ИНФОРМАЦИОННАЯ И ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ, ТЕЛЕМЕХАНИКИ И СВЯЗИ

УДК 681.322:621.391

ЗАЩИТА ДАННЫХ В ОПЕРАТИВНЫХ СИСТЕМАХ ПЕРЕДАЧИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

С. Н. БЕЛАН, Г. Д. КАЛЭНСКАЯ, В. Ф. ЛАКАТОШ
Государственный университет инфраструктуры и технологий, г. Киев, Украина

Информационная безопасность имеет большое значение для обеспечения жизненно важных интересов любого государства и транспортных систем. Создание развитой и защищенной среды является непременным условием развития общества и страны в целом, в основе которого должны быть новейшие автоматизированные технические средства. Важными стратегическими отраслями любого государства являются его транспортные инфраструктуры, объекты управления и учета. Для успешной и надежной организации работы таких подразделений необходима надежная защита данных, которые передаются. Особенно это касается оперативных данных. Объектом защиты в информационной системе является информация с ограниченным доступом, которая циркулирует и сохраняется в виде данных, команд, сообщений, имеющих определенную ограниченность и ценность как для ее владельца, так и для потенциального нарушителя технической защиты информации.

Информация, которая хранится на носителях может быть защищена как программными, так и аппаратными средствами, которые предотвращают доступ к средствам считывания с носителя. Существует также информация, которая передается по незащищенным каналам связи. В первую очередь это касается систем передачи данных массового пользования. В таких системах данные передаются по разным средам (электрический кабель, оптический кабель и радиоэфир). В такой ситуации информацию защищают двумя подходами: криптография и стеганография [1–3]. Первый метод характеризуется наличием сведений о зашифрованном сообщении, а второй метод характеризуется сокрытием самого факта наличия сообщения. Причем стеганография использует криптографию и скрывает заранее зашифрованное сообщение.

Существующие на данный момент стеганографические подходы используют контейнеры различной природы. Одним из таких контейнеров являются графические файлы, в байты которых записываются соответствующие биты цифрового сообщения. Причем накладываются требования относительно искажения исходного изображения. Для уменьшения видимых искажений биты цифрового сообщения записываются в младшие биты выбранных байтов файла изображения, что значительно уменьшает объем возможного сообщения и требует графических файлов большого объема. В случаях, когда используются графические контейнеры фиксированной длины необходимы разрабатывать методы увеличения объема внедряемого сообщения без видимых визуальных искажений изображений контейнеров.

Для увеличения объема внедряемого сообщения без изменений объема изображения ставится задача поиска таких зон изображения, значительные искажения которых не приводили бы к искажению общей зрительной картины. Также используется предварительное шифрование секретного сообщения, для чего используются генераторы псевдослучайных чисел (ГПСЧ), которые могут быть реализованы различными методами и средствами [4].

Генераторы псевдослучайных последовательностей являются неотъемлемыми элементами большинства систем защиты. Сфера их применения очень широка. Среди них: космическая связь; транспорт; коды, обнаруживающие и исправляющие ошибки; встроенное самотестирование ПЛИС; защита информации и др.

Качественные псевдослучайные последовательности, которые по своей сути являются детерминированными, тем не менее обладают практически всеми свойствами реализации истинно случайных процессов и успешно их заменяют. Наиболее распространены ГПСЧ, реализуемые математически и аппаратно.

В исследованиях рассматриваются методы стеганографического скрытия информации в контейнеры, представленные графическими файлами (изображениями). В изображениях контейнеров осуществляется поиск пикселей, искажение цвета которых не приводит к существенным изменени-

ям визуальной картины изображения. В коды таких пикселей можно внедрить большое количество битов секретного сообщения. Были использованы исследования, которые описаны в работах [5–7]. В этих работах на основе конструирующей стеганографии биты секретного сообщения внедряются в младшие разряды кодов специально выделенных пикселей (шумовые пиксели, краевые пиксели, пиксели, определенные с помощью пороговой обработки).

В данной работе используется оператор Собеля для выделения краевых пикселей, в двоичные коды которых внедряются биты секретного сообщения [8]. Оператор Собеля использует фрагмент изображения в виде матрицы 3×3 и организует свертку по формулам:

$$G_x = (z_7 + 2z_8 + z_9) - (z_1 + 2z_2 + z_3),$$
$$G_y = (z_3 + 2z_6 + z_9) - (z_1 + 2z_4 + z_6).$$

Формулы описаны согласно кодировки, представленной на рисунке 1.

В коды выделенных пикселей внедряются биты зашифрованного изображения с помощью ГПСЧ. Используется ГПСЧ, построенный на клеточных автоматах с активными и неоднородными клетками [4]. Эти ГПСЧ показали высокое качество сформированных псевдослучайных битовых последовательностей. Также были исследованы различные типы окрестностей, которые были реализованы в клеточных автоматах. Анализировались локальные функции переходов и влияние дополнительных бит.

z_1	z_2	z_3
z_4	z_5	z_6
z_7	z_8	z_9

Рисунок 1 – Область матрицы изображения для реализации оператора Собеля

Заключение. В данной работе проведены исследования современных методов и средств стеганографического сокрытия информации. Разработана система стеганографической защиты информации с применением контейнеров, представленные файлами графического формата. Увеличен объем внедряемой информации за счет использования пикселей, выделенных как краевые пиксели с помощью оператора Собеля. Внедрены дополнительные меры защиты внедряемого сообщения за счет шифрования секретного сообщения с помощью ГПСЧ, реализованных на клеточных автоматах. Показано, что использование дополнительного бита, формирующего самим клеточным автоматом, дает возможность получить битовые последовательности большой длины.

Список литературы

1 **Грибунин, В. Г.** Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.

2 **Рябко, Б. Я.** Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов. – 2-е изд. – М. : Горячая линия – Телеком, 2013. – 232 с.

3 **Конахович, Г. Ф.** Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

4 **Bilan, S.** Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities / S. Bilan // IGI Global. – USA. – 2017. — P. 301.

5 **Albdour, N.** Selection Image Points Method for Steganography Protection of Information / N. Albdour // WSEAS transactions on signal processing. – 2008. – Vol. 14. – P. 151–159.

6 **Bilan, M.** Research of Methods of Steganographic Protection of Audio Information Based on Video Containers. Handbook of Research on Intelligent Data Processing and Information Security Systems / M. Bilan, A. Bilan ; ed. by S. M. Bilan & Al-Zoubi, S. I. Hershey. – USA : IGI Global. – 2019. – P. 79–94.

7 **Albdour, N.** A Novel Methods for Image Steganography by Effective Image Points Selection / N. Albdour // Journal of Electrical and Electronics Engineering. – 2019. – Vol. 14, is. 5. Ser. II. – P. 06–11.

8 Real-time volume graphics / K. Engel [et al]. – Wellesley. Massachusetts: A K Peters, Ltd., 2006. – P. 112–114.

УДК 656.2.08

КИБЕРБЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ОТВЕТСТВЕННЫМИ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

К. А. БОЧКОВ, П. М. БУЙ

Белорусский государственный университет транспорта, г. Гомель

В соответствии с Концепцией информационной безопасности Республики Беларусь, которая была утверждена Президентом Республики Беларусь 18 марта 2019 года, кибербезопасность – это