УДК 37.075.8

Защита информации при использовании облачных платформ

Околов А.Р., Дрозд А.В., Ходько В.В.
Белорусский национальный технический университет

Облачные вычисления – это перенос всех вычислений и хранения всех данных в Интернет и взаимодействие клиентов облака через Web-интерфейс облачных приложений. Такой подход к организации вычислений дает небывалые возможности клиентам, независимо от мощности и класса их компьютеров, и при этом обеспечивает доступ к облаку миллионам пользователей в каждый момент. Однако подобный подход создает и проблемы, связанные с безопасностью пользовательских данных (нет уверенности в сохранении конфиденциальности информации, хранящейся на "чужих" компьютерах).

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 еще одна актуальная копия данных.

Безопасность хранения данных в "облаке". Весь трафик между клиентом и "облаком" шифруется (используется, как минимум, протокол SSL, а в некоторых случаях RSA+AES), что очень сильно затрудняет просмотр передаваемой информации посторонними лицами. Поэтому уровень безопасности работы с данными выше, чем, например, при отправке обычным письмом по электронной почте. Некоторые сервисы облачного хранения (SpiderOak, Wuala) предлагают шифрование данных не только при передаче, но и при хранении в "облаке".

Надежным способом защиты информации при размещении в облачном хранилище является применение средств шифрования и для этих целей целесообразно использовать программное обеспечение TrueCrypt, которое является кросс-платформенной программой и поддерживается такими операционными системами как Windows 7/Vista/XP/2000, Linux. Также TrueCrypt поддерживает несколько криптографических алгоритмов блочного шифрования, таких как AES, Twofish, Serpent, позволяет осуществлять каскадное шифрование файлов и предлагает возможность правдоподобного отрицания. Данные алгоритмы являются надежными алгоритмами шифрования – в настоящее время не было обнаружено каких-либо реально реализуемых атак на них. Кроме того, TrueCrypt является свободным программным обеспечением с открытым исходным кодом и может применяться в образовательных учреждениях.