

# ДИНАМИКА КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ И РАСШИРЕНИЕ КЛАССА ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ ОБУЧЕНИЯ

Рыков В.Т., Шевченко С.В.

*Кубанский государственный университет*

*Краснодар, Россия*

*rykovw@rambler.ru*

Динамические функциональные элементы обучения [1] получили большое распространение в коммерческих обучающих программах, иллюстрируя, прежде всего, динамику физических процессов в виде графиков соответствующих величин. Построение графика под наблюдением, а иногда и управлением учащегося одновременно с имитацией реального физического процесса развивает воображение и позволяет «прочувствовать» процесс. Эта динамика очевидная, так сказать, «открытая». Однако часто динамического представления требуют и внешне статичные объекты, отражающие внутреннюю динамику математических преобразований.

К таким объектам относятся алгоритмы различных криптографических преобразований. Будучи представлены статическими изображениями последовательности действий над числами, они значительным числом студентов (превышающим, как правило, 50 %) и воспринимаются как не изменяющиеся формы. Знакомые очертания самих форм создают ощущение сиюминутного понимания, скрывая от самих студентов и преподавателя реальное непонимание сущности алгоритма. Это непонимание открывается преподавателю, как правило, только на этапе проверки умения применить полученные знания на практике. Между тем большинство нетривиальных криптоалгоритмов осуществляют постоянное движение чисел по непрерывно изменяющимся траекториям.

В том случае, если траектории движения чисел не изменяются, имеет смысл использовать стационарные функциональные элементы обучения, отображающие постоянные траектории, содержание элементов которых начинает изменяться в соответствии с заданным алгоритмом (например, скремблер) по команде учащегося, реализация которой заложена в кнопках «старт» и «стоп». С помощью аниматора Flash MX 7.0 алгоритм движения чисел реализуется в виде последовательных перемещений и превращений чисел в соответствии с исходным текстовым файлом.

Более сложная динамика алгоритма Хаффмана, реализуемая в виде дерева с изменяющимся строением ветвей, оказывается трудной для восприятия без соответствующих пояснений и многократных повторений. Это заставляет расширить число базовых атрибутов функционального элемента обучения, путем введения стереотипов Sound broadcasting – звуковое сопровождение и speaker – диктор, уточняющий, что звуковое сопровождение должно носить характер дикторских пояснений.

Усложняется и режиссура данного функционального элемента. На наш взгляд имеет смысл разъясняемые диктором действия демонстрировать дважды: до дикторского текста и сразу после него. В спецификации соответствующих элементов можно добавить стереотип Cycle – цикл, указывающий на наличие определенного количества циклических повторений в обучающем элементе.

Рассмотренные атрибуты имеет смысл включать во все функциональные элементы обучения, иллюстрирующие непрерывно изменяющиеся процессы, так как сама непрерывность процесса мешает четкому осознанию этой непрерывности в случае отсутствия альтернативного (прерывного) движения.

## Литература

1. Рыкова Е.В., Рыков В.Т. Функциональный элемент обучения как дидактическая единица ИОС. – Успехи современного естествознания, №. 3, 2005. – с. 96-99