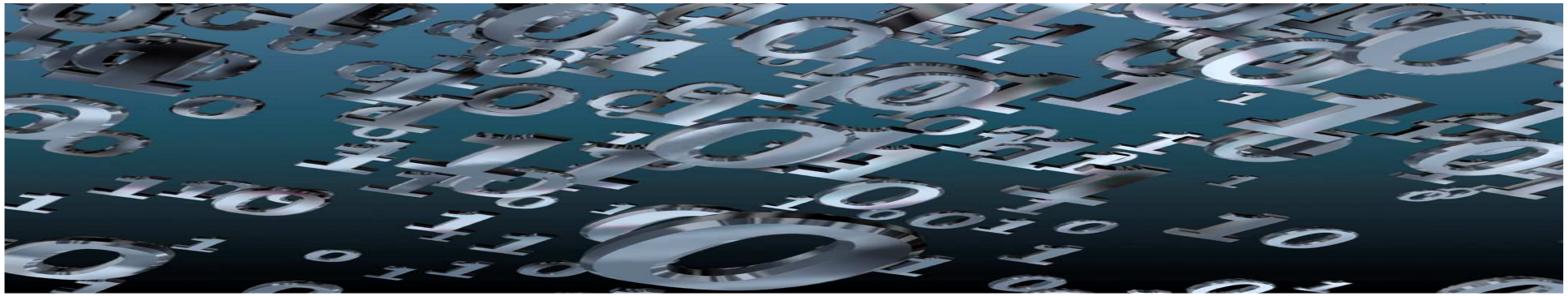
ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ДЛЯ АТТЕСТАЦИИ РАБОЧИХ МЕСТ ИТ

С. И. Киркоров,

Научно-производственное предприятие МедиаСкан,

Республика Беларусь



Стандарты безопасности ИТ

- TCSEC (Оранжевая книга)
  - Критерии оценки безопасности высоконадёжной компьютерной системы.
- Общие критерии оценки безопасности в Информационных технологиях (ИТ) (ISO/IEC 15408-1, в РБ СТБ 34.101.1)
  - Критерии оценки безопасности ИТ;
  - 7 уровней оценки безопасности.
- СТБ ISO/IEC 27001-2011
  - устанавливает требования к внедрению средств управления безопасностью с учётом потребностей конкретных организаций и их подразделений.
- ТКП 288-2010 (07040)
  - Технический кодекс устанавливает требования к процессам управления рисками в сфере информационных технологий банков, относящихся к категории операционного риска.
- СТБ П 34.101.41-2009
  - Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения.
- СТБ П 34.101.42-2009
  - Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности.

Значима ли надёжность программного обеспечения?

- Несомненно значима! На маркетинговом уровне ☺
  - Ни один поставщик не скажет, что его программное обеспечение ненадёжно
  - Ни одна команда разработчиков не сообщит, что разрабатывает ненадёжное ПО
- В действительности, есть огромное количество ПО, ошибки в котором нас никак не задевают
- Не все программы нуждаются в том, что бы требование надёжности ставилось на первый план
- Сбой полезных, но некритичных программ все еще приемлемо 😐
  - Если произойдет сбой во время этой презентации – достаточно просто перегрузить компьютер
  - Если Ваш текстовый редактор зависнет во время набора важного документа, это не принесет Вам ощутимого вреда, если Вы часто сохраняли результаты своей работы

ПО и Критичность

- Критичность по отношению к бизнес-процессам
  - Сбой программного обеспечения может привести к значительным финансовым потерям и даже к полной остановке бизнеса
  - Например, система межбанковских платежей

- Критичность по отношению к решаемой задаче
  - Сбой программного обеспечения может привести к невыполнимости поставленной задачи
  - Например, спутник для исследования Марса

- Критичность по отношению к безопасности
  - Сбой программного обеспечения может привести к человеческим жертвам или большим разрушениям
  - Например, самолет

Сбои ПО в средствах связи и последствия

- Январь 15, 1990: на 9 часов остановлена общенациональная телефонная сеть США
  - месяц ранее AT&T обновила ПО на 114 коммутируемых телефонных станциях
  - Причина: 1 неуместный оператор “break” в программе на языке C
- Январь 2001: отзывается 230,000 единиц новых мобильных телефонов с доступом в Интернет
  - Пользователи сообщают, что их телефоны зависают после посещения некоторых web-узлов, а после перезапуска телефона все сохраненная на нем информация (адреса, ссылки, записи) теряется
- Matracom 6500 PABX (телефонный коммутатор)
  - Искажение случайных телефонных разговоров
  - Внезапное прерывание длинных телефонных звонков

Международные стандарты на критичное к безопасности ПО

- RTCA/EUROCAE DO-178B
  - Международный стандарт на критичное для безопасности ПО в области авиастроения
- IEC 880
  - Стандарт на ПО для атомных электростанций
- IEC61508 / DEF STAN 00-55/56
  - Европейский стандарт безопасности
- Руководство разработчика ПО для транспортных средств
  - Стандарт безопасности, предложенный Ассоциацией разработчиков безотказного ПО для автомобильной промышленности MISRA (Motor Industry Software Reliability Association)

Существующие инструментальные средства.

- Испытательные лаборатории для проведения аттестации рабочих мест руководствуется программой аттестации подсистемы защиты информации информационной системы и методикой проверки организационно-технических мероприятий по защите информации. Использование специальных инструментальных средств позволяет найти уязвимости в сетевых распределённых и локальных системах, а также в сетевом оборудовании и приложений работающих под управлением сетевых ОС.

Существующие инструментальные средства

- Сканеры сетевой безопасности, разработанные с применением архитектуры клиент-сервер, например: NESSUS [1] требуют предварительной установки своих компонентов в информационной системе.
- Владелец ИС может обосновать запрет на применение таких сканеров сетевой безопасности.
- Проблемы также возникают при наличии большого количества географически удалённых рабочих мест ИТ с низкоскоростными каналами связи или просто большого количества ПЭВМ с ограничением времени на проведения аттестации.

Требования к инструментальным средствам аттестации

- Загрузка программы для выполнения осуществляется с **внешнего носителя** (USB Flash) или с временного каталога встроенного диска ПЭВМ.
- При этом программа **не требует**:

1. установки на компьютер, с которого производится запуск программы;
2. наличия специальных динамически загружаемых библиотек (например, библиотек Delphi и т.д.);
3. наличия установленных виртуальных машин (например, VM Java);
4. дополнительной среды исполнения (например, Microsoft .Net FrameWork);
5. подключения к глобальной сети Internet.

Обоснование выбора языка

- Встроенная поддержка многозадачности является уникальной и широко известной особенностью языка программирования Ada, которая выгодно отличает его от большинства современных языков программирования
- Одним из решением задачи – интеграция подходов и АПП на самом раннем этапе подготовки к проведению вычислительного эксперимента и при создания реальных систем, для которых необходимо проводить сертификационные испытания и аттестацию по требованиям информационной безопасности. Своеобразным "программным клеем" целесообразно использовать язык программирования Ada. Реализацией идеи интеграции является расширяемая платформа OEM-2011 for Windows разработанная на языке программирования Ada в УП МедиаСкан.

Сравнение языков программирования отвечающий требованиям реализаций ПО средств связи

Требования	C#	Java	C/C++	Ada
Применение в различных аппаратно-программных платформах в текущий момент времени	+	+	+	+
Принят ISO стандарт языка программирования	-	?	+	+
Развитие языка должно происходить в рамках стандартизации и обеспечиваться инструментальными средствами разработки для всех версий стандартов языка	-	-	-	+
Интеграция с современными технологиями ИТ	-	-	+	+
Язык программирования должен быть перспективным в будущем	?	?	+/?	+
Имеется версия транслятора языка сертифицированная по требованиям стандартов технической защиты информации	-	-	+/?	+

Содержимое Лицензии Windows 2000

ЗАМЕЧАНИЕ ПО ПОДДЕРЖКЕ JAVA

ДАНОЕ ПРОГРАММНОЕ ИЗДЕЛИЕ МОЖЕТ СОДЕРЖАТЬ ПОДДЕРЖКУ ПРОГРАММ, НАПИСАННЫХ НА JAVA .

ТЕХНОЛОГИЯ JAVA - НЕ УСТОЙЧИВАЯ 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 ПОДДЕРЖАНИЯ ЖИЗНЕОБЕСПЕЧЕНИЯ ИЛИ ОРУЖЕЙНЫЕ СИСТЕМЫ, В КОТОРЫХ СБОЙ В ТЕХНОЛОГИИ JAVA МОЖЕТ ПРИВЕСТИ НЕПОСРЕДСТВЕННО К СМЕРТИ, ТЕЛЕСНОМУ ПОВРЕЖДЕНИЮ, ИЛИ СЕРЬЕЗНОМУ ФИЗИЧЕСКОМУ ИЛИ ЭКОЛОГИЧЕСКОМУ УЩЕРБУ.

Sun Microsystems, Inc письменно обязал Microsoft делать эту оговорку.

Ada: использовать для систем, связанных с безопасностью

- Требования безопасности рекомендуют использование языка Ada для самых высоких уровней целостности

- Даже документ MISRA-C рекомендует использование Ады:

  Рекомендации по использованию языка С для создания ПО для транспортных средств:

  –*“...очевидно, что есть и другие языки, которые в многом лучше подходят для создания систем, связанных с безопасностью, обладающие (к примеру) большей надежностью и лучшим контролем соответствия типов . Примером подобных языков, в целом значительно превосходящих С, есть Ada и Модула 2. Если эти языки доступны для предлагаемых систем, то их применение, в сравнении с С, считается более предпочтительным.” стр.3.*

Язык программирования и надежность - философия (1).

- Создание программы (программной услуги) – не написание кода, а определение и использование моделей и абстракций, соответствующих объектам и процессам в решаемой задаче или проблемной области.

- Уровень и разнообразие базовых абстракций должен соответствовать уровню и разнообразию решаемых задач («принцип сундука»)
  - готовые и удобные решения для часто встречающихся технологических потребностей;
  - удобные средства создания проблемно-ориентированных абстракций;
  - высокая производительность на полном жизненном цикле программной услуги;

Язык программирования и надежность - философия (2).

- «Все, что не разрешено – запрещено!» Язык реализует жесткую дисциплину прогнозирования (определения свойств абстракции при ее создании) и контроля* (использования абстракции в соответствии с определенными для нее свойствами);

- Чем раньше обнаружится ошибка (несоответствие использования абстракции определенным для нее свойствам), тем проще, быстрее и дешевле оказывается ее устранение;

---

* Кауфман В.Ш - Языки программирования. Концепции и принципы М.:Радио и связь, 1993

Язык программирования и надежность - философия (3).

- Программист в основном занят сопровождением и модификацией чужого кода, а не созданием своего
  - ясность и хорошая структурированность кода многократно важнее возможности быстро его написать!
- Сложный инструмент редко бывает надежным
  - предоставляя больше возможностей, чем Си++, Ada оказывается существенно более простым языком для изучения и понимания;
- Все, что может быть определено – должно быть явно определено!
  - умолчания и надежда на «здравый смысл» - один из основных источников недоразумений и ошибок!
  - определение Ada «замкнуто». По сравнению с Си/Си++, например:
    - правила видимости не требуют привлечения мифического понятия «пространства имен», а вполне обходятся синтаксическими конструкциями языка;
    - правила модульности и раздельной компиляции не требуют привлечения внеязыкового понятия «файл», а также обходятся синтаксическими конструкциями языка;

Язык программирования и надежность - философия (4).

- Опережающая стандартизация
  - Ada возникла и развивалась как ***стандарт*** языка программирования;
  - Средства контроля стандарта Ada были разработаны к моменту принятия первого стандарта языка – все индустриальные реализации Ada достаточно точно соответствуют той или иной версии стандарта, диалектов Ada в индустрии не было и нет;
- Классификация ошибок в программе на уровне стандарта языка. Стандарт чётко подразделяет все содержащиеся в нем требования на следующие группы:
  - проверяемые во компиляции отельного модуля (нарушение требования означает, что компиляция не является успешной, в ее результате не будет создан объектный код);
  - проверяемые при сборке программы из успешно скомпилированных модулей (нарушение требования означает, что исполняемый файл создан не будет);
  - проверяемые при выполнении программы (нарушение требования приводит к возбуждению предопределённого исключения);
  - правила, нарушение которых реализация проверять не обязана.

  Средства контроля стандарта проверяют, что поведение реализации соответствует этой классификации!

Инструментарий, разработанный на языке Ada в УП МедиаСкан

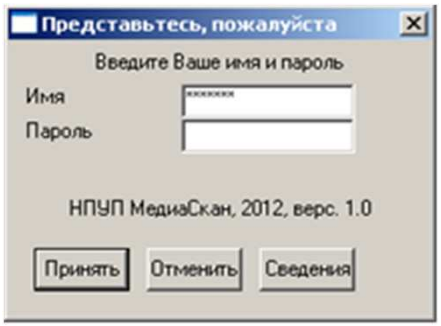
- Программа HlocM «Обнаружение компьютеров в сети TCP/IP» предназначена для обнаружения подключения компьютеров в вычислительной сети стека TCP/IP при проведении аттестационных испытаний в локальных сетях. HlocM разработана на основании документа «Программа методического и инструментального обеспечения испытательной лаборатории средств и систем защиты информации».
- Уникальность решения - в использовании низкоуровневого интерфейса и утилит операционной системы, что позволило, не нарушая работы подсистемы защиты информации, собрать необходимые сведения текущего профиля пользователя и быстро формировать отчёт.

Инструментарий, разработанный на языке Ada в УП МедиаСкан

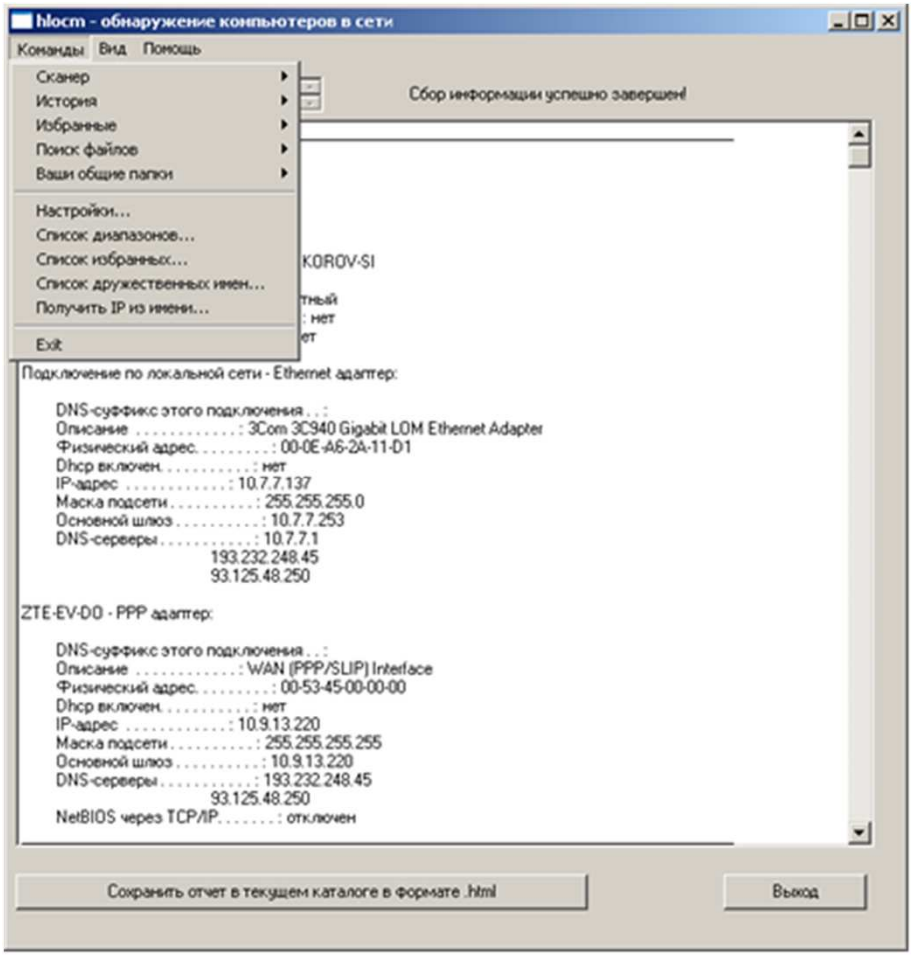
- Программа HlocM «Обнаружение компьютеров в сети TCP/IP» предназначена для обнаружения подключения компьютеров в вычислительной сети стека TCP/IP при проведении аттестационных испытаний в локальных сетях. HlocM разработана на основании документа «Программа методического и инструментального обеспечения испытательной лаборатории средств и систем защиты информации». Программа HlocM обеспечивает:
- а) сканирование компьютера по следующим параметрам:
    1. текущие ресурсы компьютера;
    2. параметры загрузки компьютера;
    3. доступные сетевые ресурсы компьютера;
    4. учётные записи пользователей на компьютере;
    5. локальные группы пользователей на компьютере;
    6. текущие локальные открытые порты и соединения;
    7. список ресурсов сети и их доступность;
    8. параметры входа пользователя из реестра;
    9. автоматически запускаемые программы;
    10. расшаренные диски;
    11. существующий удалённый доступ (в т.ч. Internet);
    12. служба удалённого доступа (прописанные модемы);
    13. проверка подключения к Internet;
- б) получение отчётов в формате .html и .txt по считанным параметрам.

Инструментарий, разработанный на языке Ada в УП МедиаСкан

- В появившемся на экране окне нужно ввести имя оператора, пароль для запуска программы и нажать на кнопку «Принять» или на клавишу «Enter»



- После того, как завершился процесс сбора информации, в текстовом окне отображаются все считанные данные о компьютере.
- Для сохранения всех данных в виде отчёта в файле .html в текущем каталоге, нужно нажать на кнопку «Сохранить отчёт в текущем каталоге в формате .html».



Апробация решения

- Сбор сведений о технических и информационных ресурсах ПЭВМ – обязательный этап программы-методики проведения аттестации. Существует большое количество программ, которые позволяют провести аудит системы, но при этом формирование отчёта в необходимой форме они не производят. Для выполнения на ПЭВМ эти программы требуют своей инсталляции, тем самым косвенно могут нарушить подсистему защиты. Использование библиотеки «Платформа OEM-2011 для MS Windows XP» [2,3] научно-производственного предприятия МедиаСкан и транслятора с инструментальными средствами для языка программирования Ada GNAT GPL 2011 корпорации AdaCore [4] позволило разработать инструментальны средства аттестации, удовлетворяющие выше изложенным требованиям.

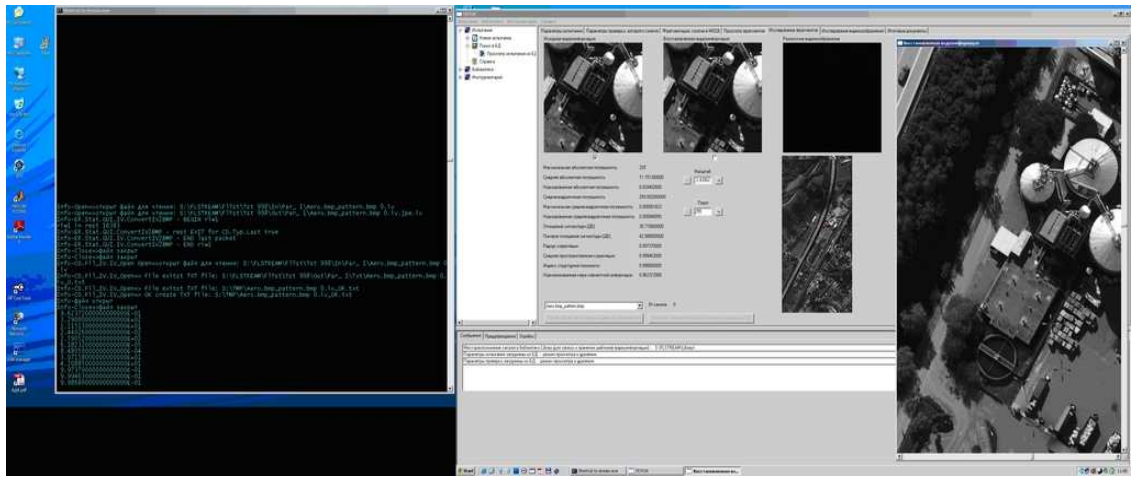
Апробация решения

- Разработанные инструментальные средства аттестации использовались для проведения проверки объекта ИСУ организации. Проверки включают в себя анализ действующих в организации организационно-распорядительных документов по защите информации и испытания средств защиты информации в реальных условиях эксплуатации объекта ИСУ организации. По результатам аттестации подсистемы защиты информации был выдан аттестат соответствия требованиям по защите информации. Благодаря применению разработанных инструментальных средств аттестации задокументированные проверки более 50 ПЭВМ заняли менее четырёх часов без остановки информационного процесса в организации..

Примеры разработок на языке Ada НПП МедиаСкан

1. Подсистема управления въездом-выездом подземного паркинга ТЦ «СТОЛИЦА» г. Минск - 2005 г.

2. Программное обеспечение испытательного стенда аппаратуры сжатия видеоинформации г. Минск – 2008 г.

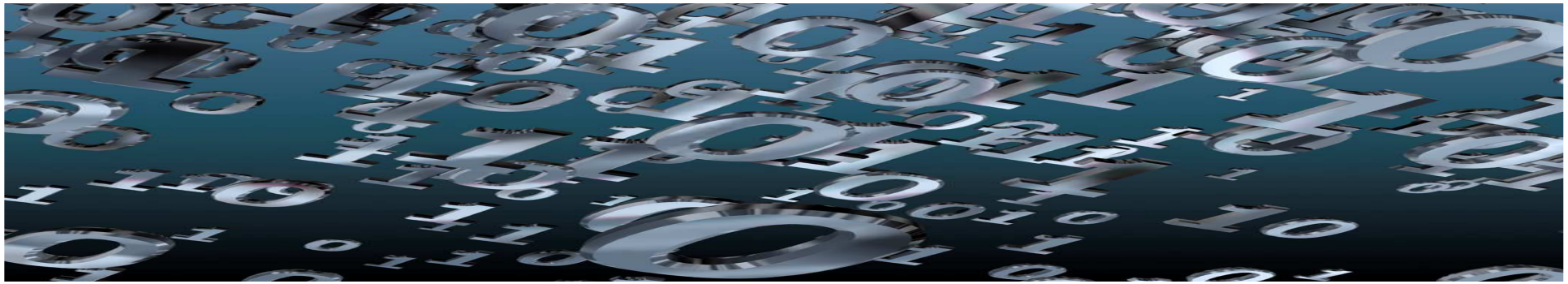


Заключение

- Приведённые в сообщении аргументы доказывают актуальность созданных специализируемого инструментального средства аттестации и библиотеки OEM для Ada программистов, а их характеристики позволяют рассчитывать, как на профессиональные, так и учебные применения в академической среде совместно с дополнительной литературой [5].

ЛИТЕРАТУРА

1. Сканер Nessus. [Электрон. ресурс]. – http://www.nessus.org/products/nessus .
2. Киркоров С. И. Новая библиотека OEM как средство обучения и база для доверенных платформ программирования на языке Ada в Win32. Харьков, май 2010 года тезисы доклада на конференции «КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ В НАУКОЕМКИХ ТЕХНОЛОГИЯХ» (КМНТ-2010).
3. Платформа OEM-2011 для MS Windows XP. [Электрон. ресурс]. – http://www.mediascan.by/index.files/Page695.html .
4. GNAT GPL 2011 корпорации AdaCore. [Электрон. ресурс]. – http://www.adacore.com .
5. Гавва А. Е. “Адское” программирование. Ada-95. Компилятор GNAT: [Электрон. ресурс]. – http://www.ada-ru.org.



СПАСИБО ЗА ВНИМАНИЕ

Media Scan by
Наука, разработка, внедрение