УДК 661

Студ. К. В. Тозик
Науч. рук. ассист. С. А. Осоко
(кафедра информатики и веб-дизайна, БГТУ)

ЗАЩИТА ИНФОРМАЦИИ В ОТКРЫТЫХ ОБЛАЧНЫХ ХРАНИЛИЩАХ

Облачное хранилище данных – модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам в основном третьей стороной.Облачными хранилищами являются такие интернет-сервисы как: Dropbox, OneDrive, GoogleDrive, iCloud, Яндекс Диск, облако Mail.Ru [1].

У данных интернет сервисов есть много плюсов, например, возможность доступа к данным с любого компьютера, имеющего выход в Интернет, возможность организации совместной работы с данными, высокая вероятность сохранения данных даже в случае аппаратных сбоев и другие. Однако, главный вопрос, возникающий при использовании данных облачных хранилищ это насколько безопасно хранить данные в таких интернет-сервисах. В 2011 году одна аналитическая фирма провела исследования в данной области, которое показало, что 68% опрошенных руководителей европейских IT-компаний в целях безопасности отказываются использовать облачные технологии из-за того, что данные могут стать достоянием общественности[2–3]. Например, провайдер имеет возможность просматривать данные клиента (если они не защищены паролем), которые так же могут попасть в руки хакеров, сумевших взломать системы защиты провайдера. Так же известны несколько инцидентов, связанных с утечкой данных с облачных хранилищ. Так как же можно тогда защитить свою информацию в открытых облачных хранилищах?

Цель работы: рассмотреть, сравнить и проанализировать способы защиты информации при хранении в открытых облачных хранилищах. Наверно, один из самых простых способов, это создание запароленного архива с помощью программ WinRARи 7-Zip. Каким образом это сделать? Порядок действий в этих программах практически не отличается. При использовании WinRAR для начала необходимо выбрать папку, которая будет помещаться на облачном хранилище, нажать правой кнопкой мыши, в появившемся списке выбирается «Добавить в архив». В открывшемся окне выбирается «Установить пароль». Устанавливается пароль и далее, при открытии данного архива и разархивировании папки будет запрашиваться пароль.

При использовании 7-Zip так же выбирается папка и нажимается по ней правой кнопкой мыши. В появившемся списке выбирается «Добавить в архив». На следующем шаге необходимо найти раздел «Шифрование», который показан на рисунке 1. В поле под цифрой 1 вводится пароль, в поле под цифрой 2 подтверждается этот пароль и нажимается кнопка «ОК». В результате чего появляется заархивированная папка, при открытии или разархивировании которой так же будет запрашиваться пароль. Данный способ, наверно, один из самых простых и легкодоступных. Однако не самый удобный.

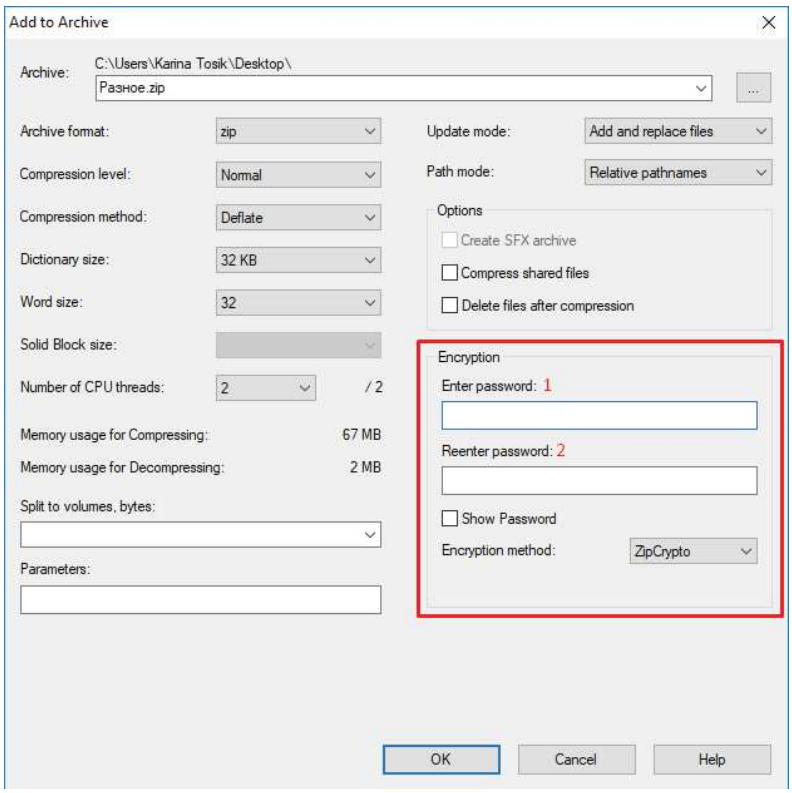

Рисунок 1 – Окно шифрования в программе 7-Zip

Имеется программное обеспечение SpiderOak, которое разработано компанией SpiderOakInc., которое предназначено для резервного копирования пользовательских данных и дальнейшего хранения на «облаке». Информация предоставляется на сервер только в зашифрованном виде, а пароль не передаётся никогда, кроме тех случаев, когда пользователь работает с веб-интерфейсом. Также имеется возможность синхронизации файлов и папок на нескольких устройствах одновременно и автоматического устранения дублирования файлов. Данная программа использует многоуровневый подход к шифрованию, используя комбинацию 2048 бит RSA и 256-битное AES. История изменения файлов ведётся по принципу дельта-кодирования, что-

бы сэкономить место, занимаемое файлами. В истории изменения записывается только отличие версии файла от другой.

Отличительными возможностями данной программы является следующие: экономия места в хранилище и времени выгрузки файлов за счёт дедупликации и внесения изменений в уже имеющиеся в хранилище файлы (вместо перезаписи файлов целиком). Далее настраиваемая мульти платформенная синхронизация.DropBox для синхронизации создаёт специальную папку, в которую надо помещать все синхронизируемые файлы. SpiderOak может работать с любым каталогом; сохранять все хронологические версии файлов и удалённых файлов; получать файлы с любого подключенного к Интернету устройства с полным шифрованием данных по принципу «нулевого знания»; поддерживать неограниченное количество устройств. В качестве плюсов у данной программы можно выделить то, что для взаимодействия с сервисом данные передаются в открытом виде (не шифруются на своей стороне). Поэтому все данные не будут доступны для всеобщего обозрения в случае неполадок, что уже случалось в некоторых альтернативных вариациях облачных технологий. На стороне клиента происходит полное шифрование всех данных. Отсутствие длительных регистраций, регистрация есть, но она сокращена до минимума и не подразумевает длительное заполнение различных форм. Так же у этой программы много других плюсов, которые можно узнать в сети Интернет.

Конечно, говоря о защите информации на облачных хранилищах, не стоит забывать об аутентификации. Защита паролем для обеспечения более высокой надежности. Наиболее простой и достаточно надежный метод аутентификации – это технология одноразовых паролей (OneTimepassword, OTP). Такие пароли могут генерироваться либо специальными программами, либо дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS.

Ещё один метод защиты информации в облачных хранилищах это изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развёрнуты с применением таких технологий, как VPNи VPLS. Часто провайдеры изолируют данные пользователей друг от друга за счёт изменения кода в единой программной среде. Этот подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющем получить доступ к данным. В случае возможной ошибки в коде пользователь может получить доступ к информации другого пользователя. Последнее время такие инциденты часто имели место.

Таким образом, можно выделить 4 наиболее популярные метода защиты информации в «Облачных технологиях»:

1. Шифрование.
2. Защита данных при передаче.
3. Аунтефикация.
4. Изоляция пользователей.

В заключение следует сказать, что безопасность не всегда обеспечивается только защитой. Она может быть достигнута также соответствующими правилами поведения и взаимодействия объектов, надёжность всех видов обеспечения функционирования объектов информационной безопасности.

ЛИТЕРАТУРА

1. Сравнение облачных хранилищ – самые популярные облака: https://www.boxcryptor.com/ru/blog/post/list-best-clouds-private-use/.
2. Защита информации в «Облачных технологиях» как предмет национальной безопасности:https://moluch.ru/archive/86/16357/.
3. Безопасность облачных хранилищ: https://moluch.ru/conf/tech/archive/286/13236/.

УДК 004.451.642

Студ. В. В. Назаренко
Науч. рук. ст. преп. Т. В. Кишкурно
(кафедра информатики и веб-дизайна, БГТУ)

ТЕМНЫЕ ПАТТЕРНЫ: ИСПОЛЬЗОВАНИЕ UX ДИЗАЙНА ДЛЯ ОБМАНА ПОЛЬЗОВАТЕЛЕЙ

Опыт пользователей прошел большой путь за последнее десятилетие, особенно в мире веб-дизайна. Сейчас, как никогда ранее, люди больше сосредоточены на том, чтобы убедиться, что пользователю не только легко, но и нравится продукт или услуга, которые они используют.Но пока большинство людей работают над созданием более удобной и приятной для пользователя сети, некоторые работают, чтобы обмануть пользователя и обмануть его с помощью методов UX, известных как темные паттерны [1].

Темные Паттерны – это пользовательские интерфейсы или методы взаимодействия с пользователем, разработанные специально для того, чтобы обмануть людей. Эти методы могут быть относительно безвредными и оставить только чувство раздражения у пользователя. Другие, однако, могут стоить пользователю гораздо больше в финансовом или даже профессиональном плане. Хотя их не следует путать с антипаттернами, которые являются обычной практикой, приводящей к плохому UX (и не преднамеренно вводящей в заблуждение).