

Справка

КИРКОРОВ Сергей Иванович.

Ведущий специалист. Награжден Главным комитетом ВДНХ СССР бронзовой медалью «За достигнутые успехи в развитии народного хозяйства СССР».

Научные интересы:

- информационные технологии в образовании, компьютерное моделирование,
- безопасность информационных систем и технологий.



Сергей КИРКОРОВ
ksiby@mediascan.by

Слабым звеном в обеспечении информационной безопасности и надежности прикладного программного обеспечения (ПО) наряду с другими факторами является использование неконтролируемых, закрытых и не сертифицированных по требованиям безопасности информационных технологий (ИТ). Уровень доверия ИТ определяется самым слабым звеном в цепи средств обеспечения информационной безопасности. Поэтому перспективным и востребованным ныне подходом к проблеме формирования собственных доверенных сред разработки ПО является использование инструментальных программных средств с открытым кодом. При этом задачу обеспечения безопасности ИТ в значительной степени решает наличие средств автоматизации верификации и формального доказательства правильности алгоритмов программ.

Проводившийся автором в течение ряда лет мониторинг качества доступных сред программирования показывает, что разработка программных средств в среде GNAT на языке программирования Ada и применение инструментария SPARK для формального доказательства правильности алгоритмов программы обеспечивают создание программных средств критического назначения, соответствующих ISO/IEC 15408-1 с уровнем гарантий EAL5 и выше (в Беларуси СТБ 34.101.1, в России ГОСТ Р ИСО/МЭК 15408).

Однако создание ПО критического назначения (к примеру, для современных медицинских, ядерных и космических технологий) всегда сопровождается разработкой большого объема кода, который по принятой сейчас терминологии относится к классу бизнес-приложений. Он тоже требует обеспечения высокой согласованности функциональности, защищенности, надежности (хотя, как правило, формально не верифицируется), а также совместимости по технологии производства с основной продукцией критического назначения.

Имеются в виду потребители программных средств для операционной системы MS Windows, которые требуют определенного, хотя не самого высокого уровня гарантий информационной безопасности. Для них библиотека OEM for Windows дает возможность объединить среду разработки GNAT GPL 2009 на языке программирования Ada-2005 и существующие технологии для применения в операционной системе Windows от фирмы Microsoft. Библиотека OEM — разумный компромисс между надежностью и безопасностью, с одной стороны, и простотой применения, разработки, низкой стоимости современных ИТ на базе семейства операционных систем (ОС) MS Windows, с другой стороны.

Библиотека OEM проходит всестороннее тестирование. Некоторые тесты можно рассматривать как образцы рационального использования ее средств. Они были положены в основу примеров, которые поставляются вместе с библиотекой.

По мнению автора, чем меньше требуется промежуточного, стороннего, не доверенного слоя ПО для функционирования конечной прикладной системы, тем более высокий уровень гарантий можно обеспечить. Напротив, промежуточные средства, неподконтрольные разработчикам прикладного ПО (типичные для услуг, предоставляемых популярными серверами), снижают такой уровень. Подтверждением этого тезиса может служить, например, оговорка в лицензии на ОС MS Windows 2000, которую фирма Sun

представляет платформа Microsoft .NET Framework в связи с ее повсеместным применением. В основе ее лежит «виртуальный компилятор». Программа при каждом запуске транслирует виртуальный код из файла в исполняемый код аппаратной платформы с помощью .NET Framework. Только после этого ОС загружает фактически неконтролируемый код для выполнения в оперативную память. Разработчик программы может доказать правильность работы только виртуального кода программы на «своем рабочем месте». Фактически .NET Framework может выступать как «ГЛОБАЛЬНЫЙ ВЫКЛЮЧАТЕЛЬ» при необходимости. Злоумышленник может произвести «обновление платформы» или активировать уже существующую программную «закладку» с целью повысить уязвимость платформы .NET Framework (никто не дает гарантий, что таких «закладок» нет, а потребителю не будет возмещен урон от результата ее применения — так написано в лицензии). Альтернативой на основных промышленных платформах может служить

фихацию и сертификацию программных систем;

— простота перехода на другую платформу: основные компоненты GNAT Pro имеют одинаковый интерфейс на всех платформах, на которых реализована технология. Тем самым существенно упрощается перенос разработки с одной платформы на другую;

— эффективная поддержка со стороны разработчиков: неотъемлемой компонентой технологии GNAT Pro является комплекс услуг, включающий в себя консультации по языку Ada и программным компонентам GNAT Pro, помощь в установке и настройке GNAT Pro, оперативное устранение замеченных пользователями дефектов технологии вплоть до поставки исправленных версий компонент GNAT Pro.

Накоплен богатый успешный опыт использования GNAT Pro в промышленных проектах различного объема и сложности, например, в разработке систем с повышенными требованиями к надежности,

— SPARK Pro — технологию, обеспечивающую доказательство корректности разрабатываемого кода.

Решения GNAT GPL 2009 платформа независимые, но пакет Win32 Ada позволяет использовать специфические функции ОС на уровне программного интерфейса Win32 и взаимодействовать с ОС MS Windows, учитывая особенности последней. Это, однако, требует от программиста глубоких знаний интерфейса ОС Win32. Пакет GNATCOM/GWINDOWS позволял формализовать и облегчить задачу для программиста, но совместим только с Ada-95, не отвечает современным требованиям и сложен в установке.

Совместив достоинства этих двух пакетов, мы заложили основу библиотеки OEM — платформы для программирования на языке Ada-2005 в GNAT GPL 2009 Win32 с возможностью локализации для русского языка.

Основные характеристики библиотеки OEM (по современному состоянию):

- интеграция со средой разработки GSP 4.3.1 (20090114);
- наличие средств перекодировки русского (OEM для консоли, ANSI (CP-1251) и Unicode-16 для графической консоли), а также BASE64 для электронной почты;
- собственный менеджер графических окон (исключительно на функциях Win32);
- собственный менеджер COM компонент (исключительно на функциях Win32);
- собственные функции работы с USB устройствами;
- собственные функции работы по протоколу TCP/IP;
- собственные функции работы с СУБД по интерфейсу компонента ADO;
- средства генерации интерфейсов вызова зарегистрированных, создания новых COM объектов на языке Ada-2005/95 (например, OPS сервера для SCADA);
- платформа зависима от Win32.

Сформированная нами библиотека OEM — новый продукт, вобравший в себя опыт и средства многих разработчиков, в том числе и автора [Киркоров С. И., Киркорова Л. С. *Параллельные алгоритмы математических моделей: исследование локальности и применение языка Ada* // «ВІСНИК Харківського національного університету імені В. Н. Каразіна». — № 863. — Серия: Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. — Випуск 12. — С. 129–142. — Харків, 2009].

Он свободно доступен в образовании, позволяя бесплатно (и особенно удобно для участников GAP [The GNAT Academic Program] [Электронный ресурс]. — <http://www.adacore.com/home/academia/>) использовать основные компоненты технологии GNAT Pro под Win32 (без каких-либо ограничений по функциональности) в образовательных и научно-исследовательских целях (http://www.mediascan.by/index.files/CD_Ada-2009_OEM.zip).

ДОВЕРЕННАЯ ПЛАТФОРМА ПРОГРАММИРОВАНИЯ НА ЯЗЫКЕ Ada в Win32



УП «МедиаСкан», г. Минск, Республика Беларусь

Замечание по поддержке java

Данное программное изделие может содержать поддержку программ, написанных на java.

Технология java — неустойчивая к сбоям и не разработана, изготовлена, или предназначена для использования или перепродажи как интерактивное оборудование управления в опасных средах, требующих отказоустойчивой работы, таких как системы управления ядерным оборудованием, системы навигации самолета или системы связи, системы управления воздушным движением, машины поддержки жизнеобеспечения или оружейные системы, в которых сбой в технологии java может привести непосредственно к смерти, телесному повреждению или серьезному физическому или экологическому ущербу.

Microsystems, Inc письменно обязала сделать компанию Microsoft.

Интересная ситуация сложилась с повсеместным использованием программной платформы Microsoft .NET Framework и Microsoft Visual Studio 2008 и более поздних версий. Практически все программные продукты Microsoft от серверных (например SQL Server 2005) до прикладных и клиентских приложений обеспечивают свой функционал при обязательной установке Microsoft .NET Framework. Платформа разработки Microsoft Visual Studio 2008 позволяет выполнять так называемую «AGILITY» разработку, более того, проводит разработку программистов в таком подходе. Последняя версия эффективна в бизнесе для выманивания финансовых средств у потребителя. В результате потребитель-заказчик получает «вечно» недоделанную программу или комплекс программ — «программу сегодня». Разработчики 80% своего времени проводят за отладкой программы в отладчике, а потребителю только и успевают ставить «сервиспаки» и новые версии. При этом на каждой бесконечной стадии цикла разработки можно наблюдать такую же картину, как в общеизвестном шарже «качели», родившемся на свет лет 35 назад (рис. 1). Цикл заканчивается, когда финансирование проекта прекращается, а потребитель работает на системе с огромным количеством «костылей».

Мало что дает такой подход и при подготовке программистов. Фактически программиста, прекрасно знающего прежнюю версию Microsoft Visual Studio, приходится в корне переучивать (еще в большей степени это относится к ПО фирмы BORLAND). А то и заменять на более молодого выпускника вуза. Тот начинал с изучения недавней последней версии и не тянет за собой ненужный старый багаж узкого специалиста. Последний подход экономически более выгоден. Чаще всего так и поступают руководители, но очень скоро ситуация повторяется.

Серьезную проблему для безопасности ИТ в дальней перспективе, по мнению авто-

современная среда разработки программ на языке Ada — GNAT Pro [Рыбин С. И., Годунко В. *GNAT Pro — Ada — технология для серьезных проектов. Семинар, выставка PTS-2009, Минск. [Электронный ресурс]. — <http://www.mediascan.by/index.files/GNAT-AdaCore.pdf>]. Она позволяет разрабатывать как программные системы, полностью реализованные на языке Ada, так и создавать многоязыковые системы. Технология присутствует на основных промышленных платформах (в том числе MS Windows, различные версии UNIX и GNU/Linux, Mac OS, HP-UX), она включает в себя кросс-компиляторы для популярных встроенных архитектур. GNAT Pro распространяется с исходными кодами всех своих компонент. Важным аспектом технологии является постоянная техническая поддержка клиентов (в том числе — бесплатная для университетов, участвующих в программе GAP (GNAT Academic Program) [Мищенко В. О., Гахов А. В. *Обучение проектированию систем и основам параллельных вычислений на базе языка Ada в Харьковском национальном университете. Семинар, выставка PTS-2009, Минск. [Электронный ресурс]. — <http://www.mediascan.by/index.files/adaedu.pdf>].**

GAP — это программа, предоставляющая возможность высшим учебным заведениям бесплатно использовать основные компоненты технологии GNAT Pro (без каких-либо ограничений по функциональности) в образовательных и научно-исследовательских целях [Рыбин С. И., Годунко В. *Ada — перспективы использования в индустрии и образовании. Семинар, выставка PTS-2009, Минск. [Электронный ресурс]. — <http://www.mediascan.by/index.files/Ada-AdaCore.pdf>].* В этом случае используется версия GNAT GPL.

GNAT Pro удовлетворяет реальным требованиям индустриальной разработки программного обеспечения:

— разработка и сопровождение больших программных систем: GNAT Pro в состоянии работать с проектами, включающими в себя тысячи модулей, предлагает при этом удобные средства структурирования и конфигурирования компонент разрабатываемой системы с поддержкой коллективной разработки;

— разработка многоязыковых систем: использование единой для всех компиляторов семейства GNU GCC технологии генерации объектного кода облегчает использование в рамках одной системы модулей, реализованных на разных языках (Ada, Си, Си++, Фортран). GNAT Pro поддерживает все средства межязыкового взаимодействия, определяемые последней ревизией стандарта языка Ada (Ada-2005);

— высокая эффективность и производительность: эффективность объектного кода обеспечивается сочетанием технологий оптимизации кода, специфических для языка Ada, с мощными средствами оптимизации кодогенератора семейства компиляторов GNU GCC. При реализации библиотек поддержки периода исполнения особое внимание уделено оптимизации обработки исключитель-

ных ситуаций и межпроцессного взаимодействия;

— развитый инструментарий (включаящий в себя, в частности, монитор использования программного стека, средства автоматизации тестирования, систему подсчета метрик, средства анализа программного кода, средства контроля стиля кодирования и др.);

— набор библиотек и программных интерфейсов;

— набор решений, облегчающих вери-

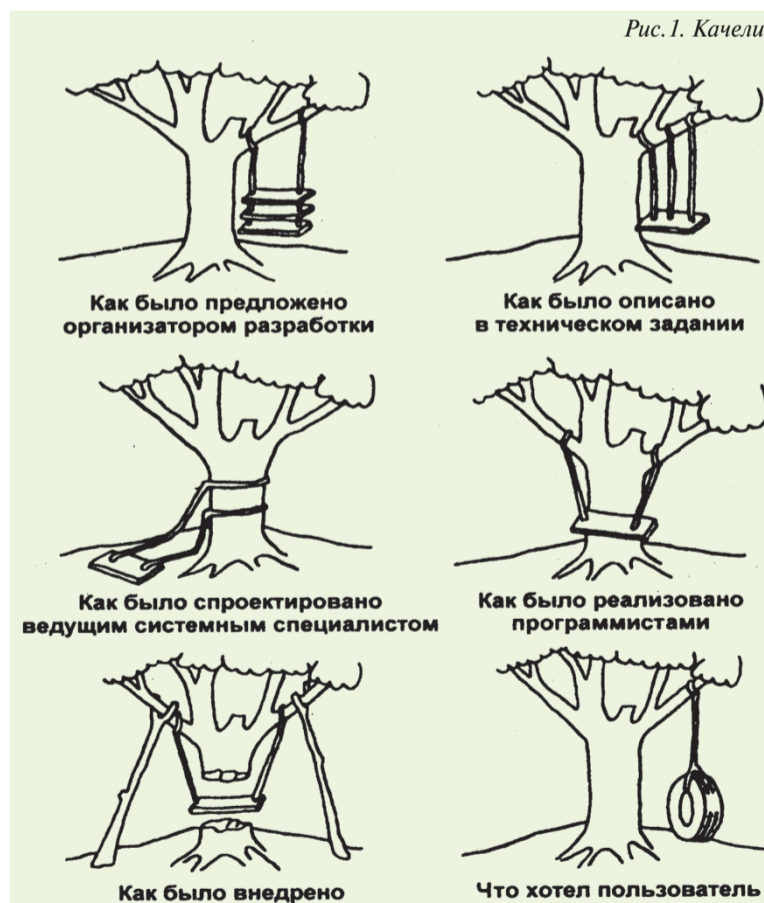


Рис. 1. Качели

Как было предложено организатором разработки

Как было описано в техническом задании

Как было спроектировано ведущим системным специалистом

Как было реализовано программистами

Как было внедрено

Что хотел пользователь

Учредитель — Министерство обороны Республики Беларусь



Начальник государственного учреждения «Военное информационное агентство Вооруженных Сил Республики Беларусь «Вяр»

Андрей ШУБАДЕРОВ
Заместитель начальника агентства — главный редактор печатных СМИ
Владимир АЛЕКСАНДРОВ

Для писем:
220029, Минск-29,
ул. Архитектора Заборского, 4

E-mail:
vsr@mail.by
mod@mod.mil.by

Наш адрес в Интернете:
<http://vsr.mil.by>

Телефоны агентства:
Заместитель начальника агентства — главный редактор печатных СМИ — 297-16-26

Отдел идеологической работы — 297-29-90, 297-16-95
Отдел боевой подготовки и строительства Вооруженных Сил — 297-14-90
Отдел зарубежной военной информации — 297-16-24
Отдел новостей — 297-14-90
Отдел подготовки материалов — 297-18-68, 297-16-84
Группа писем и рекламы — 297-14-23

Факс — 293-44-92
Бухгалтерия — 297-10-44
Дежурный — 293-43-18, 297-14-14

Посткорровские пункты:
Витебск — 24-77-51
Борисов — 79-55-10

При перепечатке ссылка на «Белорусскую военную газету» обязательна.

Редакция может публиковать материалы, не совпадающие с точкой зрения редакции, в порядке обсуждения. Авторы материалов несут ответственность за точность приведенных фактов, цитат, цифр и прочих сведений.

Рекламные материалы обозначаются значком R

Свидетельство о регистрации №1142 от 4 февраля 2010 г.

Печать: Республиканское унитарное предприятие «Издательство «Белорусский Дом печати» ЛП 02330/0494179 от 3.04.2009 г. Р/с 3604901562013
Адрес: 220013, Республика Беларусь, Минск-13, пр. Независимости, 79

Подписной индекс: 63869
Выходит 5 раз в неделю

Подписана в печать 23.03.2010
Заказ №1401
Тираж 31.741

ISSN 1993-1336

