СОКРЫТИЕ ИНФОРМАЦИИ В ФАЙЛАХ ФОРМАТА SVG

А.Н. Николайчук

Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Информация, передаваемая по открытым каналам связи, подвергается угрозам раскрытия, изменения и уничтожения. Одним из возможных решений проблемы угрозы раскрытия является использование стеганографических методов. Существующие стеганографические алгоритмы лишь частично удовлетворяют требованиям, которые предъявляются к системам скрытой передачи данных. Актуальной является задача поиска новых алгоритмов и каналов стеганографического встраивания информации. В процессе изучения данной проблемы была выявлена резко возросшая популярность векторных форматов изображений, которые сейчас активно внедряются на web-ресурсах и могут представлять собой достаточно эффективный стеганографический канал [1].

Файл SVG формата представляет собой XML-документ, который может содержать информацию разных видов: текст, растровые изображения, векторные объекты. Такое разнообразие типов данных, которыми оперирует данный формат, позволяет применять стеганографические методы, используя в качестве контейнера любой из типов элементов, перечисленных выше [2].

Стеганография векторных изображений обычно использует внедрение сообщения непосредственно в сами фигуры. Отображаются фигуры в SVG с помощью координат, по которым они описываются, в соответствии с рабочей областью, которая ограничивается с помощью значений атрибутов *width* и *height* тега <*path*>. Уникальность описания фигур в векторных изображениях позволяет формировать объекты вне рабочей области, и использовать данное свойство для внедрения скрытых данных. Такой способ стеганографического осаждения информации в контейнер позволяет размеру сообщения быть независимым от размера самого контейнера или его содержимого, а также предотвратить модификацию внедренной информации при использовании операции сдвига, которая может рассматриваться как тип несанкционированной модификации стеганоконтейнера [3].

Список литературы

1. Николайчук А.Н., Урбанович П.П. Анализ стеганографических методов на основе контейнеров SVG-формата // Информационные технологии: матер. 86-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 31 января – 12 февраля 2022 г. С. 49–51.

2. Николайчук А.Н., Урбанович П.П. Стеганография в векторных изображениях // 73-я науч.-техн. конф. учащихся, студентов и магистрантов: сборник научных работ, Минск, 18–23 апреля 2022 г. С. 947–949.

2. Николайчук А.Н., Урбанович П.П. Стеганографический метод на основе использования особенностей отображения элементов в формате SVG // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2023. № 1 (266). С. 64–70.