ОБЗОР И АНАЛИЗ БЕЗОПАСНОСТИ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В.А.Вишняков, Гондаг Саз Мостафа

Облачные вычисления (ОВ) — технология для обеспечения вычислительными ресурсами и предоставление услуг через Интернет для пользователей. Хотя ОВ имеют много преимуществ, но очень важно обеспечить безопасность работы пользователей и их распознавание.

Выделены классы угроз в среде ОВ, связанные с атаками: на ПО, на элементы облака, на клиента, на гипервизор, на системы управления; а также угрозы виртуализации, перенос виртуальных машин. Представлен класс угроз превышения полномочий пользователей, в том числе за счет взаимного влияния пользовательских задач на вычислительных узлах, приводящих к несанкционированному доступу пользователей к данным. Анализ механизмов безопасности в системах ОВ показал, что защита от присоединения к ОВ неавторизованных компонентов обеспечивается с помощью механизмов взаимной аутентификации пользователей и провайдеров ресурсов с использованием цифровых сертификатов X.509, шифрования и цифровой подписи информации, передаваемой между узлами сред ОВ.

Основные аспекты безопасности пользователя в ОВ:

– конфиденциальность, для ее обеспчения имеются два основных метода: физическое разделение и шифрование. 2. Целостность: два основных подхода к ее достижению: a) кода аутентификации сообщения (MAC: Message Authentication Code); b) цифровую подпись (Digital signature). 3. Доступность: убедится, что пользователи могут получить доступ к Интернет в любое время и в любом месте.

СОСТАВ БЕЗОПАСНОЙ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Гондаг Саз Мостафа, В.А.Вишняков

В докладе представлены элементы предлагаемого подхода для безопасной работы пользователей в среде облачных вычислений. Участники взаимодействий: пользователь (пользователям могут быть физические лица и организации), аутентификатор подлинности (Trusted Authenticator — TA), облачный провайдер услуг (Cloud Service Provider — CSP), цифровая подпись (Digital Signature — DS), агент CSP's. Ниже представлены функции элементов данного подхода.

1. Пользователь имеет ограниченный доступ к услугам из облака предлагаемых услуг, он запрашивает облачные ресурсы у CSPs.

2. TA устанавливает соединение доверительные отношения с органом аутентификации. Задача TA в облачной среде − обеспечить пользователю безопасный доступ к облачным сервисам через поставщика услуг.

3. Облачный провайдер услуг (CSP). Облачный сервис может динамически масштабироваться для удовлетворения потребностей пользователей, потому что поставщик услуг предоставляет необходимое для обслуживания оборудование и программное обеспечение.

4. Цифровая подпись (DS), является электронной подписью, которая идентифицирует личность отправителя сообщения или подписавшего документ, и удостоверяет, что оригинальное содержание посланного сообщения или документа, не изменилось.

5. Агенты CSP's способны принимать решения на выполнение задач от имени своих пользователей. Агенты имеют право взаимодействовать с другими агентами путем переговоров, сотрудничества и координации. В CSP, агент работает для предоставления услуг, обслуживания переговоров, услуг сотрудничества и их координации.