

[1] являются длина формируемой ключевой последовательности (длина ее периода) и ее «непредсказуемость» [1]: знание знаков  $k_1, k_2, \dots, k_t$  последовательности не увеличивает вероятности угадать знак  $k_{t+1}$  для криптоаналитика с ограниченными возможностями. Известны также и широко используются ортогональные матрицы (orthogonal arrays – OA) [2]. Под OA с параметрами  $L, f, t$  понимается прямоугольная таблица с  $L^t$  строками,  $f$  столбцами, элементы которой принадлежат множеству целых чисел  $0, \dots, L-1$ , такая, что любая комбинация  $t$  столбцов содержит бесповторно все  $L^t$  возможных комбинаций значений чисел от 0 до  $L-1$ , при этом различные комбинации  $t$  столбцов различны, т.е. не совпадают как векторы. В [3] приведен алгоритм генерации ортогональных матриц произвольной силы. В настоящем докладе рассматриваются различные способы формирования псевдослучайных последовательностей на основе ортогональных матриц произвольной силы: с использованием размещений, сочетаний, многоуровневого управления формированием выходной последовательности. Производятся предварительные сравнительные оценки их качества.

**Выводы:** первый способ позволяет формировать последовательности большей длины, чем во 2-м и 3-м случаях, однако непредсказуемость выше у 3-го способа.

#### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. Учебное пособие. М.: ПАИМС, 2000.
2. A.S. Hedayat, N.J.A. Sloane, J. Stufken. Orthogonal arrays: theory and applications. - N.Y.: Springer-Verlag New York, 1999.
3. Мазурова Т.А., Чефранов А.Г. О генерации ортогональных матриц произвольной силы. // Известия ТРТУ. Спец. вып. Материалы XLVII НТК. Таганрог, 2002. №1. С.81–82.

УДК 681.3.06

А.А. Палазиев

#### ОТКРЫТАЯ ИНФОРМАЦИОННАЯ СТРУКТУРА ГИС

Упрощенную структуру типичной географической информационной системы (ГИС) можно представить из трех составных частей. Это – графическая и семантическая базы данных, программная среда и, наконец, модуль взаимодействия программной среды с базами данных, в котором реализуются правила хранения данных и взаимодействия информационных потоков.

В настоящее время широкое распространение получают прикладные ГИС, ориентированные на локальных пользователей (в рамках предприятия, учреждения и т.д.). Такие системы имеют ряд отличительных особенностей:

- ◆ сравнительно малый информационный объем и бюджет финансирования;
- ◆ высокая степень индивидуализации решаемых задач;
- ◆ стремительная динамика развития после внедрения.

Эти особенности требуют вмешательства разработчика, причем на низком программном уровне, что не всегда удобно и возможно. Кроме этого, любое вмешательство в отлаженный, относительно сложный механизм чревато скрытыми ошибками и большими затратами на тестирование и отладку.

В докладе рассматриваются основные положения создания «открытой» информационной структуры, которая позволяла бы производить перестройку системы без низкоуровневого вмешательства в программную оболочку ГИС:

- ◆ Использование методологии объектно-ориентированного подхода;
- ◆ Разделение графической и семантической баз данных;
- ◆ Внедрение специфического языка описания структуры семантической информации и отказ от стандартных средств работы с базой данных;
- ◆ Использование древовидной структуры классов объектов и графических баз;
- ◆ Наличие наращиваемого шаблона информационной структуры, который используется всеми процедурами системы;
- ◆ Отказ от «жестких» диалоговых процедур при организации пользовательского интерфейса.

УДК 681.3.06

**М.П. Сидоренко**

### **ТРЕХМЕРНОЕ МОДЕЛИРОВАНИЕ В ГИС**

Большинство из существующих ГИС могут содержать в основном только точечные (дискретные) высотные характеристики искусственных сооружений и элементов рельефа в виде их численных значений. Для искусственных сооружений обычно это этажность, для выдающихся сооружений (трубы, башни и т.д.) и рельефа – высота в метрах или иных единицах. При наличии таких данных уже возможно построение цифровой модели местности (рельефа) или застроенных территорий. В докладе производится анализ существующих программных средств и методов трехмерного моделирования в ГИС.

Среди существующих ГИС, активно использующих трехмерное моделирование, можно выделить AutoCAD MAP, Autodesk Land Desktop, Vertical Mapper (модуль MapInfo), TerraModeler (модуль MicroStation), Geostatistical Software Tool (локальное расширение ГИС ИНТЕГРО), ArcGIS Geostatistical Analyst. Данным продуктам характерна функциональная направленность на решение определенных задач: создание виртуальных макетов местности для задач обучения (тренажеров) и поддержки принятия решений; ландшафтное моделирование и проектирование.

Для цифрового моделирования чаще всего используют триангуляцию Делоне и кригинг. Триангуляция – есть разбиение поверхности на треугольники с вершинами в опорных точках, а кригинг – геостатистический метод интерполяции, использующий статистические параметры распределения опорных точек для более точного построения поверхностей. Преимуществом триангуляционной модели является то, что в ней нет никаких преобразований исходных данных. Кригинг же позволяет исследовать пространственные автокорреляции между данными. Кригинг выполняет две группы задач: количественное определение пространственной структуры данных и создание прогноза.

В дополнение к методам, широко применяемым в области трёхмерного моделирования, в докладе представлена технология восстановления объёмных моделей ландшафта и отдельных зданий по данным электронных карт.