ЗАКЛЮЧЕНИЕ

В результате была разработана база данных телеметрии СКА в формате CSV-файлов, создана структура телеметрических данных по бортовым системам, по временным интервалом, по работоспособности; разработан пользовательский интерфейс для анализа состояния систем СКА.

Литература

4. *Назаров А.В., Козырев Г.И* Современная телеметрия в теории и на практике. Учебный курс СПб.: Наука и Техника, 2007;
5. *Гольцман В*. MySQL 5.0. Библиотека программиста. Питер; Санкт-Петербург; 2010;

РАЗРАБОТКА АЛГОРИТМА ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКОЙ ДИНАМИКИ

Д. А. Жуковец

ВВЕДЕНИЕ

С развитием науки, техники и технологий стремительно возрастает информация в окружающей нас сфере. Поэтому информационная безопасность выступает как одна из важнейших характеристик информационной системы. Во многих системах, включая государственные и банковские, первостепенная роль отводится фактору безопасности информации. Большинство современных предприятий, занимающихся бизнесом, не могут вести нормальную деятельность без уверенности в обеспечении защиты своей информации. Нельзя забывать и про персональные компьютерные системы, связанные между собой сетью Интернет. Информация в современном обществе является ценностью, требующей защиты от несанкционированного доступа.

Целью работы является разработка алгоритма и программных средств для шифрования/расшифрования на основе динамического хаоса и проведение исследований алгоритма на его устойчивость к различным видам криптографических атак при использовании режима шифрования без сцепления блоков.

Решение поставленных задач проводилось в следующих направлениях:

- разработка алгоритма шифрования на основе динамического хаоса;
- разработка программных средств для шифрования и расшифрования на основе динамического хаоса;
- разработка компьютерных программ для оценки устойчивости к различным видам криптографических атак.

АЛГОРИТМ ШИФРОВАНИЯ

Криптографические методы защиты информации при ее передаче и хранении являются наиболее надежными и стойкими по отношению к различного рода атакам. Наряду с традиционными алгоритмами шифрования, которые постоянно разрабатываются и совершенствуются, все большую популярность в криптографическом сообществе приобретают алгоритмы шифрования на основе систем динамического хаоса.

На рисунке 1 приведена структурная схема шифрования на основе хаотических отображений. Используется 14 раундов для реализации схемы шифрования, в каждом раунде используется подключ, каждый из которых содержит четыре компоненты ($K_i(1)$, $K_i(2)$, $K_i(3)$, $K_i(4)$). Эти дополнительные ключи генерируются по определенному алгоритму. В то же время, в целях повышения безопасности этого алгоритма, F функция представляет собой сочетание двух хаотических отображений (см. рисунок 2). Определено отдельно место перестановочной функции для обработки 32 бит один раз в начале и в конце этого алгоритма.

В предлагаемом нами алгоритме шифрования используются два хаотических отображения: двумерное кубическое отображение (функция **f1**) и логистическое отображение (функция **f2**)

На рисунке 2 показана внутренняя структура F, где обозначены:

$\oplus$ операция XOR,

$\boxplus$ операция сложения по модулю 2^8,

f1 и **f2** хаотические отображения.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ И АНАЛИЗА ЕГО УСТОЙЧИВОСТИ

Аппаратно-программная база для осуществления программной реализации включает персональный компьютер с установленной операционной системой Microsoft Windows 7 и программным обеспечением среды разработки Microsoft Visual Studio 2010. В качестве языка программирования использовался C++.

В ходе работы было разработано программное обеспечение, для реализации алгоритма шифрования, интерфейс которой приведен на рисунке 3. Данная программа позволяет зашифровать изображение и соответственно расшифровать его. Предусмотрена возможность изменения использующихся отображений, а так же режимов шифрования и ключа

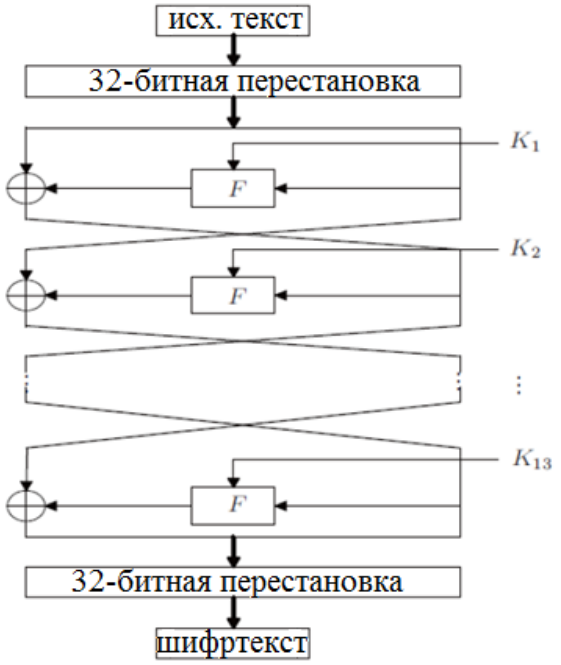

Рис. 1. Структурная схема шифрования

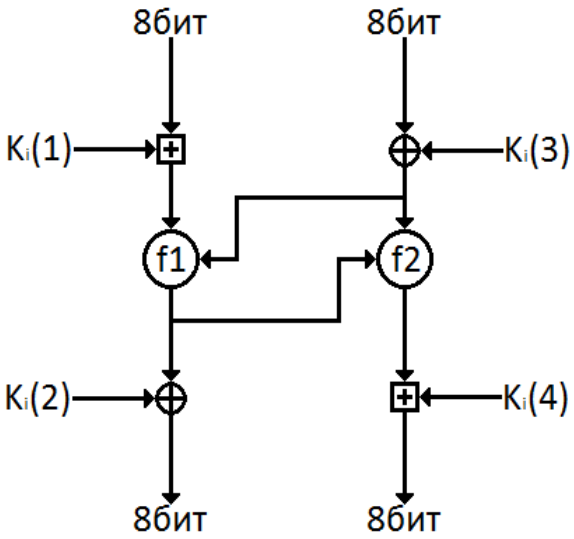

Рис. 2. Внутренняя структура раундовой функции F

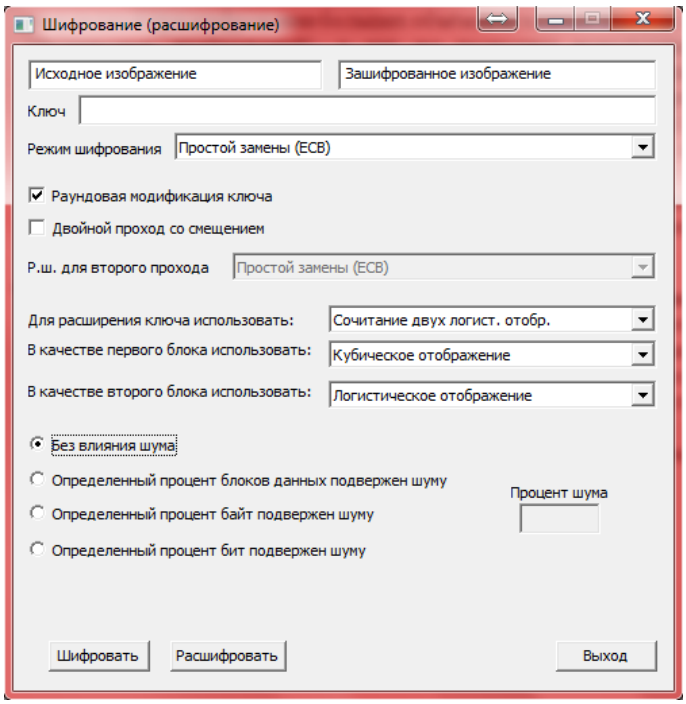

Рис. 3. Интерфейс программы шифрования

Для автоматизации оценки устойчивости алгоритма к различным криптографическим атакам было разработано программное обеспечение (ПО). Данное ПО позволяет рассчитать такие параметры, как: математическое ожидание и дисперсия байт изображения; информационную эн-

тропию; статистическую меру сложности; коэффициенты корреляции в горизонтальном, вертикальном и диагональном направлении.

С помощью данной программы, можно проанализировать в количественном отношении степень схожести двух зашифрованных изображений. Для данной оценки рассчитываются такие показатели, как: коэффициент взаимной корреляции; коэффициент устойчивости к линейным атакам; процент байт, изменивших значение (NPCR); среднее изменение интенсивности (UACI). Эти параметры выводятся в главном окне программы, интерфейс которой представлен на рисунке 4

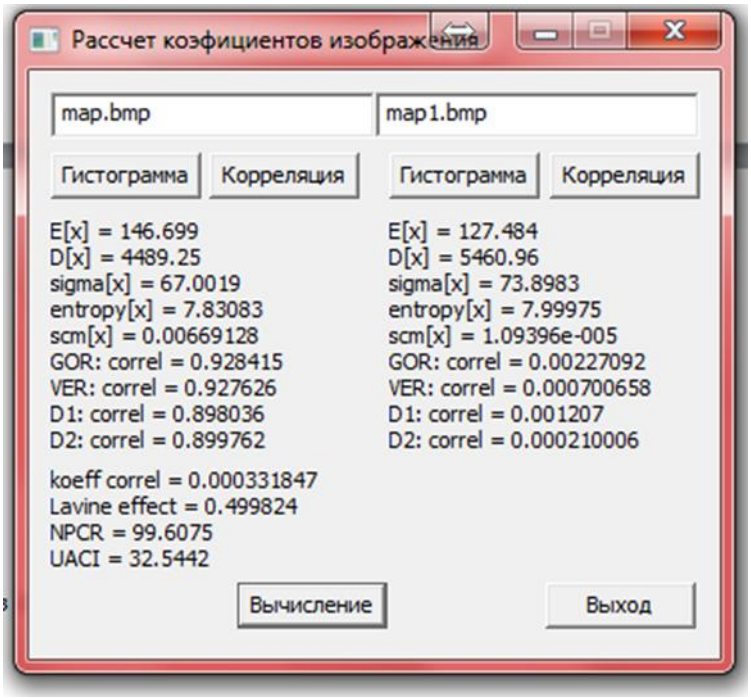

Рис. 4. Интерфейс программного обеспечения для оценки устойчивости алгоритма

ЗАКЛЮЧЕНИЕ

Таким образом, нами разработан алгоритм шифрования и программное обеспечение для его реализации. Создана программа оценки устойчивости алгоритма, из результатов которой можно сделать вывод о том, что предложенный алгоритм удовлетворяет количественным показателям при оценке его стойкости