

Направления исследований и проекты  
Студенческой Учебно-Исследовательской Лаборатории  
Прикладной Математики и Программирования  
Сыктывкар, 2012 г.

#### LitePAC

Инструментарий разработки и среда запуска управляющих программ АСУТП. Реализованы компилятор Си-подобного языка, виртуальная машина с простым планировщиком задач, утилиты сборки и линковки. Поддерживаются периферия контроллеров ICPDAS LinCon/LinPAC, протокол DCON, протокол Modbus/TCP Slave. На сайте проекта содержится полное описание внутреннего устройства проекта. Много чего хотелось бы доделать, переделать и доработать.

Разработчики: Ильин М.Н.

<http://www.litepac.org>

#### bclite

Интерпретатор для вычислений с плавающей точкой IEEE-754 и поддержкой функций матричной алгебры, с привязками к GSL, CBLAS. Хотелось бы увидеть работающую векторную и матричную математику, методы декомпозиции матриц (LU и Холецкого) а также решение СЛАУ. У нас есть реализация метода численного интегрирования дифференциальных уравнений Рунге-Кутты 4-го и 5-го порядков, хотелось бы иметь возможность использовать его в этом интерпретаторе.

Разработчики: Петрунов А.А.

<svn://wiki.syktu.ru/svn/bclite>

#### bgmodel

Моделирование фона видеопотока на основе смеси Гауссовских распределений, обнаружение движения. Есть рабочая версия EM-алгоритма, поверх которого реализуется моделирование фона как смеси Гауссовских распределений. Для декодирования видеопотока используется libavcodec из проекта FFmpeg. Код нуждается в оптимизации, упрощении и подготовке к релизу и внедрению.

Разработчики: Ануфриев А.Е.

<svn://wiki.syktu.ru/bgmodel>

#### libnvt

Библиотека реализующая Network Virtual Terminal в соответствии с RFC 854 Telnet. Есть готовый, рабочий прототип. Нужно убрать зависимости от GLib, GIO, GTK+ и переделать модель ввода-вывода на POSIX I/O. Возможно, на базе этой библиотеки сразу же сделать мини-клиента telnet. Тогда тогда нужно добавить качественно поддержку минимума опций subnegotiation, такие как NAWs (RFC 1073), TERMINAL-TYPE (RFC 930), ECHO (RFC 857). Интересно было бы попробовать сделать ещё и простой telnetd сервер, который поддерживал бы COM-PORT-OPTION (RFC 2217) и autologin.

<svn://komitex.ru/console/nvt>

#### Console GTK+ Widget

Простой и лёгкий виджет терминального окна. Реализует низкоуровневые функции консоли, такие как перемещение курсора, изменение цвета фона и символов, очистка строки и т.д. Для рендеринга символов используется cairo а битмапы глифов извлекаются с помощью библиотеки FreeType. Виджет не использует текстовые функции Pango. Хотелось бы увидеть подготовленный релиз этого виджета, который можно было бы легко включать в проекты на GTK+. Все public функции нужно документировать в формате GTK-Doc или Doxygen.

<svn://komitex.ru/console>

#### Pangoless GTK+ Font Selection Dialog

Виджет диалога выбора шрифтов. Копирует вид и поведение стандартного диалога выбора шрифтов из библиотеки GTK+, но при этом не использует pango и её функции, а напрямую обращается к Fontconfig. Этот виджет предназначался в первую очередь для использования с Console GTK+.

<svn://komitex.ru/console>

#### Метод конечных разностей (FDM)

Численное решение уравнений в частных производных. Предлагается изучить метод конечных разностей, так как он наиболее простой и понятный из всех. На первом этапе следует начать с варианта реализации, где задача решается обычным последовательным программированием. На втором этапе нужно разработать метод и реализовать его для параллельной вычислительной системы. Задача включает в себя несколько второстепенных, например, необходимо реализовать или научиться пользоваться готовыми библиотеками для работы с разрежёнными матрицами, для решения системы линейных уравнений используют итерационные методы и др.

#### Вычислительный кластер

Лаборатории передано оборудование кластера Beowulf а также персональная супер-ЭВМ с GPU NVidia. Необходимо запустить кластер и персональную супер-ЭВМ, установить туда систему пакетной обработки, организовать возможность удалённого доступа через ssh. GPU NVidia программируются или на проприетарном API CUDA или на относительно свободном и переносимом OpenCL. Актуальна исследовательская задача научиться работать с этими расширениями и интерфейсами программирования. Последние будут отражать аппаратную архитектуру GPU.

#### libmp

Реализация библиотеки целочисленной арифметики произвольной точности и основных теоретико-числовых алгоритмов. Нужно подготовить релиз и документацию к проекту.

<svn://wiki.syktu.ru/svn/crypto/mp>

#### Криптографический калькулятор

Интерпретатор, поддерживающий целочисленную арифметику произвольной точности, основные теоретико-числовые алгоритмы и включающий в себя функции элементарных криптографических преобразований, такие как MD5, SHA1, SHA2, Whirlpool и т.д. Область применения — инструмент прототипирования криптографических протоколов и приложений, генерация тестовых векторов.

Разработчик: Липин Б.Р.

#### Библиотека криптографических примитивов

Имеется набор алгоритмов симметричного шифрования (GOST, AES, Blowfish, IDEA и др.) а также набор алгоритмов хеширования (MD5, SHA1, SHA2, Whirlpool). В библиотеку желательно добавить реализацию криптографически стойкого PRNG и скомпоновать всё в один архив, добавив описание всех функций. Основной мотив создания такой библиотеки — сделать каждый из её модулей максимально автономными и независимыми друг от друга так, чтобы любой мог взять только нужные ему файлы из библиотеки и включить в свой проект.