

Рисунок 4 – Зависимость времени компрессии изображения от размера рангового блока и типа изображения

### Литература

1. Кудрина М.А., Климентьев К.Е. Компьютерная графика. – Издательство СГАУ, 2013. – 140 с.
2. Ансон Л., Барнсли М. Фрактальное сжатие изображения //Мир ПК, 1992, № 4, с. 52 – 58.

А.Д. Скоков

## ПОСТРОЕНИЕ ГРАФОВЫХ МОДЕЛЕЙ ПОПУЛЯЦИЙ С ПРИМЕНЕНИЕМ ГИС-МЕТОДОВ

(Самарский университет)

Вопрос о распространении и взаимодействии саморазмножающихся объектов в настоящее время невозможно обойти стороной. Под саморазмножающимися объектами понимаются объекты реального мира, обладающие свойством саморепликации, которое передается от объекта к объекту при взаимодействии. Различные вирусы (компьютерные, мобильные, инфекционные и другие) как раз являются примерами таких объектов. Для описания распространения и взаимодействия подобного рода объектов как нельзя лучше подходят графы различного вида. Вирусы окружают человека повсюду, и изучение их распространения является очень важной задачей.

Чаще всего работы, посвященные изучению данной проблемы, решают такие задачи, как исследование поведения вредоносной программы, инфекционного вируса при некоторых заданных условиях. При этом объектом рассмотрения является асимптотическое поведение саморазмножающихся единиц. А это означает, что игнорируются важные факторы: неоднородность



среды распространения, непостоянство условий распространения во времени. Эти факторы могут быть учтены введением в модели распространения саморазмножающихся объектов «геометрических» и «географических» аспектов.

Целью работы является построение графовых моделей популяций, которые позволяют моделировать распространение эпидемий «мобильных червей», инфекций, передающихся между живыми организмами, с применением методов, используемых в геоинформационных системах (ГИС). Особенностью эпидемий подобного рода в первую очередь является возможность передачи свойства саморепликации лишь на ограниченное расстояние. Использование методов, применяемых в ГИС, позволит учитывать географические особенности территории распространения.

ГИС – это автоматизированная интегрированная информационная система, предназначенная для обработки пространственно-временных данных, основой интеграции которых служит географическая информация. Одним из основных принципов организации пространственной информации в ГИС является послойный принцип [1]. Технологически организация слоев основана на типизации данных (рисунок 1).

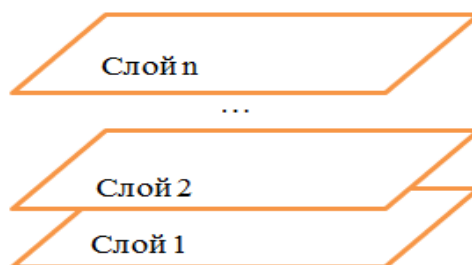


Рисунок 1 – Послойный принцип организации информации

В системе используется двухслойная структура организации пространственной информации: первый слой представляет собой карту местности, а второй – объекты, взаимодействие между которыми рассматривается в процессе моделирования.

В работе используется случайный «геометрический» граф (RGG) как наиболее близкая абстракция для сетей, моделирующих среду обитания подобных вирусов (рисунок 2).

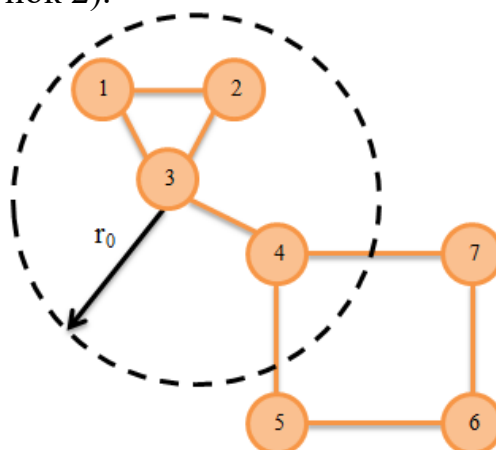


Рисунок 2 – Случайный «геометрический» граф



В построении графа со случайной геометрией участвуют «координаты» узлов. Например, если считать, что граф размещен в единичном квадрате, тогда каждому узлу приписываются координаты, представляющие собой равномерно распределенные на интервале  $[0...1]$  случайные величины. Затем для каждой пары узлов с индексами  $i$  и  $j$  рассчитывается «расстояние»  $r$ , и ребро между узлами проводится в том случае, если расстояние между ними не превышает заранее назначенного «радиуса»  $r_0$  [2].

Расстояние  $r$  при этом рассчитывается по формуле:

$$r = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2},$$

где  $x_1, x_2$  – координаты по оси абсцисс,  $y_1, y_2$  – координаты по оси ординат.

Граф в системе строится на основе «полуавтоматической» раскраски, принцип которой заключается в следующем:

9. клетка, в которой произведен клик мышью, помечается выбранной из «палитры» плотностью (например, максимальной);
10. ближайшие соседи помечаются уменьшенной на 1 градацию (например, средней) плотностью;
11. соседи соседей помечаются уменьшенной на 2 градации (например, малой) плотностью;
12. при этом действует принцип сложения плотностей.

Объекты в системе могут находиться в одном из двух состояний:

1. S (Susceptible) – здоровый и восприимчивый к заражению;
2. I (Infected) – зараженный.

Смена состояний возможна лишь в одном направлении (рисунок 3).



Рисунок 3 – SI-модель эпидемии

На рисунке 4 представлены результаты работы системы по моделированию начального распространения экземпляров вирусов, соответствующего какой-либо местности. При этом в качестве «шаблона» для заполнения используются изображения карт и схем, которые могут быть составлены самостоятельно или зашружены из Интернета.

При этом матрица смежности полученного графа может быть сохранена в файл и использоваться для моделирования распространения инфекций в динамике.

В будущем планируется добавить в систему больше различных состояний объектов, топологий графов. Также будут изучены однофакторные и двухфакторные модели скорости распространения вирусов. Все это позволит моделировать разнообразные по своим характеристикам эпидемии.



Рисунок 4 – Построение графовой модели на примере карты кампуса Самарского университета

### Литература

1. Бугаевский, Л.М., Цветков, В.Я. Геоинформационные системы [Текст]: учебное пособие для вузов/Л.М. Бугаевский, В.Я. Цветков. – М.: Златоуст, 2000. -222 с., ил.
2. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста [Текст]. – М.: ДМК-Пресс, 2013. -656 с.

С.Ю. Самароков

## ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА ДАННЫХ НА МОБИЛЬНЫХ УСТРОЙСТВАХ ОС ANDROID

(Самарский университет)

Мобильные устройства являются неотъемлемой частью современного мира. В настоящее время сложно представить современного человека, который бы существовал без портативного устройства – телефона, смартфона, планшета, умных часов – подключенного к сети Интернет. На сегодняшний день мобильные устройства предназначены не только для ведения телефонных переговоров и отправки сообщений, они способны создавать, обрабатывать, хранить и передавать огромное количество информации.

Как и любая информационная система, мобильные системы связи подвержены атакам нарушителей информационной безопасности, реализующим угрозы и уязвимости [3]:

- кража или потеря мобильного устройства;
- несанкционированный доступ;
- целенаправленная кража мобильного устройства с целью получения доступа к данным;
- атака вредоносного ПО;