УДК 004.056

РАЗРАБОТКА СОВРЕМЕННЫХ СИСТЕМ ШИФРОВАНИЯ В ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ

Автор: Адигамов Д.Р., магистрант, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург

Научный руководитель: Коржук В.М., ассистент, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики г. Санкт-Петербург

Введение

В наше время цифровая безопасность и методы криптографического шифрования с каждым днем набирают все большую значимость. Любая организация все больше зависима от компьютеров, которые требуют защиты личных данных от злоумышленников. Существует множество способов обезопасить пользователей, используя различные системы шифрования. Каждый специалист в сфере компьютерной безопасности может предложить свой способ обезопасить пользователей, используя различное множество алгоритмов шифрования, в том числе и стандартные алгоритмы шифрования. Таким образом, встает задача исследования уровня защищенности таких систем и разработка современной системы шифрования.

Цель работы

Необходимо проанализировать существующие системы шифрования, обратить внимание на то, какие алгоритмы шифрования в них используются и на способы их реализации. Это необходимо для разработки современной системы шифрования учитывая недоставки существующих систем.

Базовые положения исследования

Исследование заключается в анализе общенаучных теоретических и эмпирических методов. Из теоретических методов применялся анализ известных данных о методах симметричного шифрования и метода двухключевой криптографии, а также синтез полученных данных для получения представлений об эффективности данных методов. Из эмпирических методов использовалось изучение симметричного шифрования и ассиметричного шифрования на примере методов двухключевой криптографии. На основе полученных данных разработка современной системы шифрования.

Промежуточный результат

Рассмотрены такие алгоритмы как ГОСТ 28147-89, AES, Twofish, Serpent, произведено сравнение по таким критериям, как криптостойкость, скорость шифрования и дешифрования, эффективность. Предложен современный способ системы шифрования на анализе рассмотренных.

Основной результат

Разработана современная система шифрования в деятельности государственных органов, а также оценена ее эффективность с учетом требований к современным криптографическим системам.

Автор _____ Адигамов Д.Р.

Научный руководитель _____ Коржук В.М.