

функций. В зависимости от выбранного алгоритма шифрования можно оценивать стойкость стеганографических систем. Теоретические подходы в целом можно использовать для оценки стойкости многоключевой стеганографической системы, однако имеются существенные недостатки использования данных подходов.

Очевидно, что использование идеальной модели криптосистемы Керкгоффса не вполне адекватно реалиям информационно скрывающих систем. Если передаваемые избыточные сообщения сжимаются с частичной потерей данных, или канал связи может вносить помехи в передаваемые информационные потоки, то данные подходы не будут иметь смысла, так как будет иметь место отклонение статистики наблюдаемого нарушителем в канале связи сообщения от среднестатистических характеристик пустых контейнеров и будет выявлен факт наличия стеганоканала.

## ЛИТЕРАТУРА

1 Урбанович, П. П. Защита информации методами криптографии, стеганографии и обfuscации: учеб.-метод. пособие для студ./ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2 Urbanovich, P. Theoretical Model of a Multi-Key Steganography System / P. Urbanovich, N. Shutko // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Vol. 2, Chapter 11. – Lublin : KUL, 2016. – P. 181-202.

3 Urbanovich, P. A formal description of a multi-key steganographic systems / P. Urbanovich, N. Shutko, A. Zapala// 10th Intern. Conf. NEET'2017, Zakopane, Poland, June 27 – 30, 2017. – P. 47.

4 Берников, В.О. Анализ стеганографической стойкости текстового документа-контейнера в многоключевой стеганосистеме// 69-я НТК студентов и магистрантов: сб. науч. работ: в 4-х ч., 17-22 апреля 2018 г. – Минск: БГТУ, 2018. – Ч. 4. – С.14-17.

УДК 003.26

Е. А. Блинова, ст. преп. (БГТУ, г. Минск)

## АЛГОРИТМИЧЕСКИЕ ОСОБЕННОСТИ И ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ В ЭЛЕКТРОННЫХ КАРТАХ

Электронные карты – это набор компьютерных файлов, содержащих пространственные данные в векторном формате. Электронные

карты широко используются в приложениях для управления инфраструктурой населенных пунктов, навигации и чрезвычайных ситуаций. Изготовление электронных карт требует значительных затрат, и картографическая информация должна быть предоставлена конечному пользователю с учетом защиты как от неправомерного использования, так и от умышленного искажения данных. Поскольку электронные карты могут только ограниченно использовать криптографические методы защиты на уровне файла или GIS-системы, наиболее оптимальным представляется использование стеганографических методов.

В литературе широко освещается возможность осаждения скрытой информации в файлы электронных карт. В период с 2000 по 2018 годы выросло число публикаций, посвященных проблеме осаждения скрытых данных в файлы электронных карт, в то время как ранее основной интерес сосредотачивался на растровых картах, которые представляют собой изображение. Основные подходы к осаждению скрытых меток в электронные карты приведены в таблице 1.

**Таблица 1 – Основные подходы к осаждению скрытых меток в электронных картах**

Наименование	Описание
Нулевые водяные знаки	Использование ключевых характеристик контейнера при генерации водяного знака
Адаптивные водяные знаки	Размещение водяного знака в определенной области в зависимости от характеристик контейнера
Множественные водяные знаки	Наличие нескольких разноплановых водяных знаков
Обратимые водяные знаки	Возможность получить оригинал контейнер после извлечения водяного знака
Аддитивные водяные знаки	Добавление водяного знака в координаты вершин полиномов пространственных объектов

При осаждении скрытых меток (водяного знака) все стеганографические методы могут быть разделены на две основные группы: изменение характеристик отдельных вершин пространственных объектов и трансформация пространственного объекта в целом. При изменении характеристик отдельных вершин пространственных объектов встраивание может производиться путем изменения младших цифр координат вершин пространственных объектов, изменением топологии, т.е. объединением или разделением пространственных объектов, а также делением электронной карты на взаимосвязанные части. Достоинствами таких методов являются простая программная реализация и объем размещаемого водяного знака, а основным недостатком — низкая стойкость к атаке на конкретный метод. К методам трансформации про-

пространственного объекта в целом относятся методы, использующие вейвлет-преобразование, дискретное преобразование Фурье и дискретное косинусное преобразование. Такие методы обеспечивают высокую стойкость к атакам, основанным на пространственных преобразованиях, таких как поворот или масштабирование, однако они подходят не для всех типов электронных карт и сложно реализуются.

## ЛИТЕРАТУРА

1 Блинова Е.А., Смелов В.В. Применение стеганографических методов при хранении картографической информации в экспертной системе прогнозирования последствий пролива нефтепродуктов// Сахаровские чтения 2017 года: Экологические проблемы XXI века, материалы 17-й МНК, 18-19 мая 2017. Международный государственный экологический институт им. Д. А. Сахарова Белорусского государственного университета. Минск. 2017. С. 223–224.

2 Блинова Е.А., Урбанович П.П. Защита целостности данных электронных карт стеганографическим методом// Тезисы 4-ой Международной научно-практической конференции «Веб-программирование и интернет-технологии WebConf2018», 14-18 мая 2018. БГУ. Минск. 2018. С. 147.

3 Блинова Е.А., Урбанович П.П. Стеганографический метод на основе встраивания дополнительных значений координат в изображения формата SVG // Труды БГТУ. Сер.3, Физ.-мат. Науки и информатика, № 1(206). Минск, БГТУ. 2018. С. 104-109.

4 Блинова Е.А., Голик А.А. Модификация стеганографического метода на основе встраивания дополнительных значений координат в изображения формата SVG // Развитие информатизации и государственной системы научно-технической информации (РИНТИ-2018): доклады XVII Международной конференции, Минск, 20 сентября 2018 г. Минск: ОИПИ НАН Беларуси, 2018. С. 130-133.

5 Blinova E., Shutko N. The use of steganographic methods in SVG format graphic files // New Electrical and Electronic Technologies and their Industrial Implementation; proc. of the 10-th Intern. Conf., Zakopane, Poland, 23–26.06.2017. / Lublin University of Technology; Media Patronage “Przeglad Elektrotechniczny”. Lublin. 2017. P .45.