Лекция №3

Технологии и методы проектирования вычислительных модулей

Обеспечение информационной безопасности на этапах жизненного цикла вычислительных модулей

Бычков Игнат Николаевич

МФТИ/МИРЭА

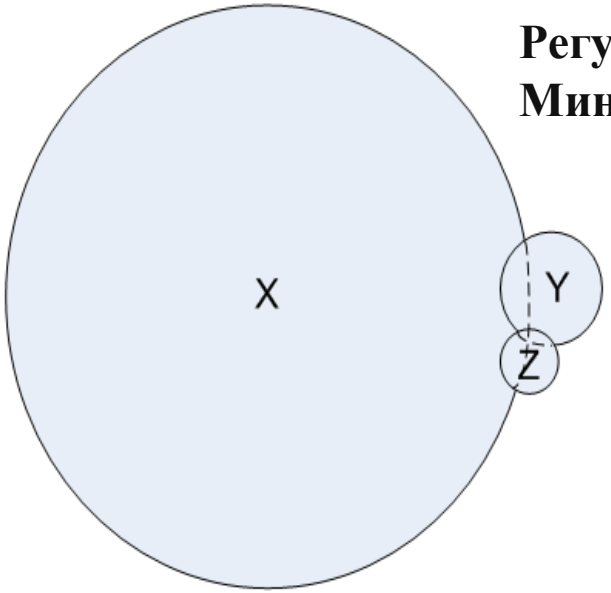
Москва, 2024 г.

Стандарты для обеспечения информационной безопасности

Стандарт ГОСТ РВ 0015-002-2012 регламентирует работу систем менеджмента качества компаний, чья деятельность связана с исследованиями, разработкой, производством, поставкой, обеспечением эксплуатацией, ремонтом и утилизацией оборонной продукции.

ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

Регуляторы ФСТЭК, ФСБ и Минобороны России



X- ошибки, приводящие к нарушению доступности информации

Y- ошибки, приводящие к нарушению целостности информации

Z- ошибки, приводящие к нарушению конфиденциальности информации

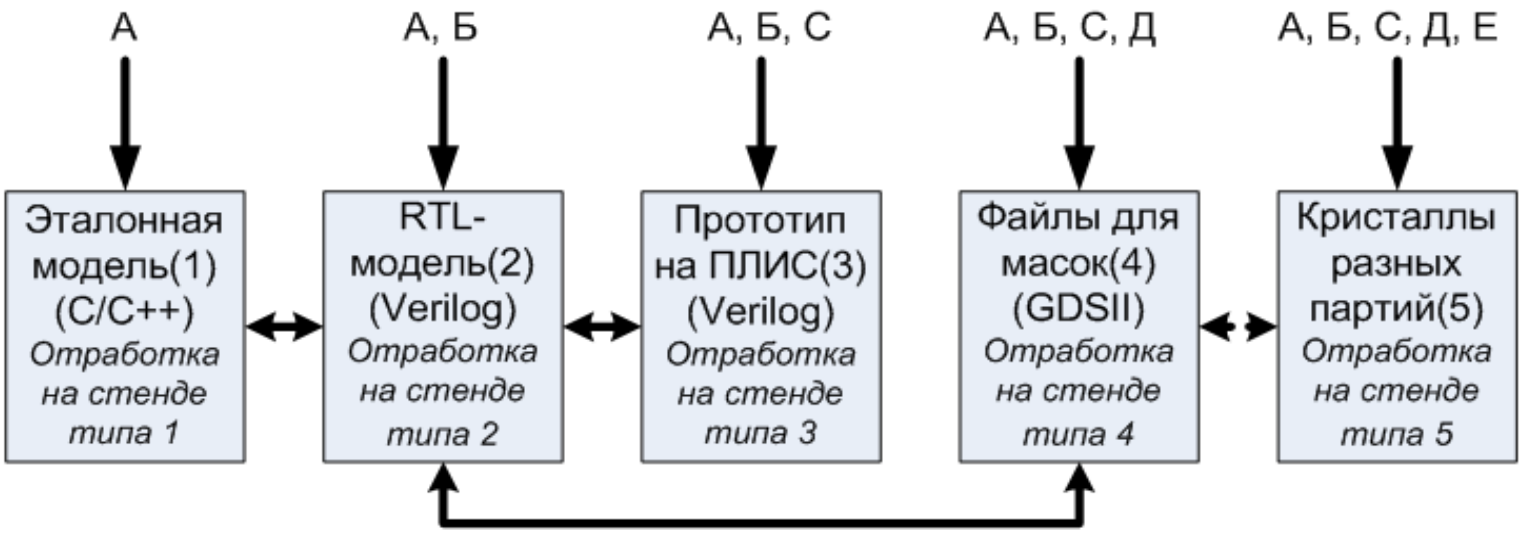
Уязвимости процессоров в основе модулей (пример)

Уязвимость / нарушение	Процессор и год выпуска	Краткое описание уязвимости
Двойная сигма / доступность	Intel 80386/ 1985-1986 г.	Процессоры Intel 80386 (еще до 386DX и 386SX) могли зависать при выполнении 32-битного кода. Компания не могла найти сбойные процессоры при производстве.
Pentium FDIV / целостность	Pentium 60/66 МГц / 1993-1996 г.	Ошибка выражалась в том, что при делении чисел с плавающей запятой при помощи команды FDIV результат мог получаться некорректным.
God Mode / целостность доступность конфиденциал.	Все процессоры Intel с 1995 - 2010 г.	Использование режима System Management Mode (SMM) для отладки процессора, в котором приостанавливается исполнение любого стороннего кода и запускается специальная программа, хранящаяся в защищенной области памяти. Получение всех прав доступа.
Spectre CVE-2017-5753 и CVE-2017-5715 / конфиденциал.	Все процессоры Intel с 1995-2017 г.	Возможность анализа изолированных данных пользователей в программах, выполняемых с применением спекулятивных вычислений.
Meltdown CVE-2017-5754 / конфиденциал.	Все процессоры Intel с 1995-2017 г.	Возможность обойти меры изоляции памяти и получить доступ на чтение памяти операционной системы, что приводит к возможности анализа данных пользователей, включая клиентов облачных инфраструктур.
Foreshadow/ L1 Terminal Fault (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646) / конфиденциал.	Intel® Core™ и Xeon® Processor E3 processors 2015-2017 г.	Составная уязвимость на технологию защиты данных SGX из трёх составляющих: уязвимость в Intel Software Guard Extensions (SGX), уязвимость ядра операционной системы и System Management Mode (SMM), уязвимость программ виртуализации и Virtual Machine Monitors (VMM).

Примеры уязвимостей процессоров.

Тесты на этапах жизненного цикла (неполный список)

Типично для модулей – аттестация каналов. Обязательны тесты на DDRx, PCIe, межпроцессорные каналы и т.д. с определением зон работоспособности.



↔ - проверки соответствия моделей

А- тесты проверки архитектуры (AVS)

Б - автономные и направленные тесты устройств

С – тесты через JTAG с использованием встроенных анализаторов

Д – анализ/расчеты временных характеристик, мощности, напряжений и т.д.

Е – тесты и анализ данных от встроенного диагностического оборудования
(датчиков температур, напряжений в кристалле и токов потребления стенда и т.д.)

Тестирование загрузчика (BIOS / BOOT)

При адаптации свободного программного обеспечения с учетом обхода аппаратных уязвимостей эффективна практика применения общих технических требований к общему программному обеспечению и общесистемному программному обеспечению общего назначения. Эти требования включают нормы ГОСТ Р 56939-2016 при совместном применении с ГОСТ Р 58412-2019. В указанном стандарте можно выделить следующие ключевые нормы:

- требования к содержанию и порядку выполнения работ, связанных с созданием безопасного программного обеспечения;
- меры по разработке безопасного программного обеспечения применяются в течение всего жизненного цикла, есть связь с процессами, описанными в ГОСТ Р ИСО/МЭК 12207-2010;
- введен базовый набор мер по разработке безопасного программного обеспечения;
- предусмотрено шесть видов испытаний программного обеспечения: статический анализ и экспертиза кода, функциональное тестирование программы, тестирование на проникновение, динамический анализ кода и фаззинг-тестирование.

Применение двоичной трансляции

Интересным применением двоичной трансляция уровня системы является запуск операционных систем в двоичных кодах популярной системы команд x86-64, например операционных систем типа *Windows*.

Преобразование кодов нецелевой системы команд с оптимизациями может исключить вредоносное программное обеспечение для исполнения. В общем случае уязвимостью является нарушение информационной безопасности при выполнении условий ее реализации:

$$V(CVE) = \{Proc, Prog, Vector\}$$

где *Proc* – процессор для исполнения, *Prog* – совокупность программ для исполнения, *Vector* – вектор атаки как результат исполнения программ и направленность действий по его применению. При использовании двоичного транслятора во множестве случаев имеется следующее неравенство:

$$V(CVE) = \{Proc, Prog, Vector\} \neq \{Proc_N, Prog_N, Vector\}$$

где $Proc_N$ - процессор для исполнения преобразованного кода, $Prog_N$ - код программ для исполнения на целевой платформе (*native*).

- программа начального старта ТВГИ.00727-28 (сертификат соответствия №4541, выдан 09 декабря 2019 г., действителен до декабря 2024 г.)

-встроенный комплексом средств защиты операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10265-01 («Ленинград») (сертификат соответствия №4295, выдан 29 марта 2019 г. действителен до марта 2022 г.);

- встроенный комплексом средств защиты операционной системы Альт 8 СП ЛКВН.11100-02, ЛКВН.11100-01

- антивирус Dr.Web Enterprise Security Suite RU.72110450.00311-09 (сертификат №3075 с инсп. контролем от 27.09.2019 г. действителен до сентября 2022 года)

- система битовой компиляции ТВГИ.00357-28 (сертификат №4542, выдан 09 декабря 2019 г., действителен до декабря 2024 г.) для запуска защищенных магнитных носителей информации («JaCarta SF/ГОСТ АЛДЕ.26.20.21.120-03/ АЛДЕ.26.20.21.120-04»)

Средства защиты информации (ФСБ России)

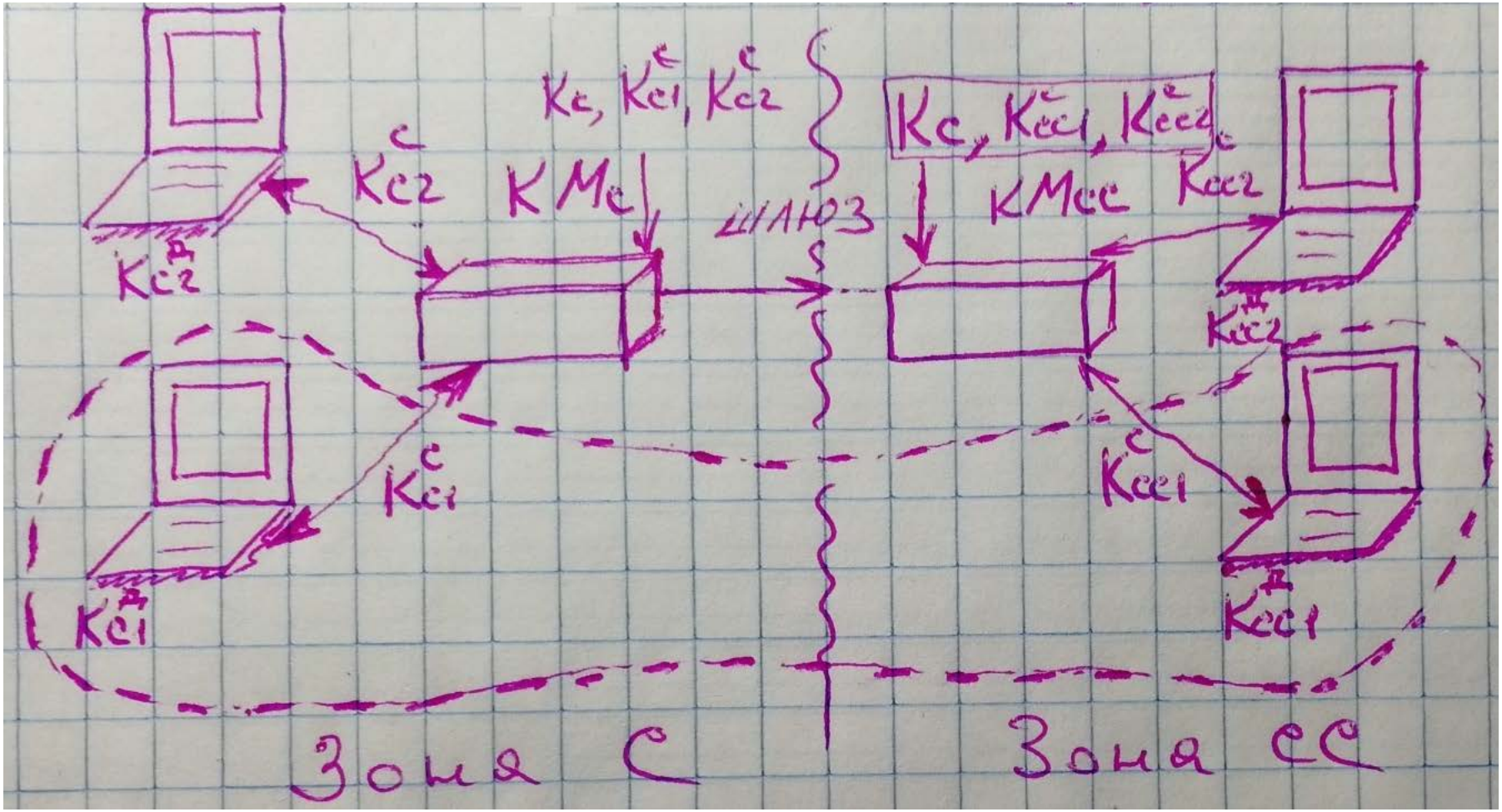
- встроенный комплексом средств защиты (далее по тексту – КСЗ) операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-16 исполнение 2 («Ленинград») (сертификат соответствия № СФ/СЗИ-0265, выдан 10 апреля 2019 г., действителен до 4 апреля 2024 г.);

- КПС Э-8С РНДК.00953-01 включая бинарный компилятор уровня системы ТВГИ.00383-02 (сертификат соответствия № СФ/СЗИ-0345, выдан 20 февраля 2020 г., действителен до 20 февраля 2025 г.);

- аппаратно-программным модулем доверенной загрузки АПМДЗ-И/Э КБДЖ.468243.173 (сертификат соответствия № СФ/527-3729, выдан 16 августа 2019 г., действителен до 31 октября 2022 г.);

- САВЗ от АО «Лаборатория Касперского» с сертификатом в Системе сертификации средств защиты информации по требованиям безопасности информации для сведений, составляющих государственную тайну (СЗИ-ГТ) ФСБ России РОСС RU.0003.01БИ00.

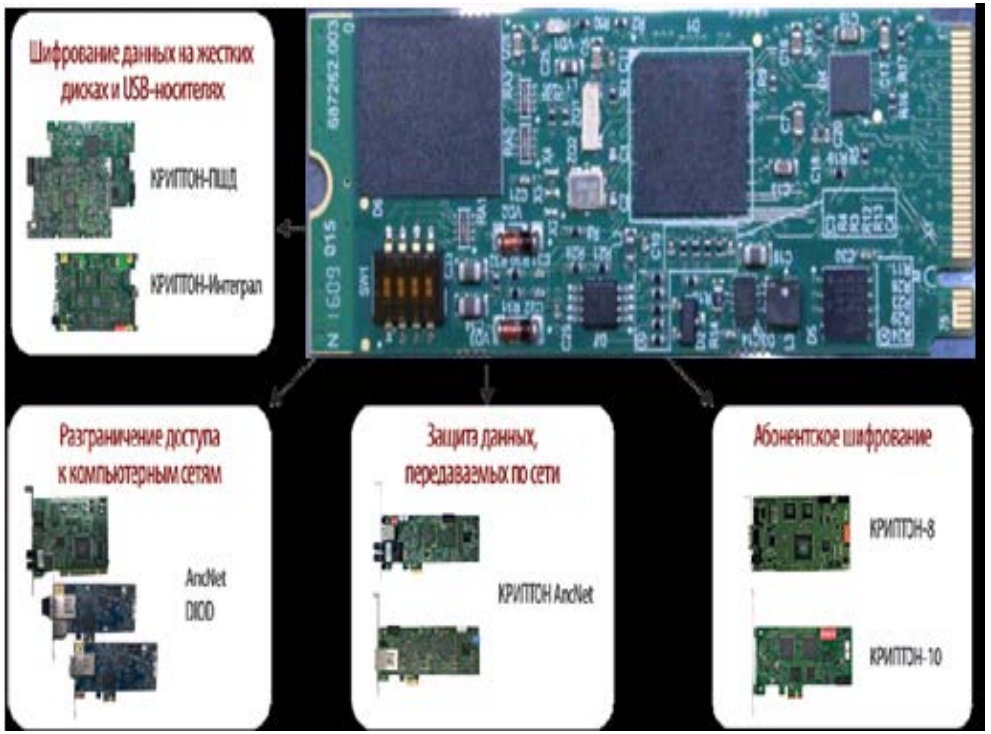
Уровни конфиденциальности (применение СКЗИ)



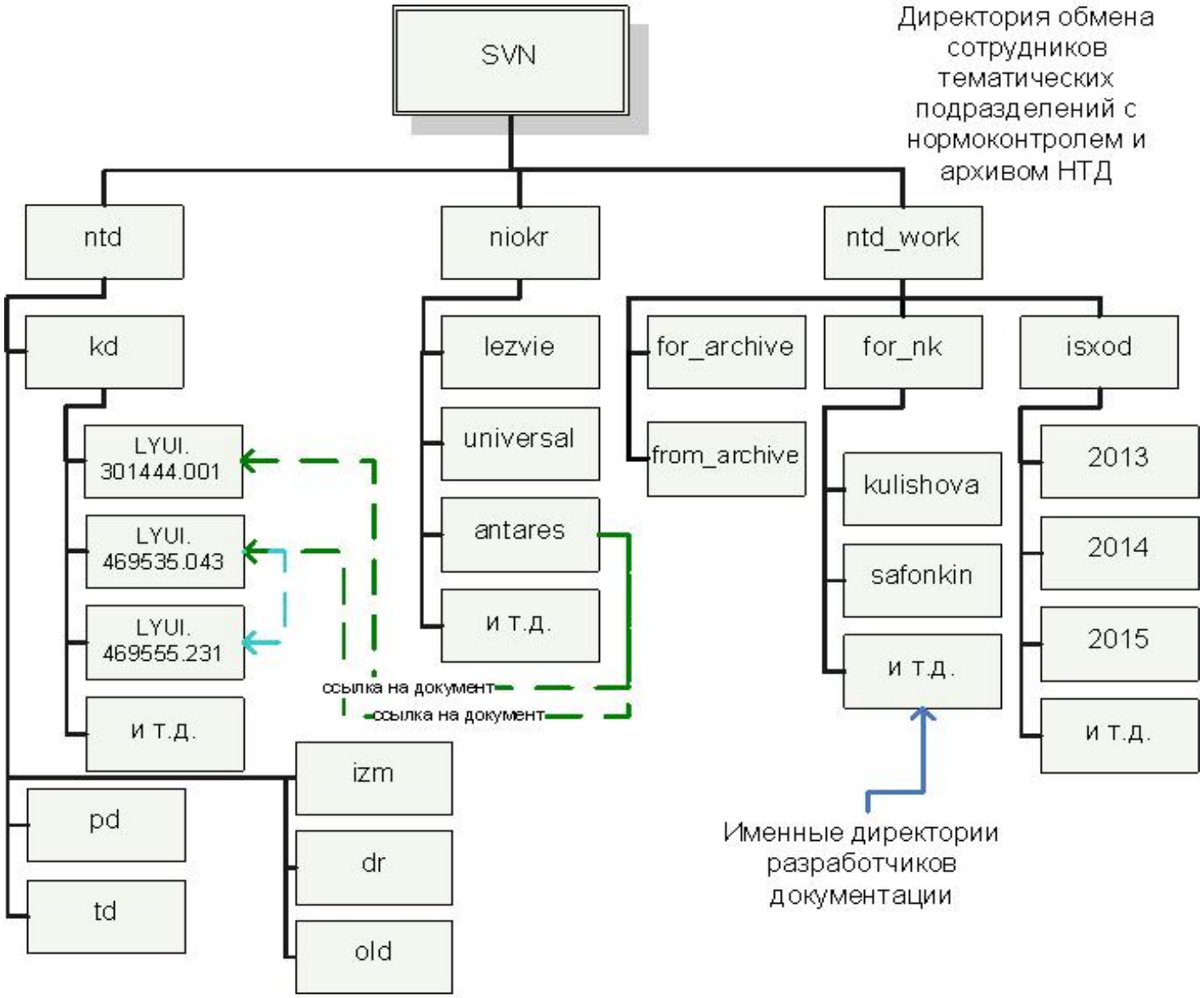
АПМДЗ или СДЗ (например класс 1Б, требования ФСБ России)

Для каждого АПМДЗ обеспечена совместная работа с шифраторами. Имеется поддержка проходного шифратор диска и сетевого шифратора.

Помимо АПМДЗ (СЗД) процессорные модули (материнские платы) поддерживают дополнительные решения для удаленного управления сервером МУС-А (IPMI 1.5)



Уровни целостности и конфиденциальности на примере



Спасибо
за внимание!