УДК 004.056.55

РАЗРАБОТКА АЛГОРИТМА ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ЧАСТИЧНО ГОМОМОРФНЫХ КРИПТОСИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ОБЛАЧНЫХ СЕРВИСАХ

Ахвердиева А.А. (Университет ИТМО)
Научный руководитель –к.т.н., Таранов С.В.
(Университет ИТМО)

Аннотация
Целью работы является увеличение уровня защищенности конфиденциальной информации в облачных сервисах при помощи частично гомоморфного шифрования. Исследование включает в себя анализ некоторых существующих алгоритмов шифрования. В результате работы смоделирован алгоритм шифрования и дешифрования данных в облачном сервисе.

Введение. Разработка и поддержание собственного хранилища требует больших временных, денежных расходов, что приводит к необходимости использования сторонних мест для хранения информации, в частности, облачных сервисов. Поэтому особенно актуальна защита информации в облачных сервисах.

Процессы обработки и, непосредственно, хранения информации происходят на серверах провайдера. Безусловно проблема конфиденциальности является одной из важных проблем информационной безопасности.

Основным и наиболее эффективным методом обеспечения конфиденциальности данных является шифрование данных. Шифрование данных позволит повысить безопасность передаваемых файлов, поскольку данные представляются уже в защищенном формате.

Объектом исследования являются облачные вычисления.

Предметом исследования является безопасность в облачных средствах.

В 2009 году Крейг Джентри представил рабочую схему полного гомоморфного шифрования в своей диссертационной работе. Однако недостаток данной схемы заключается в том, что выполнение вычислений приводит к накоплению ошибок, что делает невозможным расшифрование сообщения. Различные модификации также имеют существенные недостатки, например, превышение вычислительных возможностей процедуры генерации ключей.

В настоящее время не разработан такой алгоритм, который позволял бы проводить операции шифрования и дешифрования больших данных в облачных сервисах быстро, обеспечивая при этом надлежащий уровень защиты конфиденциальной информации.

Основная часть. В этой работе для реализации алгоритмов шифрования и дешифрования выбрана криптосистема Паскаля Пэйе. Для проведения операций без существенных затрат шифруется не вся информация, передаваемая в облачное хранилище, а лишь та часть, которая является критичной с точки зрения информационной безопасности. В свою очередь, стоит отметить, что такая информация будет передаваться в облако исключительно в зашифрованном виде.

Выводы. Результаты, полученные в ходе данного исследования, могут быть применены в дальнейших работах для достижения необходимого уровня защищенности информации в облачных сервисах, для программной реализации выбранной криптосистемы и дальнейшей оценки эффективности разработанного алгоритма**.**

Ахвердиева А.А. (автор)

Таранов С.В. (научный руководитель)