0.1. *Степанов А.В.* Описание концепции и разработка защищенного облачного хранилища данных

В современном мире угроза нарушения конфиденциальности, целостности и доступности хранимых данных является серьезной проблемой для людей и организаций. Деятельность организаций нередко тесно связана с использованием облачных технологий, в том числе облачных хранилищ данных. Согласно отчету «Cloud Security Report 2019» компании Synopsys основной проблемой безопасности в облачных технологиях является утечка и потеря данных пользователей [1]. Результаты исследования «Лаборатории Касперского» также подтверждают наличие угрозы безопасности хранимых в облаке данных [2].

С целью снизить риск нарушения конфиденциальности данных в облачном хранилище и сделать его удобным в использовании, было принято решение разработать свое защищенное облачное хранилище данных с применением симметричного и асимметричного шифрований и с элементами социальной сети, используя SaaS в качестве подхода по предоставлению услуг, так как, согласно отчету «2020 SaaS Trends Report» от Blissfully, такой формат предоставления услуг является наиболее удобным для пользователей [3]. Элементы социальной сети добавляют разработанному программному комплексу уникальности. В качестве алгоритмов шифрования файлов были выбраны отечественный алгоритм шифрования «Кузнечик» [4], описанный в ГОСТ Р 34.12–2015, а также AES-256 на выбор пользователя. В качестве асимметричного алгоритма шифрования для разделения доступа к зашифрованным файлам был выбран RSA. Загружаемые пользователем файлы шифруются на его стороне симметричным шифром, после чего он может разделить к ним доступ с другим пользователем из его списка друзей в данном облачном хранилище. Доступ разделяется путем шифрования симметричного ключа шифрования файла первого пользователя открытым ключом второго, после чего среди файлов второго пользователя появляется переданный ему таким образом файл, зашифрованный ключ которого расшифровывается на стороне второго пользователя с использованием его закрытого ключа. Помимо описанной возможности разделения доступа к файлу среди элементов социальной сети, в данном программном комплексе, разработанном на ReactJS и Node.js, также присутствует возможность поиска человека в сервисе для добавления в список друзей и в черный список, возможность текстового обмена сообщениями, а также возможность совершать аудио и видео звонки. Для удобства пользователя информация о предоставленном доступе к файлам представляет собой всплывающие окна с уведомлением.

Научный руководитель — к.ф.-м.н. Вайнштейн В. И.

Список литературы

[1] Cloud Security Report 2019. [Электронный ресурс]. URL: https://arato.inf.unideb.hu/huszti.andrea/ibiza/2019_Cloud_Security_Report.pdf (дата обращения 15.09.2023).

[2] «Лаборатория Касперского»: 9 из 10 утечек данных из облаков происходит из-за человеческого фактора. [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2019_laboratoriya-kasperskogo-9-iz-10-utechek-dannyh (дата обращения 15.09.2023).

[3] Cloud Security Report. [Электронный ресурс]. URL: https://cdn2.hubspot.net/hubfs/2093754/eBooks/2020%20SaaS%20Trends%20Report.pdf (дата обращения 15.09.2023).

[4] ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. Введён 2016-01-01 / М.: Стандарт информ, 2015. 20 с.