ОБ ИСПОЛЬЗОВАНИИ СРЕДСТВ ЗАЩИТЫ ПРИ РАБОТЕ С ОБЛАЧНЫМИ СЕРВИСАМИ

Ошурков В.А., Майорова Е.С.
ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск

Сегодня под облачными вычислениями понимают возможность получения необходимых вычислительных мощностей по запросу из сети. По прогнозу аналитической компании IDC, за ближайшие 5 лет рынок облачных услуг в России вырастет более чем на 500%, что говорит об актуальности направления. Доступ к облачными сервисам обеспечивается через Интернет посредством обычного интернет-браузера или других сетевых приложений, например, через сетевой диск на ПК. На сегодняшний день безопасность в «облаке» является открытым вопросом. В докладе рассмотрено 3-х ступенчатое обеспечение защиты при работе с облачными технологиями через сетевой диск на ПК (рис.).

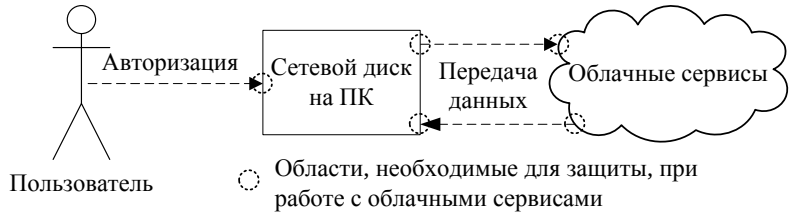

Рис. Модель взаимодействия пользователя с облачными сервисами

На первой ступени т.н. «авторизации» обычно используется схема логин-пароль, необходимая для доступа к сервисам облачного хранилища. Вторая и третья ступень подразумевает более надежную защиту информации. Для работы с файлами на удаленных серверах был разработан протокол WebDAV, позволяющий создавать, редактировать и перемещать документы. Средство WebDAV интегрировано в операционные системы семейства Windows Server 2003 и IIS, что позволяет использовать все преимущества встроенных средств безопасности среды и веб-сервера, включая управление разрешениями и списки управления доступом на уровне пользователей файловой системы NTFS.

На сегодняшний день разработано множество WebDAV клиентов для работы с файлами популярных хранилищах как SkyDrive, Dropbox, GoogleDrive и пр. Например средство CarotDAV для шифрования файлов использует симмертичный алгоритм блочного шифрования AES256. Еще один клиент Duplicati предлагает на выбор шифрование встроенной библиотекой SharpAESCrypt или средствами GnuPG.

Во избежание хищения информации при работе с облачными сервисами, нами было представлено 3-х ступенчатое обеспечение защиты, являющееся основополагающим фактором защиты данных пользователя и, как следствие, благополучной работы этих сервисов.