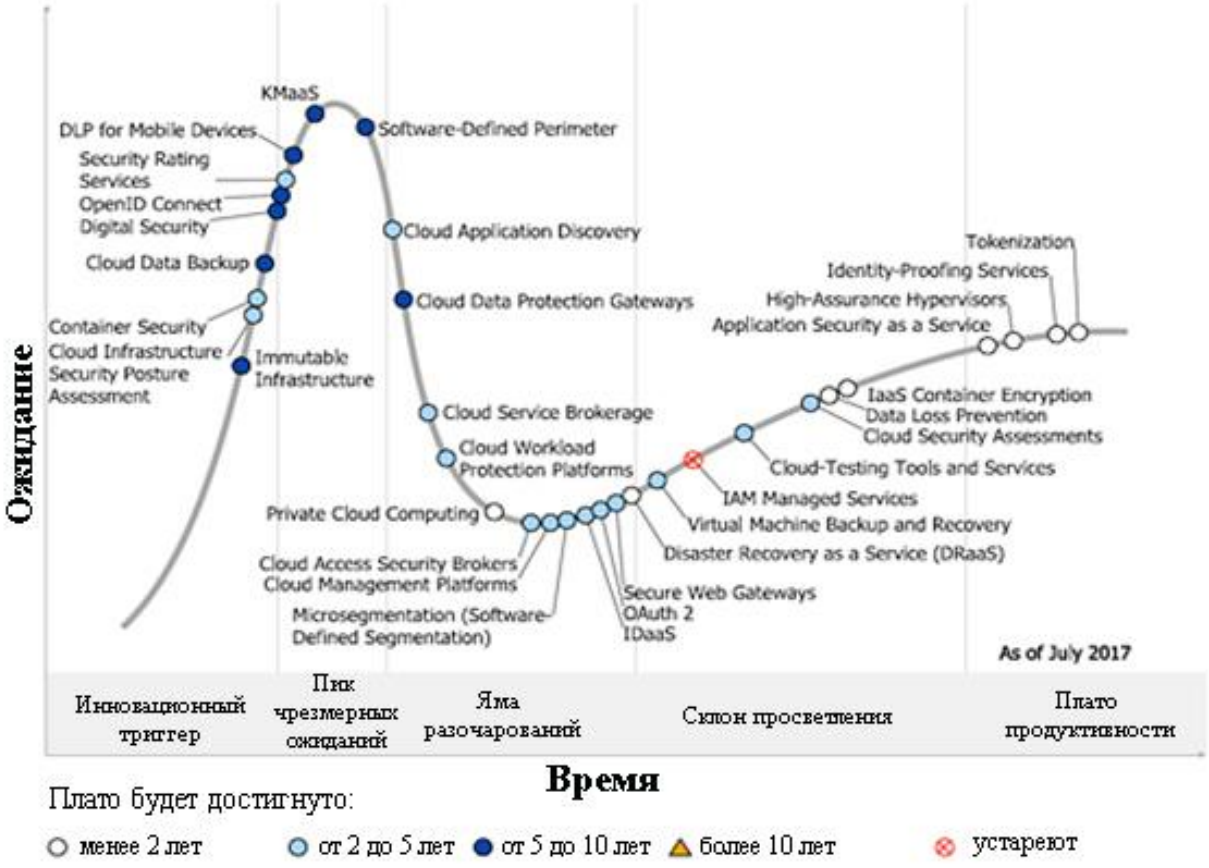

Рис. 1. Цикл зрелости Gartner для облачных технологий, 2017

По мнению аналитиков, каждый технологический тренд проходит 5 этапов:

1. Инновационный триггер – появление новых перспективных технологий.

2. Пик чрезмерных ожиданий – этап чрезмерного энтузиазма и нереалистичных прогнозов, когда реклама не соответствует успешным развертываниям по назначению. В этом году технологии на пике включают защиту от потери данных для мобильных устройств (DLPformobiledevices), ключевое управление как сервис (KMaaS) и программно-оп-ределяемую сеть (Software-definedperimeter). Gartner ожидает, что для достижения полноценного внедрения всех этих технологий потребуется не менее пяти лет.

3. Яма разочарований – технология не оправдывает шумиху пика чрезмерных ожиданий, она становится немодной и движется по циклу к яме разочарования. В этом разделе есть две технологии, которые Gartner ожидает в яме в течение следующих двух лет:

Предоставление услуг, связанных с ликвидацией последствий чрезвычайных ситуаций (*Disaster recovery as a service – DRaaS),* находится на ранней стадии зрелости, с проникновением на рынок от 20% до 50%. Пользуются данными услугами, как правило, небольшие организации с менее 100 сотрудниками, кото-

рым не хватает центра восстановления данных, опытного ИТ-персонала и специализированных навыков, необходимых для управления программой DR самостоятельно.

Частные облачные вычисления (Privatecloudcomputing) используются, когда организации хотят, чтобы преимущества публичного облака, такие как ИТ-гибкость, способствовали процветанию и росту бизнеса, но не могут найти облачные сервисы, которые отвечают их потребностям с точки зрения нормативных требований, функциональности или защиты интеллектуальной собственности. Использование сторонних специалистов для создания частных облаков быстро растет, т.к. стоимость и сложность построения реального частного облака часто высоки.

4. Склон просветления – этап, заключающийся в том, что эксперименты и упорная работа с новыми технологиями начинают окупаться в различных организациях. В настоящее время на склоне есть две технологии, которые Gartner ожидает видеть созревшими в течение следующих двух лет:

– защита данных (Data loss protection – DLP) воспринимается как эффективный способ предотвращения случайного раскрытия регламентированной информации и интеллектуальной собственности. На практике это оказалось более полезным в случаях выявления недокументированных или неработающих бизнес-процессов, которые приводят к случайному раскрытию данных. Организации с реалистичными ожиданиями считают, что эта технология значительно снижает риски непреднамеренной утечки конфиденциальных данных;

– избирательное шифрование IaaS (*IaaS*ContainerEncryption) – это способ для организаций защитить свои данные, хранящиеся у облачных провайдеров. По аналогии с шифрованием жесткого диска на ноутбуке, только в масштабах всех процессов или приложений, хранящихся в облаке. Вероятно, IaaSContainerEncryption станет ключевой функцией, поддерживаемой облачными провайдерами. Например, Amazon уже предлагает собственное бесплатное предложение в этой области, а Microsoft поддерживает бесплатные инструменты BitLocker и DMcrypt для Linux.

5. Плато продуктивности – наконец технологии достигли плата производительности, т.е. преимущества технологии в реальном мире были продемонстрированы и признаны.Например, токенизация (Tokenization), гипервизоры с высокой степенью достоверности (high-assurancehypervisors) и безопасность приложений как служба (Applicationsecurityasservice)поднялись на плато и присоединившись к службам проверки подлинности (identity-proofing services).

«Понимание относительной зрелости и эффективности новых технологий облачной безопасности и сервисов поможет профессионалам в области безопасности переориентировать свою роль на расширение бизнеса», – говорит Хейзер. «Это означает, что ИТ-пользователи организации должны обеспечиваться безопасным и эффективным доступом к облачным службам для их использования и управления» [5].

Gartner также прогнозирует, что мировой рынок услуг Cloud Service Brokerage (CSB) будет расти и совокупный ежегодный темп роста повысится на 19,8% по сравнению с 2013 годом [6].

Заключение

По мере того как облачные хранилища набирают популярность, все большее внимание уделяется вопросу безопасности облака. Более того, безопасность часто является причиной отказа от использования публичного облака. Вероятно, облако подвергается атакам в том случае, если облачная служба стала неустойчивой и небезопасной, исходя из повышенных требований со стороны компаний.

Безопасность, надежность и конфиденциальность также являются частью кибербезопасности всей инфраструктуры компании. Когда эти системы начинают давать сбой, в первую очередь, человек, становится ответственным за безопасность рабочих и производственных сред, а также всех активов компании.

Когда дело доходит до облака, специалистам по безопасности нужно решить, кому они могут доверить свое облако, а кому нет. Компании должны разработать рекомендации по безопасности для частного и публичного использования облака и внедрить модель принятия решений для облачных вычислений для регламентации мер относительно облачных рисков.

Библиографический список

1. Просто о корпоративном IaaS: что это, для кого и как оплачивается [Электронный ресурс]. 2015. URL: https://habrahabr.ru (дата обращения: 05.10.2017).

2. Cloud security and IoT are the new peanut butter and jelly [Электронный ресурс]. 2017. URL: http://www.techproresearch.com/ (дата обращения: 05.10.2017).

3. John W. Coffey. Ameliorating Sources of Human Error in CyberSecurity: Technological and Human-Centered Approaches // The 8th International Multi-Conference on Complexity, Informatics and Cybernetics, Pensacola, 2017. Pensacola: University of West Florida, 2017. С. 85–88.

4. I stheCloudSecure? [Электронный ресурс]. 2017. URL: https://www.gartner.com (дата обращения: 07.10.2017).

5. Hype Cycle for Cloud Security, 2017. [Электронныйресурс]. 2017. URL: https://www.gartner.com (дата обращения: 07.10.2017).

6. Gartner's Hype Cycle For Cloud Security, 2017 Update [Электронныйресурс]. 2017. URL: https://www.forbes.com (дата обращения: 08.10.2017).

Бобрышева Галина Владимировна
Пензенский государственный университет, г. Пенза, Россия
E-mail: g_bobr@mail.ru

Bobrysheva G.V.
Penza State University, Penza, Russia

Пудовкина Елена Михайловна
Пензенский государственный университет, г. Пенза, Россия

Pudovkina E.M.
Penza State University, Penza, Russia