Р.А. Лобов, А.И. Мартышкин

ОБЗОР СИСТЕМ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В ОБЛАЧНЫХ ХРАНИЛИЩАХ

Россия, г. Пенза, Пензенский государственный технологический университет

The article is devoted to the review of systems of encryption and decryption of confidential data in cloud storage. Cloud technologies are popular among active Internet users, as they provide a wide range of services in terms of multi-user structure, ease of operation, and cost-effectiveness. Users, using cloud technologies, improve the quality of their work, which leads to the popularization of "clouds" in the IT services market. One of the advantages of using cloud technologies is their cost-effectiveness. The purpose of the article is to compare the currently available programs for encrypting and decrypting confidential data in cloud storage, to identify their advantages and disadvantages. To achieve this goal, you need to solve a number of tasks: analyze the currently operating systems for encrypting and decrypting confidential data; identify their advantages and disadvantages; consider the characteristics of the system that meets the requirements of users. The main criterion for choosing the encryption method is fast access to the necessary files on the cloud storage to work with them: updates or decryptions.

Введение. Проблема информационной безопасности является наиболее актуальной в современном мире. Переход на дистанционное обучение на всех уровнях образования, удаленную работу общества всего мира, приводит к появлению глобальной проблемы современности: как сохранить большой объем информационных данных? Информационная безопасность затрагивает не только вопросы стабильности и благополучия общества, но и формирования потенциала всей страны.

Среди активных пользователей сети интернет огромной популярностью пользуются облачные технологии, потому что предоставляют широкий спектр услуг [1, 2].

Целью настоящей работы является сравнение доступных на сегодняшний день программ шифрования и дешифрования конфиденциальных данных в облачных хранилищах, выявление их недостатков. Для достижения указанной цели требуется решить ряд задач: проанализировать работающие на данный момент системы шифрования и дешифрования конфиденциальных данных; выявить их достоинства и недостатки; рассмотреть характеристики системы, отвечающей требованиям пользователей.

Анализ предметной области. Самыми известными облачными хранилищами на 2017-2020 год являются следующие интернет-сервисы: «DropBox»; «Google Drive»; «Newxcloud» и т.п. Поскольку организациям очень важно не допустить утечки информации, то необходимо выбирать облачные сервисы, обеспечивающие безопасность, т.е. элементы управления должны аутентифицировать приложения и пользователей. Клиентам облачных сервисов очень важно шифрование своих данных. Но хакерам все равно удается добиться утечки конфиденциальной информации. Поэтому необходимо разработать систему с хорошей защитой конфиденциальных данных, отвечающей требованиям пользователей облачных вычислений.

Материалы, методы и ход исследования. Основным критерием выбора метода шифрования является хороший, быстрый доступ к необходимым файлам на облачном хранилище для работы с ними: обновления или дешифрации [3]. А также невозможность передачи огромных потоков паразитных данных и доступный, русскоязычный, приятный глазу, интерфейс.

Итак, рассмотрим более подробно уже существующие системы, предназначенные для хранения конфиденциальных данных.

1. «Сервисы для защиты частных данных пользователей и компаний в случае, если они хранятся облачными сервисами – Boxcryptor, Cloudfogger и т.п.» [4].

Принцип работы у всех один: пользовательские данные для шифровки берутся из всех нужных файлов, в дальнейшем подключаются библиотеки Dokan или Eldos CBFS. [5]. На рисунке 1 показан интерфейс программы «Boxcryptor».

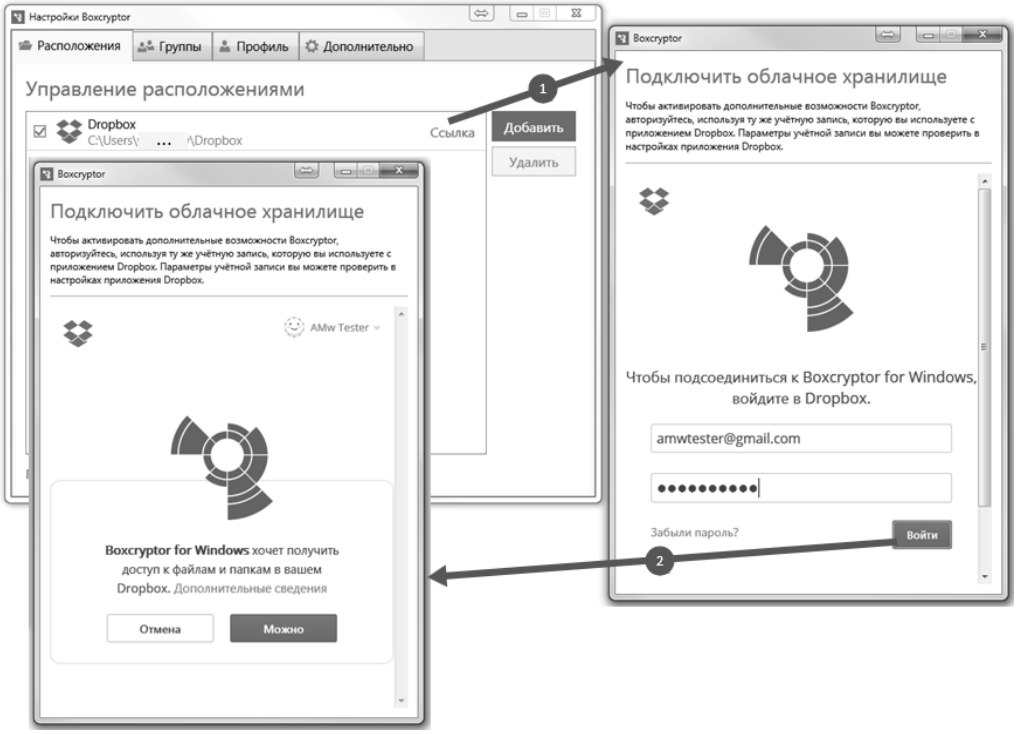

Рисунок 1 – Интерфейс программы «Boxcryptor»

Недостатками данных сервисов являются:

- очень ограниченный набор функций в бесплатных версиях;
- при использовании множества файлов происходит большая нагрузка на систему;
- не поддерживают отечественных провайдеров таких, как Mail.ru и Яндекс.Диск (есть только у Boxcryptor).

2. Webdav клиент Carotdav. Помимо webdav-облаков, поддерживаются SkyDrive, Dropbox, GoogleDrive, Box, SugarSync и FTP(S) [3]. Интерфейс данного сервиса можно увидеть на рисунке 2.

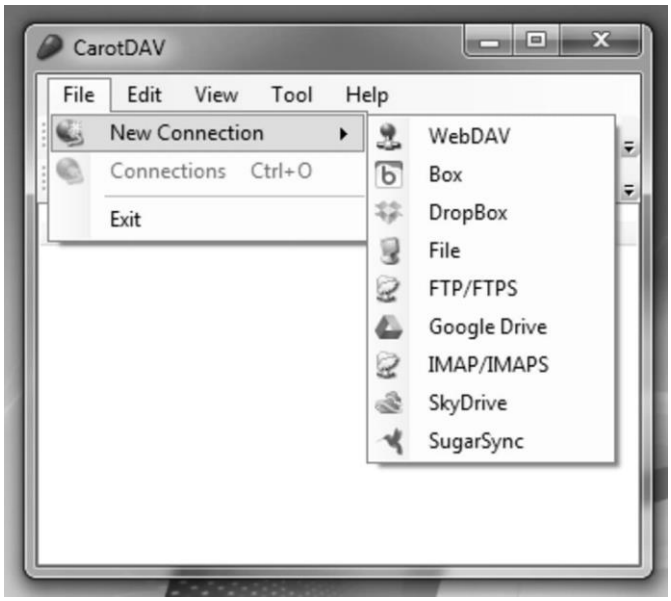

Рисунок 2 – Интерфейс программы «CarotDAV»

Недостатками данной системы являются:

- нет локализации под отечественный рынок;
- нет поддержки отечественных провайдеров;
- возникают частые ошибки при работе с некоторыми webdav облаками. При решении проблемы увеличивается время на обработку;
- проблемы при использовании кириллицы.

3. Duplicati – программа резервного копирования данных. Является свободным ПО, присутствует кроссплатформенность. Главной особенностью является функция полноценного инкрементального бэкапа напрямую в облачное хранилище. Поддерживаются такие сервисы, как Google Drive, Skydrive, Amazon S3, Rackspace, Webdav, SFTP, FTP [3]. Присутствует шифрация данных при помощи библиотеки SharpAESCrypt или методами GnuPG. «Duplicati» так же имеет возможность быстрого восстановления отдельного файла из облака.

На рисунке 3 показан интерфейс программы «Duplicati».

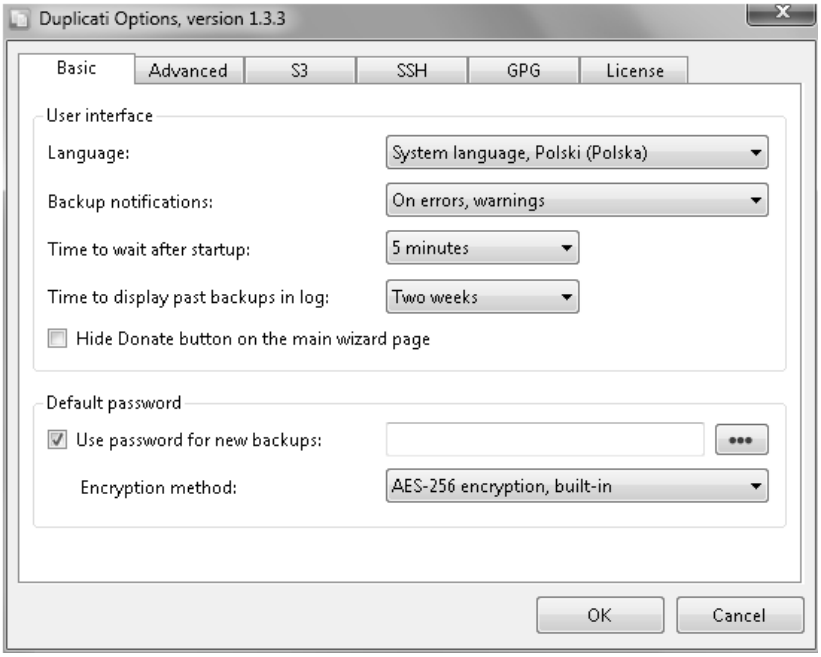

Рисунок 3 – Интерфейс программы «Duplicati»

Недостатками данной системы являются:

- специфический внешний вид графического интерфейса, требует привыкания;
- нет локализации для нашего рынка;
- не поддерживает отечественные облака;
- нет возможности обновить тот или иной файл на облаке. Приходится повторно проделывать все операции с файлами.

4. Порт encfs для Windows.

Помимо свободных исходников, главное отличие от остальных методов, что в encf4win используется ключ -reverse. Чтобы порт encfs4win [3] корректно работал, обязательно наличие библиотек Dokan (версии выше 0.6).

Рисунок 4 – Интерфейс программы «encfs»

Можно выделить следующие недостатки системы:

- нет графического интерфейса и тем более русификации;
- недоделанность возможностей;
- нет возможности корректно размонтировать том из консоли;
- само по себе самое слабое шифрование.

Таким образом, можно сделать вывод, что в «большинстве рассмотренных систем отсутствует локализация продукта для отечественного рынка. Также некоторые сервисы являются платными и не имеют кроссплатформенного автономного приложения с внятным графическим интерфейсом пользователя» [6].

Таблица 1 – Результаты сравнения вариантов шифрования данных в облаках для Windows [5]

Параметр	Проприетарные программы	Порт encfs для Windows — encfs4win	Duplicati	Webdav клиент CarotDav
Платность	Да	Нет	Да	Да
Кроссплатформенность	Нет	Нет	Нет	Да
Русская локализация	Нет	Нет	Нет	Нет
Поддержка мобильных приложений	Да	Нет	Да	Да
Шифрование имени файлов	Да	Да	Да	Да
Безопасное предоставление сторонним лицам доступа к своим зашифрованным файлам	Да	Нет	Нет	Да
Производительность (по десятибальной шкале)	5	4	10	7

Реализация программы. Проведя данный анализ систем шифрования и дешифрования, мы считаем, что необходимо устранить недостатки вышеизложенных систем и разработать приложение со следующими задачами и характеристиками:

- Улучшить техническую поддержку пользователей и поддержку мобильных приложений;
- Система должна повысить безопасность хранения данных в облачных хранилищах путем применения стеганографии;
- В системе должна быть реализована двухфакторная аутентификация входа для учетной записи;
- Система должна быть обеспечена постоянной поддержкой пользователей;
- В системе должен быть интуитивно понятный интерфейс [7];
- Система должна быть локализирована для отечественного рынка;
- Должна быть поддержка основных популярных в России облаков Google Drive, Mail.ru и Яндекс.Диск [3].

1. Гринюк О.Н., Алексашина О.В., Санаева Г.Н. Операции с большими числами и информационная безопасность облачных технологий // Журнал естественнонаучных исследований. – 2019. – № 1. – С. 21-24.

2. Вишняков А. С., Макаров А. Е., Уткин А. В., Зажогин С. Д., Бобров А. В. Обеспечение защиты данных, представленных в облачных сервисах // Вестник науки и образования. – 2019. – № 11-2(65). – С. 22-29.
3. Вишняков А.С., Макаров А.Е., Уткин А.В., Зажогин С.Д., Бобров А.В. Обеспечение защиты данных, представленных в облачных сервисах // Вестник науки и образования. – 2019. – № 11-12. – С. 22-29.
4. Мартышкин А.И., Плахина Л.Н., Лобов Р.А. Разработка системы скрытого хранения конфиденциальной информации в облачных хранилищах // European Journal of Natural History. – 2020. – № 2. – С. 80-84.
5. Обзор вариантов шифрования данных в облаках для Windows [Электронный ресурс] //Интернет-ресурс/ URL: https://habr.com/ru/post/207306 (дата обращения 07.04.2021).
6. Плахина Л.Н., Лобов Р.А. Создание прототипа системы скрытого хранения конфиденциальной информации в облачных хранилищах// Результаты современных научных исследований и разработок: сборник статей VII Международной научно-практической конференции: Часть 1. – Пенза: МЦНС «Наука и Просвещение». – 2019. – С.76-78.
7. Пащенко Т.Ю., Мартышкин А.И., Лобов Р.А. Вариант архитектуры облачной системы для пользовательских данных // XXI век: итоги прошлого и проблемы настоящего плюс. – 2020. – Т. 9. – № 4 (52). – С. 68-72.