2) обучение конструкциям алгоритмических языков программирования высокого уровня и их использованию для кодирования разработанных алгоритмов.

Соответственно программное обеспечение АСО строится как совокупность трех подсистем, общей чертой которых является: а) поддержка банка аттестованных и классифицированных по сложности и тематике задач с набором тестовых входных и выходных значений;

б) наличие турбо-среды, со средствами графического редактирования алгоритмов в терминах граф-схем и псевдокода, отладчиком с пошаговым трассированием алгоритма, средствами управления файловой системой и т.д.;

в) синтаксический, семантический анализаторы для контроля правильности написания алгоритма и создания его внутреннего представления;

г) процедура автоматической генерации исходного и загрузочного кода по внутреннему представлению алгоритма;

д) процедура тестирования алгоритма с использованием эталонных данных;

е) процедура для внесения в алгоритм ошибок с целью обучения его отладке.

Указанное позволит пользователю решать задачи в содержательной форме без первоначального знания какого-либо языка программирования, либо активизировать обучение в современных технологиях разработки программ, начиная с этапа алгоритмизации.

К ПРОБЛЕМЕ ПРЕОБРАЗОВАНИЯ ИЗОБРАЖЕНИЙ

Остапкевич А.С.

В системах технического зрения обычно выполняют ряд преобразований: масштабирование, повороты, симметричные отображения и т.п. В основе этих преобразований лежат давно разработанные алгоритмы, которые не учитывают специфики отображения на экране монитора. В результате разной разрешающей способности монитора по вертикали и горизонтали возникают искажения, заметные для глаза. В тех случаях, когда требуется высокое качество рисунка, алгоритмы преобразований необходимо перерабатывать.

В докладе рассматриваются и решаются проблемы преобразования графики Библии Франциска Скорины. 500-летний "возраст" книг Библии существенно сказался на качестве гравюр. Кроме улучшения качества рисунков перед исследователем ставится задача расшифровки тайнописи, закодированной просветителем в графике.

На экране дисплея в удобной для восприятия форме представляется меню пользователя, изображения буквиц и гравюр восточнославянского первопечатника. Оператор имеет возможность вызвать на экран монитора рисунок любой гравюры или буквицы с целью улучшения её ка-

чества и проведения целенаправленных исследований. Программное обеспечение позволяет производить разнообразные преобразования изображений: изменять масштаб, выделять фрагменты, инвертировать рисунок, осуществлять повороты и симметричные преобразования, выделять контуры, осуществлять фильтрацию и т.п.

В результате применения алгоритмов преобразований удалось улучшить качество рисунков, сформировать новые симметричные изображения и расшифровать элементы тайнописи Франциска Скорины.

БЫСТРЫЙ АЛГОРИТМ ЭКСПОНЕНЦИАЛЬНОГО ПРЕОБРАЗОВАНИЯ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Поденок Л.П., Садыхов Р.Х.

Предлагаемая работа посвящена разработке метода и алгоритмов для защиты и аутентификации информации в открытых системах связи.

Производительность криптосистем с открытыми ключами, основанных на нелинейных преобразованиях шифрования/дешифрования, в большой степени определяется тем, как быстро эти преобразования могут быть выполнены. Классическими примерами таких преобразований являются, в частности, вычисление экспоненциальной функции в поле $GF(n)$ по некоторому основанию, представляющему собой один из первообразных корней поля (система открытого распространения ключей Диффи и Хеллмана [1]) и вычисление степенной функции в кольце $Z/(N)$ классов вычетов по модулю N неизвестной структуры (RSA [2]).

В [3] описан бинарный метод возведения целого числа a в целую степень d, выполняемый максимум за $\lfloor log_2 d \rfloor + \nu_1(d)$ операций умножения и возведения в квадрат, где $\nu_1(d)$- количество единиц в двоичном представлении d, основанный на построении аддитивных цепочек $\{1=d_0,\ldots,d_i,\ldots,d_r=d\}$ с элементами $d_i = 2d_{i-1}$ или $d_{i-1}+1$, которые определяют последовательность вычисления a^d с помощью возведения в квадрат и умножений.

В данном докладе представлен метод и алгоритм вычисления экспоненциальной функции в поле $GF(n)$ по основанию a, имеющему мультипликативно обратный элемент a^{-1} в этом поле, максимум за $\lfloor log_2 d \rfloor + min(\nu_1(d), \nu_0(d)) + 1$ операций умножения и возведения в квадрат. Метод основан на представлении показателя d в виде последовательности целых чисел $\{1=d_0,\ldots,d_i,\ldots,d_r=d\}$ с элементами $2d_{i-1}$ или $d_{i-1}\pm 1$, не являющейся аддитивной цепочкой.

В отличие от бинарного метода [3], данный метод помимо возведения в квадрат и умножения на основание a, использует умножение на мультипликативно обратный элемент a^{-1} (деление) в поле, которое соответствует элементу $d_i = d_{i-1}-1$ построенной последовательности. Поскольку нахождение мультипликативно обратного элемента в $GF(n)$ не пред-