УДК 004.223.2

ВОЗМОЖНЫЕ ВАРИАНТЫ ХРАНЕНИЯ ИНФОРМАЦИИ, АНАЛИЗ И ВЫБОР ОПТИМАЛЬНОГО ХРАНИЛИЩА ДЛЯ ДАЛЬНЕЙШЕЙ РЕАЛИЗАЦИИ

Е.С. ДЕНИСОВА
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

Рассматривается различные варианты хранения информации. В ходе анализа был выбран оптимальный вариант хранения информации. Проектирование системы для хранения и возможности передачи информации, также вопросы защиты этих данных. Проведены исследования по актуальности разработки данной системы.

В современном мире пользователи персонального компьютера, смартфона и другого устройства с доступом к Всемирной Сети имеют большое количество информации (фотографии, видеозаписи, музыка, различные документы и т.п.), которую необходимо где-то хранить. Для хранения информации существует большое количество различных ресурсов. Рассмотрим возможные варианты хранения информации:

1. Жесткие диски – на сегодняшний день используются в большинстве настольных ПК, а также нашли применение в качестве портативных хранилищ данных. Обычно, такой носитель исправно работает в течении 3-10 лет и срок его службы зависит от множества внешних факторов и самого качества изготовления;
2. Флешки и SSD накопители – такие устройства, в среднем, исправно работают около пяти лет. Многие флешки могут ломаться даже намного раньше, ведь они могут не перенести скачок напряжения или статический разряд, в момент подключения к ПК;
3. Оптические диски – это всем известные CD, DVD и Blu-Ray. Пожалуй, это одни, из самых долговременных способов сохранить информацию, в некоторых случаях такой диск будет надежно хранить все записанные данные более чем 100 лет, но оптические диски могут занимать большое количество физического пространства, что не очень удобно будет пользователю;
4. Облачные хранилища – это модель облачных вычислений, предусматривающая хранение данных в Интернете с помощью поставщика облачных вычислительных ресурсов, который предоставляет хранилище данных как сервис и обеспечивает управление им. Использование облачных носителей очень популярно в наше время. Очень удобный вариант предоставлять информацию любому человеку, будучи в любой точке планеты, имея при себе любое мультимедийное устройство и доступ к Интернету.

Исходя из вышеперечисленных вариантов можно сделать вывод, что в век современных технологий и доступности Интернета, пользователи все чаще «доверяют» свои данные облачным сервисам, что достаточно удобно, потому что сервис не занимает у пользователя никакого физического пространства в отличии от других возможных вариантов хранения информации.

Актуальность разработки своего облачного хранилища:

Основу разрабатываемой системы, составляет возможность хранить, накапливать и обрабатывать данные. Также возможность делиться файлами со сторонними людьми. При разработке собственного облачного хранилища у нас есть возможность сделать шифрование «под себя», то есть выбрать алгоритмы, которые нам нужны и при необходимости видоизменять их. На данном этапе реализована двухключевая математическая модель криптосистемы на основе двух типов шифрований (AES+RSA) таким образом, что в любой момент можно изменить/добавить алгоритм шифрования. Что делает нашу систему гибкой для разработки и более защищенной от умышленного хищения информации.

Принцип защиты информации.

Основываясь на том, что данная система предназначена для хранения конфиденциальных данных пользователей, необходимо разработать систему аутентификации, и криптографической защиты, данных.

Для защищённой передачи данных по сети интернет предназначены следующие виды технологии:

1. Протокол HTTPS - стандарт передачи данных между различными машинами, который определяет, что должно выступать в качестве сигнала начала передачи, как обозначаются данные и т. д. При этом данные шифруются по протоколу SSL, что делает проблематичным не только перехват, но и получение конфиденциальной информации [5].
2. Протокол SRTP – это профиль расширения RTP (Real-Time Transport Protocol, транспортный протокол в реальном времени), который добавляет дополнительные функции безопасности, такие как аутентификация сообщений, конфиденциальность и защита от прослушивания. Данный протокол будет использован при передаче видео сообщений [6].

3. Шифр AES - симметричный алгоритм блочного шифрования. Данный вид шифрования будет использовать один и тот же симметричный ключ. Для разрабатываемой системы, это является оптимальным вариантом, так как подобные системы также защищены юридическими соглашениями, о неразглашении третьим лицам. Используемый метод шифрования, будет использован для шифрации конфиденциальных данных, на уровне базы данных.

4. Шифр RSA – алгоритм шифрования с открытым ключом, базирующийся на факторизации простых чисел.

Заключение. В ходе данного исследования и анализа были сделаны выводы о выборе оптимального хранилища информации для пользователя и обоснование актуальности создания своего облачного хранилища.

ЛИТЕРАТУРА

1. WebRTC API [Электронный ресурс]. – Режим доступа: https://developer.mozilla.org/ru/docs/Web/API/WebRTC_API. – Дата доступа: 23.09.2018.
2. Протокол HTTPS - что такое? [Электронный ресурс]. – Режим доступа: http://fb.ru/article/221368/protokol-https---chto-takoe. – Дата доступа: 23.09.2018.
3. SRTP — что такое безопасный протокол передачи данных в реальном времени? [Электронный ресурс]. – Режим доступа: https://www.3cx.ru/webrtc/srtp/. – Дата доступа: 23.09.2018.