ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБУЧАЮЩИХ СИСТЕМ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Гуринович А.В, Глухова Л.А. (Республика Беларусь, Минск, БГУИР)

Угрозы, возникающие при переходе обучающих систем на облачные технологии, условно разделяются на два вида: возникающие из-за потери контроля над вычислительными ресурсами и возникающие из-за разделения общих ресурсов между клиентами [1].

Учреждение образования (УО), прежде применявшее собственные вычислительные системы и перешедшее на использование облачных технологий, может столкнуться с проблемами доверия к физической безопасности центра обработки данных, аппаратному и программному обеспечению, процессу управления и администрирования вычислительных ресурсов. Физическая организация центра обработки информации может не удовлетворять требованиям безопасности клиента, а сохранность данных в системе может быть нарушена третьей стороной [1]. Серьезным источником проблем могут быть и служебный персонал поставщика облачных услуг, имеющий полный доступ к данным клиента.

Использование облачных технологий может нести угрозы внезапного прекращения работы (при банкротстве поставщика), перерасхода финансовых ресурсов (при недостаточно ясной системе платежей и отсутствии средств мониторинга), непредсказуемости качества сервиса во времени и ухудшения качества обслуживания из-за невозможности выполнения контактных обязательств. Важное значение имеют и вопросы соответствия законодательству стран, где функционирует УО и оказываются образовательные услуги.

Разделение ресурсов с другими клиентами может представлять угрозу прямого вмешательства злоумышленника [2]. Злоумышленник может использовать неявные методы извлечения данных. Кроме того злоумышленник может использовать специальные техники для выполнения атак вида “кража ресурсов” и “отказ в ресурсах”. Использование общих вычислительных мощностей может привести к угрозе побочного ущерба репутации (например внесения адресов сервера в черные списки). Использование облачных услуг лишает организацию возможностей прямого управления инфраструктурой и активного поиска и противодействия атакам.

Угрозы, возникающие из-за человеческого фактора, могут быть устранены соответствующими мерами контроля и аудита выполняемых операций на стороне поставщика. Для сокращения рисков могут быть описаны типичные процедуры поставки, обслуживания и реагирования на инциденты. Перерасход финансовых ресурсов может быть отслежен и предотвращен установкой квот на использование, применением систем мониторинга расходов и быстрым уведомлением об аномалиях в потреблении.

Проблемы с ухудшением качества обслуживания и непредсказуемостью выделенных ресурсов можно решить установлением строгого договора о качестве обслуживания (SLA), который будет регламентировать технические характеристики предоставляемых услуг (сетевая доступность, функциональное соответствие, производительность).

Часть проблем, возникающих при совместном использовании общих ресурсов, можно предотвратить, используя частные облака или выделенные программно-аппаратные ресурсы. Это несколько снижает экономическую и вычислительную эффективность облаков.

Существуют стандарты для оценки безопасности ИС. Так, стандарт ISO 27002:2005 описывает технические меры контроля и обеспечения безопасности ИС, оценки угроз и рисков без специфики облачных услуг. А стандарты NIST SP 800-53 (FedRAMP) и CSA CCM/CAIQ, рассматривают угрозы, возникающие при использовании облачных услуг, и содержат готовые рекомендации для обеспечения безопасности ИС в облаке [2].

В докладе выполняется сравнительная оценка различных угроз, возникающих в УО при использовании облачных технологий, даются практические рекомендации по их устранению.

Литература

[1] Molnar, D., Schechter, S.E.: Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud; In WEIS (2010).

[2] Vaquero, M., Locking the sky: a survey on IaaS cloud security; Springer Vienna (2011).