ОСОБЕННОСТИ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЛАЧНЫХ РЕСУРСОВ

А.В. Шанцов

Белорусский государственный университет, г. Минск;
ShantsovAV@bsu.by;
науч. рук. - Кочин В. П., канд. тех. наук, доц.

Рассмотрено влияние облачных вычислений на информационную безопасность информационных ресурсов при их переносе или развертывании на облачных платформах. Определена актуальность проблемы защиты информационных ресурсов, размещенных на облачных платформах, в том числе и для Республики Беларусь. Выделены основные особенности облачных вычислений, влияющие на защищенность информационных ресурсов, такие как: модель совместной ответственности провайдера и клиентов облака по обеспечению информационной безопасности; необходимость в защите среды виртуализации и изоляции виртуальных ресурсов клиентов облака; необходимость доработки архитектур ресурсов и средств безопасности для их функционирования в облачной среде; необходимость налаженного взаимодействия между провайдером и клиентами облака при организации аудита и реагировании на инциденты. Предложены общие подходы по реализации комплексной системы защиты информации облачных ресурсов.

Ключевые слова: информационные технологии; информационная безопасность; облачные вычисления.

ПРИЧИНЫ ПЕРЕХОДА К ОБЛАЧНЫМ ВЫЧИСЛЕНИЯМ И АКТУАЛЬНОСТЬ ДАННОГО ПРОЦЕССА ДЛЯ РЕСПУБЛИКИ БЕЛАРУСЬ

В основу облачных вычислений положена модель совместного использования ресурсов (аппаратного и программного обеспечения) центров обработки данных (далее – ЦОД). Данная модель имеет ряд существенных преимуществ по сравнению с моделью традиционных вычислений:

- Существенное снижение затрат. По сравнению с развертыванием собственных ЦОД каждой организацией в отдельности, использование облачных вычислений позволяет клиентам облака использовать и оплачивать только необходимые им ресурсы. Такая гибкость при аренде вычислительных ресурсов обеспечивает существенную экономию средств.
- Передача части ответственности по защите ресурсов облачному провайдеру.
- Возможность использовать средства защиты информации (далее – СЗИ) облачного провайдера вместо развертывания собственных.
- Возможность передачи на аутсорсинг облачному провайдеру обслуживание СЗИ ресурса (услуги).

Помимо экономических эффектов и возможностей по использованию СЗИ облачных провайдеров, в Республике Беларусь для государственных организаций нормативными правовыми актами определены требования по размещению информационных ресурсов, в том числе и на облачных платформах [1].

Тем не менее, облачные вычисления, из-за своих особенностей, вместе с преимуществами вносят повышенные риски информационной безопасности и более ограниченную возможность управления ресурсами. Для нивелирования данных рисков, система защиты информации облачных ресурсов должна учитывать особенности облачных вычислений [2].

ОСОБЕННОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ, ВЛИЯЮЩИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕСУРСОВ

1. Наличие «третьей стороны» – облачного провайдера. Наличие облачного провайдера является одной из основных особенностей в облачных вычислениях, которая изменяет модель распределения ответственности по обеспечению информационной безопасности ресурсов и приводит к переходу к модели совместной или распределенной ответственности. Однако, несмотря на то что облачные провайдеры берут на себя часть ответственности по обеспечению защиты информационных ресурсов, клиенты облачных вычислений несут ответственность за сохранность данных своих пользователей и за определение необходимых СЗИ для обеспечения безопасности их ресурсов [3].

2.Необходимость изменения (доработки) архитектуры приложения (услуги). Перенос информационного ресурса (приложения, сервиса) в облако, с сохранением его прежней архитектуры, негативно скажется на его степени защищенности. Архитектуры сервисов, приложений, не рассчитанных на облачные вычисления, как правило, являются более уязвимыми при их размещении в облаке [4, с 108-118].

3.Функционирование традиционных СЗИ в облаке. Данная особенность связана с тем, что без адаптации традиционных СЗИ под модель облачных вычислений их функционирование в облаке не будет отвечать необходимым критериям [4, с 77-90].

4.Совместное использования физических ресурсов. Из-за постоянного перераспределения физических ресурсов (память, накопители, процессоры) в облаке возникают угрозы утечки информации. В дополнение к этому, ресурсы отдельных клиентов могут быть использованы для противоправных действий в отношении других клиентов этой же платформы [4, с 91-99].

5.Платформа виртуализации. Гипервизор – основа виртуализации, обеспечивающая разделение ресурсов аппаратной платформы между виртуальными машинами (далее – ВМ). Вмешательство в работу гипервизора может привести к несанкционированному захвату ресурсов ВМ, перехвату сетевого трафика, похищению ВМ при их миграции.

6.Перенос данных в облако. В большинстве случаев перенос данных в облако не будет осуществляться в ручном режиме. Потенциальная угроза заключается в ненадежном и/или неправильно сконфигурированном механизме переноса данных клиентов в облако.

7.Аудит и реагирование на инциденты. По сравнению с традиционными вычислениями, облако существенно снижает способность клиентов осуществлять аудит. Аналогичная ситуация складывается при реагировании на инциденты [4, с 57-59, 101-107].

8.Вопросы юрисдикции. При использовании облачных услуг данные клиентов могут обрабатываться в иностранных юрисдикциях. В связи с этим возникает ряд вопросов по доступности данных, возможности их раскрытия третьим сторонам и т.д. [5]

РЕКОМЕНДАЦИИ ПО ПОСТРОЕНИЮ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЛАЧНЫХ РЕСУРСОВ

1. Определить архитектуру системы защиты информации облачных ресурсов. Выполнить оценку рисков для развертываемого информационного ресурса (услуги) и определить все необходимые СЗИ. Изучить СЗИ, предоставляемые облачным провайдером и определить перечень СЗИ, которые должны быть реализованы дополнительно. В случаях невозможности исключения всех возможных рисков, принять меры по управлению ими (например, страхование).

2. Изменить архитектуру ресурсов (приложений, услуг) для функционирования в облаке. Реализовать мониторинг активности в использовании интерфейсов приложений. Расширить внутренние возможности ресурса по аудиту. Использовать возможности облачных вычислений для повышения доступности ресурсов (распределенное хранилище, распределенные вычисления и др.).

3. Использовать сертифицированные/стандартизированные облачные платформы. Проверить наличие у облачного провайдера сертификатов (аттестатов) соответствия регулирующим техническим нормативным правовым актам и передовым практикам в области защиты информации.

4. Применять по возможности криптографические алгоритмы (шифрование) при хранении и передаче данных.

5. Наладить взаимодействие с облачным провайдером по проведению аудита и при реагировании на инциденты.

6. Узнать, по возможности согласовать, с провайдером юрисдикцию в которой будет размещен ресурс.

ЗАКЛЮЧЕНИЕ

В настоящее время облачные вычисления нашли широкое применение в различных сферах деятельности. Облачные вычисления открывают перед пользователями ряд существенных преимуществ, среди которых особенно выделяются сокращение затрат на развертывание информационных ресурсов и предоставление широких возможностей по повышению их защищенности (доступности).

Однако надежное обеспечение безопасности информационных ресурсов (приложений, услуг) становится возможным лишь в случае правильного построения системы защиты информации. Проблема построения надежной системы защиты информации является сложной и требует комплексного подхода к ее решению. Только в случае учета всех особенностей, вносимых облачными вычислениями, становится возможным создание надежной системы защиты информации облачных ресурсов.

Библиографические ссылки

1. Указ Президента Республики Беларусь от 23.01.2014 № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий» с изменениями, утвержденными Указами Президента Республики Беларусь от 31.12.2015 № 542, от 16.12.2019 № 461.
2. National Institute of Standards and Technology, Special Publication 500-292 «Cloud Computing Reference Architecture».
3. National Institute of Standards and Technology, Special Publication 500-299 «Cloud Computing Security Reference Architecture».
4. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing.
5. Шекель Н.В. Юридические аспекты использования облачных технологий // Журнал международного права и международных отношений. 2014. Т. 4(71): 3-7.