УДК 004.056.55

Безопасность информации в облачных хранилищах

Пешков О.О. студент 1 курса
Научный руководитель – Мелешко Е.В, к.т.н, доцент
Центральноукраинский национальный технический университет, г. Кропивницкий

Облачное хранилище (ОХ) - онлайн-хранилище, в котором данные хранятся на большом количестве распределённых по всему миру сетевых серверах, предоставляемых провайдером для нужд своих пользователей. Будь-то обычный пользователь, фирма или банковская компания.

Данные обрабатываются и хранятся в так называемом «облаке», которое является одним большим виртуальным сервером. С помощью ОХ пользователь сможет получить доступ к персональным данным с любого устройства, имеющего выход в сеть Интернет.

Популярные облачные сервисы для хранения данных - Microsoft OneDrive, Google Drive и Apple iCloud.

Удобство использования облачного хранилища. Со стремительным развитием технологий будет стремительно увеличиваться потребность в хранении большого количества информации, поскольку это оптимальное решение потребностей в хранении данных не только для обычных пользователей, но и для разного рода бизнес предприятий, для которых использование облачного хранилища является хорошим вместилищем данных без затрат денежных ресурсов на покупку дорогого оборудования и выделения для него территории.

Корпоративные предприниматели все же могут строить частные «облака», размещая серверное оборудование на собственной территории. Такой тип сервисов пользуется особым спросом, где заказчики предпочитают лучше сохранять «полный» контроль над своими данными. Данный метод действительно является хорошим способ защитить свои данные от нежелательной утечки. И, тем не менее, такой способ хранения не защитит данные на 100%, ведь всегда присутствует человеческий фактор. В большинстве стран, если поступит официальный запрос, компетентные органы имеют право получить доступ к любым хранилищам данных.

Защита информации в облачном хранилище. Действенного решения в 100% случаях, очевидно, нет, но можно смело утверждать, что основой для любой архитектуры в информационной безопасности служит криптография. Повсеместно криптография используется для защиты интернет-коммерции и глобальных платежных сервисах, провайдеры облачных хранилищ могут довериться ей как лучшему способу гарантировать защиту, которая предотвратит потерю данных и сохранит

целостность и доступность для своих потребителей.

Относительно, криптографии и других способов защиты информации в облачном хранилище, такие решения существуют, но они есть только для того, чтобы усложнить проникновение тому, кто хочет получить ваши данные. Решений, позволяющих гарантировать 100% защиту информации, нет, так что, если в облаках будут храниться действительно важные данные, вероятность потери конфиденциальности этих данных резко возрастает.

Защита данных со стороны пользователя

1) Самый простой в использовании способ защиты это - RAR-архив, в котором есть пароль. Файлы, входящие в архив, будут иметь зашифрованные имена, которые будут понятны только владельцу. Это наиболее приемлемый способ, большое количество пользователей пользуются архивами по всему миру, это мешает выделить информацию конкретного пользователя среди большого количества всей остальной информации, вдобавок архив еще будет иметь пароль.

2) TrueCrypt – это open-source криптографическое программное обеспечение, которое создает на жестком диске криптографический контейнер, в который можно поместить файлы, или папки с файлами.

3) Использование облачных сервисов, в которых процесс шифрования автоматизирован. Это в частности, SpiderOak и Wuala. Принцип их работы следующий, перед передачей информации на сервер она шифруется пользователем локально, в результате – что хранится на серверах не знают даже сами владельцы сервера, так как ключ находиться в пользовательском ПО. Процесс установки и настройки клиента SpiderOak слегка сложнее, чем Dropbox, зато присутствуют уникальные возможности, например, защита паролем файлов с открытым доступом некоторому кругу лиц и т.д.

4) Шифрование файлов по отдельности – при небольшом количестве файлов, есть смысл просто запаковать нужные файлы в зашифрованный архив. Для этих целей отлично подходит популярный архиватор 7zip.

5) Простая осторожность – следует уделить большое внимание настройкам безопасности пользовательского аккаунта в облачных хранилищах и всех остальных сервисах: использовать безопасное https-соединение, придумывать сложные пароли и игнорировать не запрошенные сообщения от неизвестных личностей – ссылки в таких сообщениях могут вести на вредоносное программы или фишинговые сайты.