УДК 37.075.8

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Ходько В.В., Дрозд А.В.
Научный руководитель - Околов А.Р., к.т.н., доцент

Облачные вычисления - это модель предоставления вычислительных ресурсов по требованию, охватывающая всё, начиная от приложений до центров обработки данных, через Интернет при условии оплаты за фактическое использование. Такой подход к организации вычислений дает небывалые возможности клиентам, независимо от мощности их компьютеров и при этом обеспечивает доступ к облаку миллионам пользователей в каждый момент. Однако, при такой заманчивости использования облачных платформ, пользователи предъявляют к ним и высокие требования, связанные с сохранностью данных и их защищенностью.

Надежность хранения данных. Поставщики облачных решений хранят данные на своих сервисах с использованием избыточности, что само по себе гарантирует надежность. Дополнительно к этому, на любом из устройств, подключенных к "облаку", хранится, ещё как минимум, еще одна актуальная копия данных

Сохранность данных. Лучший способ защиты расположенных в хранилище данных – использование шифрования (используется, как минимум, протокол SSL, а в некоторых RSA+AES). С целью предотвращения случаев неправомерного доступа, провайдер должен шифровать хранящуюся на своих серверах информацию клиента, безвозвратно удалять данные, когда они больше не нужны и не потребуются в будущем.

Защита данных при передаче. Передаваемые данные должны быть зашифрованы и доступны пользователю только после аутентификации. Это является гарантией того, что эти данные не сможет изменить или прочитать ни одно лицо, даже если оно получит к ним доступ посредством ненадежных узлов сети. Эти технологии давно известны, созданы надежные протоколы и алгоритмы, такие как TLS, IPsec и AES.

Аутентификация. Самым распространенным способом аутентификации является защита паролем. Однако некоторые провайдеры, для обеспечения более высокой надежности, прибегают к помощи таких средств, как сертификаты и токены. Желательно, что бы провайдеры имели возможность работы с такими стандартами как LDAP и SAML. Это важно для обеспечения прозрачного взаимодействия провайдера с системой идентификации пользователей клиента при авторизации и определении выдаваемых пользователю полномочий.