окружающей среды, планировке территорий, образовательных, разведывательных и военных целях. На спутниковых снимках отсутствуют знаки и обозначения объектов, поэтому есть необходимость в размещении на них служебной информации.

Использование стеганографических возможностей встраивания информации в картографические изображения позволит упростить работу с данными об определенном объекте исследования. Данные об объекте можно хранить непосредственно в самом изображении. При встраивании, исходное изображение можно разделить на слои и в каждый слой встроить определенную информацию. В этом случае, при извлечении некоторой информации, необходимости извлекать все, не будет.

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. М.: СОЛОН-Пресс, 2002.

2. Как карты передают географическую информацию [Электронный ресурс]/ArcGIS Recourses – 2010. – Режим доступа: http://resources.arcgis.com/ru/help/getting-started/articles/026n0000000q000000.htm.

УГРОЗЫ ТЕХНОЛОГИЙ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

С.Ю. Вашкевич, А.Е. Мишустина, Е.Е. Гачко, Т.С. Аубакирова

Особенностью развития современной сферы разработки мобильных и встроенных приложений становится использование наиболее перспективных технологий, из которых особо можно выделить технологию дополненной реальности (AR, augmented reality). Анализ рынка показал, что приложения, использующие AR-технологии, становятся популярны не только в сфере развлечений, но и получают множество вариантов практического применения.

При оценке рисков дополненной реальности в первую очередь обращают внимание на отвлекающие факторы. К примеру, слишком большое количество информации, находящейся в поле зрения водителя, может привести к фатальным последствиям. Менее вероятна угроза проникновения в системы дополненной реальности хакеров с последующим вторжением в частную жизнь, похищением цифровых данных и рисками физической безопасности. Можно подменить выходную информацию AR-систем, заставляя пользователя поверить, что сгенерированные компьютером объекты (например, поддельные дорожные знаки) реальны. Противоположный сценарий: так как приложениям дополненной реальности нужен доступ к реальным данным, собранным при помощи различных датчиков, вредоносные приложения могут похищать информацию о наблюдаемых объектах и местоположении пользователя.

В отчете 2016 Emerging Technology Domains Risk Survey [1] дополненная реальность названа одной из десяти технологических областей, которые в случае взлома могут привести к серьезным сбоям (в сфере безопасности, конфиденциальности, финансовой или операционной). Классические методы и средства повышения безопасности (например, шифрование данных, передаваемых по беспроводным каналам) позволяют защитить входные и выходные данные приложений. Но для этого необходимо иметь четкое представление об интеграции средств безопасности в сферу дополненной реальности.

Литература

1. 2016 Emerging Technology Domains Risk Survey [Электронный ресурс] / Software Engineering Institute. Carnegie Mellon Institute. – Режим доступа: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_453825.pdf. – Дата доступа: 18.05.2017.

ИСПОЛЬЗОВАНИЕ ВЕКТОРНОЙ ГРАФИКИ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ WEB-СИСТЕМ

О.Н. Виничук

Цифровое изображение – графическая форма представления данных, предназначенная для зрительного восприятия. Будучи закодированным с помощью особого алгоритма и записанным на носитель, этот массив данных становится файлом, который зачастую имеет достаточно большой размер. В современном процессе полиграфического производства все

Библиотека БГУИР