МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Національний авіаційний університет
Навчально-науковий інститут
комп'ютерних інформаційних технологій

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
IX МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2016)

21–23 квітня 2016 року

Київ 2016

УДК 004.7(043.2)

Збірник тез доповідей IX Міжнародної науково-технічної конференції «Комп'ютерні системи і мережні технології» (CSNT-2016), м. Київ, 21–23 квітня 2016 р., Національний авіаційний університет. – К.: НАУ, 2016. – 82 с.

Рецензенти:

С. Д. Винничук – д.т.н., с.н.с., провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України;

В. Є. Мухін – д.т.н., доцент кафедри обчислювальної техніки Національного технічного університету «КПІ»;

Г.С.Прокудін – д.т.н., професор, завідувач кафедри міжнародних перевезень та митного контролю Національного транспортного університету.

Збірник тез доповідей укладено за матеріалами IX міжнародної науково-технічної конференції «Комп'ютерні системи і мережні технології» (CSNT-2016). У доповідях розглянуті наукові, технічні та технологічні проблеми побудови, проектування сучасних комп'ютерних систем, засоби і методи моделюваня комп'ютерних мереж, проблеми захисту ресурсів в інформаційних систмах, технології підготовки авіаційних фахівців.

Рекомендовано до друку вченою радою Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету (протокол № 3 від 18 квітня 2016 р.).

IX Міжнародна наукова конференція
«Комп'ютерні системи та мережні технології»
присвячена **100-річчю** з дня народження
академіка Національної академії наук України
Пухова Георгія Євгеновича

Пухов Георгій Євгенович відомий вчений в галузі теоретичної електротехніки, енергетики, математичного моделювання та обчислювальної техніки. Пухов Г.Є. розробив теоретичні основи діакоптичних методів в електротехніці та моделюванні, розвинув теорію операційних методів аналізу і синтезу нелінійних систем, сформулював принцип квазіаналогій і розробив теорію квазіаналогового моделювання. Він був одним із творців сучасної електротехніки і визнаним главою наукової школи електронного моделювання.

Автор понад 600 наукових праць, 33 монографій, 152 авторських свідоцтв та патентів.

У 1957-1986 р.р. Пухов Г.Є. працював у Київському інституті інженерів цивільної авіації (Національний авіаційний університет, із 2001 р.).

У 1963 р. було створено кафедру обчислювальної техніки на електротехнічному факультеті інституту. Завідувачем кафедри був призначений Пухов Г.Є. У цей час він БУВ керівником групи аспірантів (серед яких були Бабич М.П., Пяткін Г.С., Купреєв В.І. та ін.), консультував двох докторантів (Ільницкого Л.Л. і Нагорного Л.Я.), проводив значну роботу щодо організації підготовки фахівців з обчислювальної техніки для цивільної авіації. Пухов Г.Є. був ініціатором і активним учасником створення факультету автоматики та обчислювальної техніки (1965 р.) для підготовки інженерів-системотехніків за фахом "Лічильно-вирішуючі і обчислювальні пристрої". Для навчання студентів на кафедрі обчислювальної техніки створюються навчальні лабораторії: цифрової обчислювальної техніки; обчислювальних машин безупинної дії та спеціалізованих пристроїв.

Учнями наукової школи академіка Пухова Г.Є. у Національному авіаційному університеті по праву вважали і вважають себе співробітники:

– чл.-кор. НАН України, д.т.н., професор Васильєв В.В.;

– заслужені діячі науки і техніки України, доктора технічних наук, заслужені професори НАУ Ільницький Л.Я. та Нагорний Л.Я.;

– кандитати технічних наук, професори Бабич М.П., Купреєв В.І.;

– кандидати технічних наук Гузенко А.І., Єфімов А.А., Левін А.Г., Прозоров С.Є., П'яткін Г.С., Самусь В.М., Тимошенко М.П.;

– колишні студенти кафедри обчислювальної техніки: доктора технічних наук, професори Білецький В.М., Жуков І.А., Корченко О.Г., Мохор В.В. , Плющ Ю.А., Стасюк О.І.; кандидати технічних наук Бабич О.Б., Величко С.М., Кизим Ю.Т.

ЗМІСТ

УДК 519.218.82(043.2)

В. І. Андрєєв, к.т.н.,
О. В. Андреєв, к.т.н.
Національний авіаційний університет, Київ

МЕТОД ДВОПАРАМЕТРИЧНОЇ ОПТИМАЛЬНОЇ ЕКСТРАПОЛЯЦІЇ ВИПАДКОВИХ НЕСТАЦІОНАРНИХ СИГНАЛІВ НА ТЛІ ЗАВАД, ЗАСНОВАНИЙ НА ВИКОРИСТАННІ ФУНКЦІЇ ЛАГРАНЖА

Комп'ютерні мережі отримали в наш час широке застосування в різних галузях людської діяльності. Вирішення задач прогнозування, або екстраполяції характеристик трафіку комп'ютерних мереж займають важливе місце в управлінні комп'ютерних мереж та забезпеченні їх працездатності та ефективності роботи.

Вирішення задач екстраполяції випадкових процесів, до яких відноситься і трафік комп'ютерних мереж, займають важливе місце як в теорії випадкових процесів, так і в практичному використанню цієї теорії в рішеннях практичних задач надійності, діагностиці, контролю якості, обробці сигналів на тлі завад та інших задач в різних галузях науки та техніки. На сьогоднішній день найбільш повно вивчені задачі екстраполяції випадкових стаціонарних процесів без завад, також існують практичні результати екстраполяції цих процесів на тлі стаціонарних завад.

Недостатньо вивченими залишаються задачі екстраполяції випадкових нестаціонарних сигналів (ВНС) на тлі стаціонарних та нестаціонарних завад. В той же час саме ці задачі найбільш актуальні в різноманітних галузях науки та техніки, таких як контроль працездатності комп'ютерних мереж, обробка звукових сигналів на тлі завад, та багатьох інших. Для вирішення цієї задачі було запропоновано методи оптимальної екстраполяції ВНС на тлі завад із застосуванням методів однопараметричної та двопараметричної оптимальної екстраполяції. Як подальший розвиток попередніх методів запропоновано метод оптимальної екстраполяції на базі функцій Лагранжа. За допомогою методу статистичного імітаційного моделювання (СІМ) розроблено методику дослідження та оптимальної екстраполяції характеристик ВНС на тлі завад. За допомогою експерименту показана ефективність розробленого методу.

Ми маємо два спостереження ($n=2$), в результаті спостереження отримують значення Y_1 , Y_2 замість істинних значень X_1 , X_2 , по яким необхідно визначити за допомогою функції Лагранжа X_3, але насправді оптимально спрогнозувати значення Y^*_3.

Сигнал, що спостерігається, розглядається як «адитивна суміш» сигналу $Y(t)$ і завади $\xi(t)$:

$$Y(t) = X(t) + \xi(t) .$$

Задача екстраполяції полягає в тому, щоб у найкращий спосіб по значенням Y_1, Y_2, що екстраполюються, отримати оцінку Y^*_3 майбутнього значення Y_3. З постановки задачі зрозуміло, що найкраща екстраполяція включає не тільки прогнозування Y_3 , а й зменшення похибки спостережень ε : $\varepsilon = Y_3 - Y_3^*$.

В основу методу, що пропонується, поставлено задачу визначення оптимального вагового коефіцієнта α_{opt} за критерієм мінімуму дисперсії $minD_\varepsilon(\alpha_{opt})$ похибки оптимального прогнозного (екстрапольованого) значення випадкового нестаціонарного сигналу на тлі завад. Для виконання екстраполяції, необхідно мати набір апріорної ймовірностної інформаці про ВНС. Це наступний набір для точок спостереження Y_1, Y_2: математичті сподівання - m_{Y1}, m_{Y2}; дисперсії - D_{Y1}, D_{Y2} (або їх середньоквадратичні відхилення $\sigma_{Y1}{}^2$, $\sigma_{Y2}{}^2$); кореляційна функція - $K_Y(t_1, t_2)$. Крім того, треба визначити інтервали спостереження ΔT та екстраполяції τ , а також величину потужності завади σ^2_ξ Далі треба довизначити відсутні параметри для точки ВНС, яку збираємось екстраполювати: m_{Y3}, D_{Y3}, σ^2_{Y3}, $K_Y(t_1, t_3)$, $K_Y(t_2, t_3)$.

Оцінку Y_3^* істинного значення X_3 в момент часу t_3 розглядаємо як лінійну комбінацію (функцію) попередніх значень, що спостерігаються :

$$Y_3^* = \alpha_1 Y_1 + \alpha_2 Y_2 \cdot$$

Вважаємо, що параметри α_1 , α_2 задовольняють вимозі нормування

$$\alpha_1 + \alpha_2 = 1 \cdot$$

Тоді $\alpha_1 = \alpha$, $\alpha_2 = 1 - \alpha$, а оцінка

$$Y_3^* = Y_2 + \alpha (Y_1 - Y_2) \cdot$$

Оцінка Y_3^* по формулі має наглядне фізичне пояснення: Y_2 – опорне значення, $\alpha(Y_1 - Y_2)$ – «добавка», яка є добутком різниці $\Delta Y_{12} = Y_1 - Y_2$ значень сигналу на інтервалі спостереження та параметру екстраполяції α .

Ставити задачу оптимізації оцінки значення $Y(t)$ в наступний момент часу t_{n+1} шляхом оптимального вибору параметру оптимізації α по відповідному критерію оптимізації.

Цільовою функцією оптимізації візьмемо функцію Лагранжа:

$$L(\vec{\alpha}, \lambda) = [A_0 + A_1 t_3^\gamma + \xi(t_3) - Y_3^*(\vec{\alpha})]^2 + \lambda[\sum_{k=0}^{1} \alpha_k - 1] ,$$

де $L(\vec{\alpha}, \lambda)$ – функція Лагранжа;

λ – невизначений множник Лагранжа;

$\vec{\alpha}$ – α_1, α_2 – вектор параметрів оптимізації;

$A_0 = \alpha_0$, $A_1 = \alpha_1$ являють собою випадкові незалежні величини, що мають Гаусовські розподіли з математичними сподіваннями і дисперсіями, що визначені:

$$Y_3^*(\vec{\alpha}) = \alpha_1[A_0 + A_1 t_1^\gamma + \xi(t_1)] + \alpha_2[A_0 + A_1 t_2^\gamma + \xi(t_2)] =$$

$$= (\alpha_1 + \alpha_2) A_0 + (\alpha_1 t_1^\gamma + \alpha_2 t_2^\gamma) A_1 + \alpha_1 \xi(t_1) + \alpha_2 \xi(t_2) .$$

Аналіз результатів експерименту показує працездатність і ефективність запропонованого методу екстраполяції навіть при низькому відношенню середньоквадратичних значень сигнал / шум.

Результати експерименту наглядно ілюструють новизну, корисність та ефективність методу оптимальної екстраполяції випадкового нестаціонарного процесу на тлі завад за допомогою функції Лагранжа. Крім того, запропонований метод має зручну для практичного використання форму.

УДК 531.5 (043.2)

В. К. Антонов, д.т.н.
Национальный авиационный университет, Киев

ГРАВИТАЦИОННАЯ АНИЗОТРОПИЯ РАДИОАКТИВНОГО РАСПАДА

Рабочей гипотезой является предположение о существовании различия в разлете элементарных частиц, образующихся при радиоактивном распаде химических элементов, или их столкновениях - в зависимости от направления действия гравитационного поля, что его действие имеет место непосредственно в акте распада, т.е. «внутри его механизма», или механизма столкновения. Таким образом, речь идет о предположительно слабой, но связи Стандартной модели элементарных частиц и гравитации.

Рассмотрим предельные проявления анизотропии физических процессов. Предельно сильно в природе анизотропия проявляется в излучении релятивистских джетов квазарами. Внутри вращающейся коллапсирующей массы (черной дыры) внутренние слои вещества по мере приближения к оси вращения движутся с нарастающей окружной скоростью, это приводит к увеличению их трения, и в итоге разрушению самого вещества до уровня жесткого рентгеновского излучения, образующего джеты. Направление их излучения вдоль оси вращения обусловливается ослаблением гравитации в этом направлении, что связано с нарушением принципа равного распределения энергии по степеням свободы внутри вращающейся черной дыры - вращательная степень свободы является наиболее энергоконцентрирующей. Увеличивающийся при приближении по радиусу к оси вращения градиент плотности вещества приводит к увеличению метрики, - и уменьшению градиента, некоторому (не решающему) ослаблению коллапса, что согласуется с принципом Ле Шателье. Поэтому внутренний наблюдатель видит дыру большей, чем наружный. В итоге разрушение (распад) квазара обусловлено гравитацией и внутренним движением. Косвенными подтверждающими признаками являются пульсации интенсивностей джетов в силу колебательной динамики системы «сжатие – вращение – трение - излучение», и хорошее совпадение периода жесткого γ - излучения с отношением диаметра нуклона к скорости света. Квазар является наиболее мощным естественным коллайдером, разрушающим материю до уровня излучения, и реализующим циклический с большим периодом круговорот материи (круговороты, локальные в сравнении с размерами Вселенной) в природе, самоорганизующейся затем из излучения до высоких уровней, и снова образующей квазары. Предельно слабой можно ожидать анизотропию радиоактивного распада по отношению к направлению действия гравитации. Ожидается, что это наиболее слабый физический эффект (за исключением, возможно, гравитационной анизотропии вакуумных флуктуаций для сдвига Лэмба и силы Казимира). Поэтому интересно его измерение. Эксперимент построим следующим образом (рис.1). В первом случае (а)) источник радиации ***И*** расположим выше ее приемника ***П*** относительно поверхности Земли. Во втором случае (б)) источник находится ниже приемника. В обоих случаях анализатор ***А*** принимает сигнал приемника, представляющий последовательность случайных импульсов. Задача состоит в обнаружении малого

смещения функций плотности распределения временных промежутков между импульсами для двух случаев. В случае а) ожидаем более высокой средней частоты импульсов. Тогда математическое ожидание межимпульсного времени Δt должно меньше, чем в случае б). Взаимный вид плотностей распределения

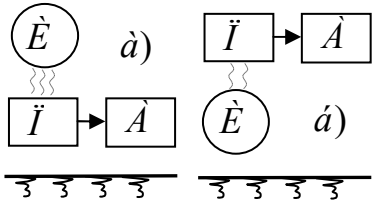

Рис. 1. Схема эксперимента

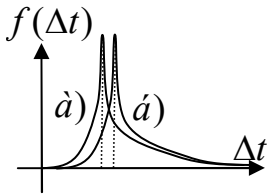

Рис. 2. Плотности распределения

приведен на рис. 2. Следовательно, период генератора межимпульсного времени анализатора ***A*** должен быть на несколько порядков меньше предполагаемого смещения.

Стандартная схема численного построения функции плотности распределения предполагает предварительное разбиение оси аргумента рис. 2 на малые отрезки, далее анализа принадлежности случайного числа конкретному отрезку, прибавления единицы в ячейку массива с номером отрезка, и нормировку по окончании анализа. В нашем случае предстоит иметь дело практически с двумя белыми шумами, максимумы плотностей распределения которых «очень плохо определены». Поэтому дополним процедуру вычислений дополнительными приемами. Сожмем полученную на первом этапе функцию плотности распределения вдоль оси Δt. Аппроксимируем результат квадратичной функцией. Построим функцию, обратную полученной, или просто поменяем знак квадратичного члена аппроксимации – получим функцию с положительной второй производной. Затем применим многократное логарифмическое преобразование по правилу $f_{k+1}(\Delta t) = A\ln(1 + f_k(\Delta t))$; $k = 0,1,.....,$ A – масштабный коэффициент На каждом его шаге сравниваем функции согласно опытам а) и б) , и анализируем искомое смещение.

Еще одна возможная процедура счета состоит во введении смещения, и его адаптивной настройке на максимум коррелируемости двух функций.

Интрига данной «затеи» состоит в том, что отрицательный результат невозможно трактовать как ставящий в этом направлении точку, – всегда остается перспектива повышения точности эксперимента.

Интересно сравнение результатов экспериментов, проведенных на Земле и на Луне – ожидается ослабление смещения на Луне как менее массивной планете. Гравитацию можно попытаться заменить инерционными силами, проводя эксперименты на центрифуге – ожидается отличие действия инерции и гравитации вопреки принципу эквивалентности А. Эйнштейна.

Возможен статистический анализ массивов данных Большого адронного коллайдера и других ускорителей с целью поиска предполагаемого эффекта.

Практическим приложением («внедрением результатов») может быть разработка «гравитационных горизонтов» – датчиков положения в гравитационном поле – для задач управления подвижными объектами.

УДК 004.056.53 (043.2)

С. В. Балакин, аспірант
Национальный авиационный университет, Киев

СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ АТАК В КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ СИГНАТУРНЫХ МЕТОДОВ

Задача обнаружения атак требует повышения эффективности методов обнаружения вторжений. Процесс автоматизации может вводиться на разных стадиях идентификации: на стадии предотвращения или обнаружения[1]. Средства повышения достоверности идентификации атак представляют собой новые технологии, которые имеют потенциал развития.

Представлены подробности подхода обнаружения отклонений для выявления вторжений в компьютерной сети. Модель обучения состоит из массивов данных с распределенной средой и сигнатурными выборками, что повышает производительность системы при обнаружении вторжений[2]. Данный подход также был испытан с использованием наборов данных KDD. Подходы машинного обучения обнаружения вторжений в компьютерной сети имеют хорошие перспективы в развитии, так как в дальнейшем имеется возможность полной автоматизации обнаружения вторжений в сетях (возможно даже полное или частичное исключение человеческого фактора).

Предложен метод обнаружения атак в компьютерной сети, а также разработана модель работы данной системы в режиме предотвращения и обнаружения.

Представлен анализ результатов обнаружения компьютерных атак с помощью сигнатурных методов отклонений (отклоняющихся значений). Определены погрешности в расчетах отклонений процессов и внесены корректировки, которые значительно повышают показатели производительности полученные ранее. Разработана модель обнаружения атак на основе информации о поведении отклоняющихся значений в сети и их виявлении.

Предложенный метод может использоваться для обнаружения вторжений в компьютерной сети. Выделены основные направления развития систем обнаружений вторжений[3].

Концепция машинного обучения обнаружения вторжений в компьютерной сети имеет хорошие перспективы в развитии, так как в дальнейшем имеется возможность полной автоматизации обнаружения вторжений в сетях (возможно даже полное или частичное исключение человеческого фактора). В дальнейшем открывается перспектива использования данного метода для моделей обучения выборок или тестирования данных.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Гамаюнов, Д. Ю. Модель поведения сетевых объектов в распределенных вычислительных системах / Д.Ю. Гамаюнов, Р.Л. Смелянский // Программирование. — 2007. — № 4. — С. 20–31.

2. Cramer H. Mathematical Methods of Statistics. —. Prinseton University Press, 1962. — 590 p.

УДК 004.492.3

Є. І. Безвершенко
Ужгородський національний університет,Ужгород,
М. М. Гузій, к.т.н.,
М. М. Проценко, к.т.н.
Національний авіаційний університет, Київ

МЕТОДИ ЗАХИСТУ КОМПЬЮТЕРНИХ МЕРЕЖ ВІД РОЗПОДІЛЕНИХ АТАК

Інтенсифікація процесів інформаційної взаємодії, розвиток територіально розподілених систем, широке використання Інтернет висуває нові вимоги до функціонування розподілених інформаційних систем (РІС), розвитку безпечних технологій роботи з інформаційними ресурсами, впровадження методів і засобів захисту інформації в РІС. Розподілена інформаційна система являє собою сукупність взаємопов'язаних програмних і апаратних ресурсів. Зростання кількості цілеспрямованих атак на корпоративні інфраструктури вимагає розробки методів і технологій інформаційного захисту.

Атаки на різні об'єкти РІС можна класифікувати наступним чином: атаки на мережеві ресурси; атаки на файлові ресурси; атаки на програмні ресурси; атаки на ресурси баз даних; атаки на обчислювальні ресурси. Найбільш небезпечними є атаки, спрямовані на відмову в обслуговуванні, в результаті яких інформаційні ресурси стають недоступними. До даного класу атак належать: DoS (відмова в обслуговуванні) - зменшення пропускної здатності каналу зв'язку; DDoS (розподілена відмова в обслуговуванні) - розподілена атака; DRDoS (Distributed Reflection DoS) - розподілена віддзеркалена атака, яка спрямована на зменшення пропускної здатності мережі.

Інформативні ознаки для виявлення атаки можуть бути розділені наступним чином [1]:

- ознаки, що виділяються з заголовка мережевого пакету;
- ознаки, що виділяються з інформаційної частини пакету на підставі експертних оцінок або інформації про стан контрольованого вузла;
- ознаки, значення яких обчислюються як статистика за минулі дві секунди мережевої активності, для TCP-протоколу;
- ознаки, значення яких обчислюються як статистика за 100 останніх з'єднань;
- ознаки, що виділяються на основі аналізу HTTP-запитів;
- ознаки, значення яких обчислюються як статистика за минулі дві секунди мережевої активності, для SNMP-протоколу.

Загальна архітектура системи виявлення атак запропонована в [2] включає: мережеві сенсори, які здійснюють збір мережевих пакетів і перетворюють отриману інформацію в набір ознак; модулі аналізу, що виконують статистичний аналіз мережевого пакету на предмет наявності ознак відомих типів; модуль реакції, що виробляє реакцію на певний тип атаки; модуль управління компонентами, що здійснює взаємодію інших модулів; модуль зберігання, що забезпечує зберігання в базі даних (БД) ознак мережевих пакетів; графічний інтерфейс.

Еволюція розподілених обчислювальних систем забезпечила розвиток хмарних обчислювальних середовищ, використання яких призвело до появи нових проблем, пов'язаних з уразливістю хмарних технологій [3].

Активні роботи в галузі захисту систем хмарних обчислень ведуться такими провыдними компаніями як Intel, IBM, HP, Sun, Cisco і Symantec.

Компанія Intel для організації хмарних серверів пропонує рішення під назвою Cloud-в-Box. Методологія забезпечення безпечної циркуляції інформації між корпоративною мережею та хмарою, включає наступні компоненти:

Web Security - забезпечує двосторонній захист HTTP- трафіку;

Mobile Security - забезпечує захист мобільних пристроїв шляхом захисту від шкідливих програм та фільтрації веб-трафіку;

Email Security - забезпечує захист пошти, інтегрується з системою захисту від витоку інформації для вихідного трафіку.

Компанія Symantec розробила програмний комплекс Symantec Endpoint Protection 12, орієнтований на виявлення і блокування загроз.

Компанія Cisco пропонує технології забезпечення хмарної мережевої безпеки Cisco ScanSafe Web Intelligence Reporting і продукт Cisco IPS Sensor для систем запобігання вторгнень в комп'ютерні мережі.

Компанія IBM представила апаратно-програмний комплекс IBM Network Intrusion Protection System GX7800.

Компанія HP представила сімейство рішень HP CloudSystem для розгортання хмарних сервісів всіх типів в складі приватних, публічних і гібридних хмар. Платформа HP CloudSystem підтримує численні механізми захисту, включаючи ідентифікацію та аутентифікацію, управління доступом, авторизацію і аудит, а також використання безпечних протоколів зв'язку.

Перспективні напрями розвитку систем захисту хмарних технологій :

– створення засобів виявлення і запобігання розподілених мережевих атак на інформаційні ресурси, засоби динамічного захисту та ідентифікації атак, підвищення автоматізації;

– розробка систем безпеки хмарних середовищ: хмарні брандмауери, засоби обмеження ресурсів і валідації додатків, побудова віртуальних каналів міжмережевої взаємодії, системи агентів спостереження і хмарні антивіруси;

– розробка архітектур серверів безпеки, систем ефективної обробки запитів і виявлення атак, системи управління доступом; технології, пристрої та засоби для безпечного використання мережевих ресурсів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. А. А. Кондратьев Распределённая система обнаружения и предотвращения сетевых атак на системы облачных вычислений Вестник РУДН. Серия Математика. Информатика. Физика. № 1. 2014. С. 99–105

2. Талалаев А. А., Тищенко И. П., Фраленко В. П., Хачумов В. М. Эксперименты по нейросетевому мониторингу и распознаванию сетевых атак // Информационное противодействие угрозам терроризма, № 15, 2010, с. 81-86.

3. Ю. Г. Емельянова, В. П. Фраленко. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления, Программные системы: теория и приложения, 2011, том 2, вып. 4, 17-31

УДК 167:004.7(043.2)

В.М. Боровик, к.т.н.
Національний авіаційний університет,Київ

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ ЯК СИСТЕМ МАСОВОГО ОБСЛУОВУВАННЯ ІЗ ПРИОРИТЕТАМИ

У цій роботі дається розширений підхід побудови моделі прийняття рішення при обробці запитів клієнтів на сервері, як системи масового обслуговування (СМО). При цьому виконується головне правило Кодда, при якому при розподілі бази даних дозволяється розширення засобів СУБД при логічній незалежності програм користувача від бази даних.

Далі ми будемо розрізняти типи запитів та інтенсивність поступу запитів і-го типу. Таким чином на сервер поступають n пуассонівських вхідних потоків різнотипних запитів.

Усі запити, які поступають на сервер, можуть бути виконані на сервері, при чому час виконання буде випадковим значенням із відповідною щільністю ймовірності. Випадковий характер вказаних показників використовується при аналізі завантаження системи. Для баз даних виконання процедури обробки запитів залежить від об'єму інформації та складності алгоритму обробки, які задіяні у кожному випадку, тому одна і таж процедура може виконуватися різний час. Крім того, пуассонівський розподіл часу доступу і обробки запитів дає критичні по завантаженню параметри системи, що гарантує успішну роботу системи у реальному часі. Запити на обробку від клієнта до серверу поступають тільки у вигляді команд ініціалізації процедур, які разом з даними знаходяться на сервері. Якщо сервер вільний(може прийняти наш запит), запит приймається на виконання. В протилежному випадку ні, то він чекає на виконання свого часу у черзі.

Розглядається ситуація управління запитами, які очікують своєї обробки. Фізична інтерпретація черги має інформаційний характер і може пояснюватися по-різному. У нашому випадку деталі цього механізму не мають принципового значення. Як зазначалося на початку, протоколи обробки запитів постійно ускладнюються, а загальна тенденція – пошук оптимальних методів контролю роботи системи з урахуванням усіх можливих критеріїв. Наша задача - дати приклад рішення вибору запиту для обробки на сервері при альтернативних ситуаціях вибору.

У подальшому використовується апарат марковських процесів, який дозволяє у стаціонарних режимах роботи розробляти ясні у інтерпретації детерміновані алгоритми керування такими системами. Відомо, що випадковий процес є марковським, якщо для усіх фазових траєкторій ймовірність попадання системи у деякий наступний стан залежить тільки від того, в якому стані вона знаходиться у даний час і не залежить від попередньої історії. Будемо розглядати систему у моменти розмноження при попаданні у чергу пуассонівських вхідних потоків , маючих властивість відсутності післядії. На етапах "загибелі" (сидіння чи перескоків), тобто етапів їх обслуговування, час якого розподілений по експоненціальному закону, одержуємо ланцюг, маючий марковську властивість.

У нашій моделі сервер інтерпретується як “прибор”, запит - як “заява”, виконання процедури (запиту) – обслуговування процедури, назва процедури – тип заяви, час виконання процедури – час виконання заяви.

Пояснимо динаміку переходів вказаної схеми та рівнянь, визначивши альтернативні та неальтернативні ситуації, що відповідають умовним та безумовним інтенсивностям переходів.

При неальтернативних ситуаціях на етапах “розмноження” поступають пуассонівські вхідні потоки заяв, при тому виконуються обмеження на число місць у черзі. У момент закінчення обслуговування неальтернативна ситуація відповідає існуванню у черзі заяв тільки одного типу. Для цієї ситуації, яка відноситься до тривіального випадку моделей “розмноження та загибелі”, стан системи являє собою лінійний ланцюг. Закон вибору заяв на обслуговування у цьому випадку може бути вільним, що не змінює розподіл стаціонарних ймовірностей станів системи. Для визначеності будемо задавати, що для черги з заявами одного типу буде виконуватися дисципліна обслуговування FCFS – “перший прийшов - перший обслугований ”

При наданні інформації “прибор вільний” може з’явитися ситуація, коли у черзі знаходяться заяви більше одного типу. Для вирішення таких конфліктних ситуацій використовується пріоритетний параметр, який визначає можливість вибору заяви s- го типу для обслуговування на приборі. Звичайно, що якась заява обов’язково буде вибрана.

Розібравши механізм зміни стану системи, ми показали можливі переходи із одного стану у інший без урахування оцінки ефективності їх функціонування по тому чи іншому алгоритму. Для визначення оптимальності функціонування треба ввести критерії ефективності.

У якості критерію виберемо мінімізацію часу перебування заяв у черзі (втрата від чекання). Для визначення цього критерію введемо показник витрат із-за перебування l-ї заяви s-го типу.

Для вирішення цієї проблеми використовується стандартний прийом заміни існуючих нелінійний складові, що дозволить у подальшому використати методи лінійного програмування. Введення вказаних додаткових змінних потребує й нових обмежень з урахуванням конкретної моделі.

Головним математичним об’єктом досліджень даної роботи є СМО з кінцевим числом можливих станів у стаціонарному режимі. Процес керування такими системами розглядається, як пошук керуючих параметрів безупинного марковського ланцюга.

Із теорії кінцевих ланцюгів Маркова відомо, що усі стаціонарні ймовірності станів $\pi(\cdot)>0$, тобто більше нуля. Оптимальне значення керуючих елементів - $\delta(\cdot)$ можуть бути рівні тільки 0 чи 1. Таким чином , оптимізаційна задача зводиться до пошуку екстремуму функції.

Розглянута методологія може бути використана для побудови пріоритетного управління запитами у системах клієнт-сервер. Результати розрахунків представляються у вигляді таблиці чи бази даних ситуаційних пріоритетів, які попередньо розраховуються по параметрам системи.

УДК 004.056.53:004.492.3 (043.2)

С. В. Водоп'янов, аспірант,
В. І. Дрововозов, к.т.н.,
Н. В. Журавель
Національний авіаційний університет, Київ

ЗВ'ЯЗОК ПАРАМЕТРІВ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ АЕРОВУЗЛІВ ТА ЕФЕКТИВНОСТІ АВІАЦІЙНИХ КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Проблема стійкості функціонування авіаційних бортових мереж в зоні аеровузла стоїть особливо гостро в зв'язку з необхідністю безумовного забезпечення безпеки польотів, виключення льотних пригод і передумов до них. Ця проблема посилюється через безперервні зміни структури мережі - одні літаки як мережні елементи входять в зону відповідальності аеровузла, інші виходять. Цей процес є суттєво нестаціонарним. Для забезпечення безпеки мережі при наявності зовнішніх і внутрішніх заважаючих впливів необхідно не просто підвищувати енергетичні та інформаційні ресурси, а застосовувати оптимальні методи управління реконфігурацією мережі. В роботі запропоновані математичні моделі марковських процесів загибелі і розмноження з нестаціонарними імовірностями переходу, якими описується поточний стан локальної авіаційної бортової мережі аеровузли. Виїдена система рівнянь Колмогорова - Чепмена для нестаціонарних ймовірностей стану мережі. Застосовано метод гаусовської апроксимації розподілу координат системи в просторі станів.

Як показано в роботах [1-3], задача інтегрування пропускної спроможності аеропортів і аеровузлів і ефективності систем організації повітряного руху (ОрПР) має міждисциплінарний характер і повинна реалізовуватися на базі концепції інтегрованої модульної авіоніки (ІМА). В основі концепції ІМА лежить відкрита мережна архітектура і єдина обчислювальна платформа. Звідси можна зробити однозначний і цілком очікуваний висновок, що завдання оптимізації ОрПР базується в т.ч. і на оптимізації інформаційно-керуючих систем (ІКС) аеропортів і аеровузлів. Для побудови математичних моделей і методів кількісного обґрунтування взаємозв'язку завдань ОрПР та ІКС аеровузли пропонується використовувати систему так званих ключових показників ефективності [4] (*Key Performance Indicators - KPIs*). В опублікованих роботах автора розроблена модифікована модель цілочисельного комбінаторного програмування, яка застосовується для маршруту польоту, яка відноситься до класу стандартних завдань розміщення з обмеженнями. Модифікація полягає у введенні додаткового адитивного компонента цільової функції (ЦФ) - комбінації поточних вартостей затримки в польоті (*airborne-holding delay*) і затримки на землі (*ground-holding delay*). Тут під вартістю ми маємо на увазі не тільки фінансові витрати, але і в більш широкому сенсі - іміджеві втрати авіакомпаній, зниження довіри пасажирів і ін., і в першу чергу - зниження рівня БП (збільшення ризиків авіаційних подій). Крім того, відібрані деякі ключові показники, які безпосередньо пов'язані з якістю роботи інформаційно-обчислювальної мережі як невід'ємного елементу системи ОрПР. Розглядається система КПЕ для мережі аеровузли як великої системи з

затримками сигнальної і керуючої інформації. На рис. 1 схематично зображено схему взаємозв'язку і взаємодії сегментів складеної мережі аеровузла і зовнішніх інформаційних мереж.

Рис. 1. Умовна схема взаємозв'язку і взаємодії сегментів складовою мережі аеровузли і зовнішніх інформаційних мереж

Проблема стійкості функціонування авіаційних бортових мереж в зоні аеровузла стоїть особливо гостро в зв'язку з необхідністю безумовного забезпечення безпеки польотів, виключення льотних пригод і передумов до них [5]. Ця проблема посилюється через безперервні зміни структури мережі - одні літаки як мережні елементи входять в зону відповідальності аеровузла, інші виходять. Цей процес є суттєво нестаціонарним. Для забезпечення безпеки мережі при наявності зовнішніх і внутрішніх заважаючих впливів необхідно не просто підвищувати енергетичні та інформаційні ресурси, а застосовувати оптимальні методи управління реконфігурацією мережі. В роботі запропоновані математичні моделі марковських процесів загибелі і розмноження з нестаціонарними імовірностями переходу, якими описується поточний стан локальної авіаційної бортової мережі аеровузли. Виїдена система рівнянь Колмогорова - Чепмена для нестаціонарних ймовірностей стану мережі. Застосовано метод гаусовської апроксимації розподілу координат системи в просторі станів.

ВИКОРИСТАНІ ДЖЕРЕЛА

*1.*2013–2028 Global Air Navigation Capacity & Efficiency Plan //Електронний *ресурс. Режим доступу: http://www.icao.int/Meetings/anconf12/Documents/Draft%20Doc%209750.GANP.en.pdf*

2.Книга Е.В. Вычислительные структуры и средства автоматизированного контроля компонентов интегрированной модульной авионики // Электронний ресурс : Режим доступу - www.elektropribor.spb.ru/cnf/kmu2014/text/128.doc

3.Федосов Е., Косянчук В., Сельвесюк Н. Интегрированная модульная авионика // Радиоэлектронные технологии, 2015, 1. - С. 66 - 71.

4.Водопьянов С.В. Ключевые показатели управления качеством сервиса в информационно-управляющей сети аэроузла // Наукові записки УНДІЗ. – 2012. – №3 (23). – С. 71 – 75.

5.Future Aeronautical Communications / Edited by Simon Plass. - Institute of Communications and Navigation, German Aerospace Center (DLR), Germany. – Published by InTech Janeza Trdine 9, 51000 Rijeka, Croatia. – InTech, 2011. – 378 PP.

УДК 004.056.53 (043.2)

Л. П. Галата,
М. С. Мариняк
Національний авіаційний університет, Київ

ОЦІНКА ТА МЕНЕДЖМЕНТ РИЗИКІВ ІНФОРМАЦІЙНО – КОМУНІКАЦІЙНОЇ СИСТЕМИ

Оцінка рівня ризику в наш час є найбільш складним і відповідальним моментом, оскільки саме від її результатів залежать подальші дії підприємства. Інформаційні технології значно розширили можливості бізнесу. Але нові можливості неминуче пов'язані з новими загрозами, які втілившись, можуть призвести до відчутного збитку компанії.

Аналіз інформаційних ризиків є інструментом, що дозволяє визначити: які об’єкти і в якому ступені потребують захисту, вартість засобів захисту, без використання яких система інформаційної безпеки не може бути ефективною. Аналіз інформаційних ризиків найчастіше потребує залучення великої групи експертів, які добре знають ситуацію на підприємстві та розуміють мету досліджень.

Пристрої отримання, обробки, зберігання та передачі інформації на основі сучасних засобів, породили безліч методів і способів несанкціонованого доступу до неї та засобів захисту цієї інформації. Засоби захисту складаються з ряду апаратних, програмних, правових і фізичних заходів по виявленню та нейтралізації впливу на циркулюючу інформацію.

Застосування якісних методів оцінки на сьогоднішній день є єдиним способом отримати уявлення про реальний рівень захищеності інформаційних ресурсів компанії. Програмні засоби, необхідні для повного аналізу ризиків, будуються з використанням структурних методів системного аналізу і проектування. Прикладом такого програмного засобу є КОНДОР (компанія Digital Security). Обов'язковим елементом цього продукту є база даних, яка містить інформацію по інцидентах в області ІБ, що дозволяє оцінити ризики і уразливості, ефективність різних варіантів контрзаходів в певній ситуації.

Програмний продукт КОНДОР дозволяє фахівцям проводити політику інформаційної безпеки компанії на відповідність вимогам ISO 17799. КОНДОР включає в себе більше 200 питань, відповівши на які фахівець отримує детальний звіт про стан існуючої політики безпеки, а також модуль оцінки рівня ризиків відповідності вимогам ISO 17799. У звіті відображаються всі положення політики безпеки, а також існуючий рівень ризику невиконання вимог політики безпеки відповідно до стандарту. Дана система реалізує метод якісної оцінки ризиків за рівневою шкалою ризиків: високий, середній, низький.

Процес мінімізації ризиків слід розглядати комплексно: спочатку виявляються можливі проблеми, а потім визначається, якими способами їх можна вирішити.

УДК 004. (043.2)

В. П. Гамаюн, д.т.н.
Национальный авиационный университет, Киев

СТАНДАРТ ОБРАБОТКИ В СРЕДСТВАХ ЦИФРОВОЙ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

В настоящее время в средствах вычислительной техники применяется стандарт IEEE 754 -2008, включающий стандарт IEEE 754 -1985. Описание стандарта включает разделы по ряду приложений полностью регулирующих применение двоичной арифметики с различными типами представления чисел, в частности с фиксированной и плавающей запятой. Обязательны процедуры преобразования из одного типа представления в другой, определены числовые диапазоны, наличие двух нулей, границы двойной, одинарной точности и многие другие вопросы, исполнение которых необходимо для корректности выполнения обработки в средствах цифровой вычислительной техники.

Известны исследования об ошибках компьютерных вычислений, вызванных применением данных по стандарту IEEE 754 . Точность представления вещественных чисел в формате стандарта, ошибки приведения типа данных, ошибки из-за сдвига мантисс, округление операндов, проблемы для чисел на границах нормализации – неполный перечень вопросов, не разрешаемых при применении стандарта.

С ростом производительности современных ЭВМ расширяется спектр и размерность решаемых на ЭВМ задач, повышаются требования к точности компьютерных вычислений. Большинство компьютерных вычислений проводятся в арифметике с плавающей точкой с жестко ограниченной длиной мантиссы, что приводит к появлению неустранимых ошибок.

Проблема точности компьютерных вычислений особенно остро стоит при решении ряда прикладных задач, таких как, например, жестких задач с разномасштабными коэффициентами в ядерной физике, наноэлектронике, анализе многосвязных мехатронных систем и др.

Один из традиционных способов борьбы с ошибками округления – применение высокоточных вычислений. В настоящее время существует множество библиотек, поддерживающие высокоточные вычисления: ZREAL (Россия), MPARITH (Германия), GMP (США) и др.

Основной проблемой существующих библиотек высокоточных вычислений, сдерживающей их применение на практике, является сильная зависимость роста времени выполнения арифметических операций от точности вычислений. При малом объеме вычислений это не существенно, но для задач большой размерности использование существующих библиотек высокоточных вычислений приводит к резкому росту времени решения задач.

Многие задачи электротехники, энергетики и др. областей науки и техники требуют вычислений с комплексными числами. При вычислениях с комплексными числами также может происходить резкая потеря точности, т.к. комплексная арифметика на ЭВМ реализуется на основе традиционной арифметики с плавающей точкой и проблема сильной зависимости роста времени

выполнения арифметических операций от точности еще в большой степени характерна для вычислений с комплексными числами. Указанная проблема требует поиска новых способов, связанных с применением нетрадиционных систем счисления и арифметик для представления и обработки чисел.

Одним из направлений решения проблемы является применение специальных арифметик. Исследуя возможности применения нового кодирования для реализации мультипликативных операций, а также общие требования к конструктивности кодирования данных (возможности выполнения операций) было предложено оригинальное кодирование данных, которое получило название разрядно-логарифмическое. Разрядно-логарифмическим (РЛ) представлением (кодированием) данных называют изображение двоичного операнда в виде набора двоичных кодов ненулевых разрядов $\{Nx_i\}$ того же операнда, каждый из которых определяется как результат вычисления логарифма от веса этого разряда.

Множество чисел, изображенных в разрядно-логарифмическое коде, имеет следующие свойства:

- разрядно-логарифмическое кодирование (изображение) есть ограниченное подмножество рациональных чисел;
- множество РЛ кодов симметрично относительно числа нуль;
- элементы РЛ распределены равномерно на действительной прямой – важный фактор повышения точности представления данных.

Надо отдельно отметить представление числа нуль при разрядно-логарифмическом кодировании. В структуре РЛ кодов применяется показатель количества значащих разрядов в каждом операнде Q. Если операнд нулевой (т.е. нуль), то такой показатель Q равняется нулю Q = 0 - операнд не имеет значащих разрядов. Такое представление нуля в компьютерной среде является наиболее точным, так как отвечает физическому трактованию нулевого значения, а не математической модели, которая принята в разных ЭВМ.

Числовой диапазон при разрядно-логарифмическом представлении (кодировании) значительно расширяется - диапазон представления чисел увеличивается на несколько порядков в соответствии с размерами разрядной сетки используемого компьютера или компьютерной среды.

Диапазон данных при разрядно-логарифмическом представлении увеличивается многократно на несколько порядков в зависимости от размерности базовой разрядной сетки компьютерной среды.

Как указывалось ранее, разрядно-логарифмическое представление определяет единую форму записи для всех типов числовых данных.

Операционная сложность при обработке разрядно-логарифмических данных отличается от двоичной применением обработки массивов и использованием процедур сортировки-упорядочения.

Разрядно-логарифмическое кодирование является расширением двоичной арифметики, что обеспечивает возможность использовать на новом качественном уровне библиотеку алгоритмов, которые уже были разработаны, а также технологическую базу реализации двоичной арифметики. Исследования показывают, что существующий стандарт IEEE 754 может быть заменен на новый на основе РЛ арифметики.

УДК 004.94 (043.2)

В. П. Гамаюн, д.т.н.,
А. А. Комар,
И. Е. Ильин,
А. В. Липкин
Национальный авиационный университет, Киев

МЕЖДИСЦИПЛИНАРНАЯ ЛАБОРАТОРИЯ МОДЕЛИРОВАНИЯ

Вопросы организации и обеспечения междисциплинарных исследований не являются новыми и составляют значительную часть общенаучного подхода. В фундаментальных и прикладных науках имеется большой арсенал методологической, теоретической экспериментальной базы, позволивший получить новые результаты на основе междисциплинарных исследований.

Применение междисциплинарных исследований, как правило, является не просто механистическим применением нескольких наук и методологий к решению одной поставленной задачи, а выполнением комплекса работ с превалированием некой концепции.

Предлагается применить универсальный подход в моделировании. основанный на моделях с безошибочной арифметикой или, другими словами, высокоточные модели как основа достоверных расчетов для решения задач любого типа. Так как расчетно-моделирующая компонента является обязательной при научных исследованиях прикладного и фундаментального направлений, то междисциплинарных характер такой организации исследований очевиден. При моделировании любой задачи предлагается использовать такой тип компьютерной арифметики, который бы сводил инструментальную ошибку к минимуму.

Основой такого типа безошибочной арифметики является разрядно – логарифмическое кодирование, которое является расширением двоичной арифметики и обладает рядом отличительных свойств:

- обработка реализуется как арифметика целых чисел, исключаются процедуры нормализации и округления;
- применяется только один тип данных ЦЕЛОЕ ЧИСЛО;
- диапазон представления числовых данных по сравнению с двоичным возрастает на несколько порядков:
- число нуль имеет единственное однозначное представление для всех типов компьютеров;
- на основе разрядно-логарифмической арифметики разработана информационная технология высокоточных вычислений для задач любого типа;
- информационная технология реализуема на языках программирования высокого уровня;
- технологическая реализация не требует новой базы, а может быть использована база для двоичной арифметики.

Междисциплинарная лаборатория моделирования представляет собой институт открытого типа, включенный с в системы локальных , корпоративных, региональных сетей и GRID структур.

Технология высокоточных вычислений и моделирования разработана таким образом, что в лабораторию поступает запрос-задание, расчетно-моделируемая

часть которого уже прошла апробацию у заказчика. В лаборатории проверяется правильность расчетов с помощью специального математического обеспечения на серийной технике. Результаты, анализ оцениваются в различных режимах по запросу заказчика.

При этом возможны такие основные направления работ :

- разработка и исследование эффективных численных методов решения научных и прикладных задач;
- компьютерное моделирование научных и прикладных задач ;
- разработка и исследование оптимальных алгоритмов численного анализа и их реализация на ЭВМ;
- разработка алгоритмов и создание программного матобеспечения для решения задач на современных персональных и супер-ЭВМ;
- участие в учебном процессе: чтение лекций, проведение семинаров и организация практикумов.

Все перечисленные основные направления работ включают как оригинальную часть, так и опыт прогресссивных технологий и разработок.

Например ряд методов м алгоритмов вычислительной математики не находил применения из-за погрешностей инструментального типа. Использование математического обеспечния на основе разрядно-логарифмической арифметики позволяет использовать известные решения на новом качественном уровне. Например новое развитие получает аппарат цепных дробей.

Вычисление факториала 500! является примером высокоточной обработки в междисциплинарной лаборатории. С применением разрядно-логарифмической арифметики было определено точное значение методом прямого умножения РЛ операндов.

Фрагмент правильного результата следующий:

1220136825991110068701238785423046926253574342803192842
192413588385845373153881997605496447502203281863013
616477148203584163378722078177200480785205159329285
477907571939330603772960859086270429174547882424912
726344305670173270769461062802310452644218878789465
754777149863494367781037644274033827365397471386477
878495438489595537537990423241061271326984327745715
5463099772027810145610811883737095310l6…….

Приведенный ряд не является окончательным.

В формате с плавающей запятой - 1.220136825991110068701238785423046926253574342803192….*10^{1134} . Всего было определено 1135 десятичных чисел результата.

Большинство процедур высокоточных вычислений разработаны на основе обратных вычислений, а также с помощью эталонных сравнений.

Для обучения пользования междисциплинарной лабораторией моделирования достаточно образования младшего специалиста IT направления.

Компьютерные системы и средства для реализации междисциплинарной лаборатории моделирования не требуют особых параметров по производительности, а должны соответствовать современному обеспечению для локально сетевых решений и вычислений.

УДК 681.51(043.2)

В. В. Горіна
Національний авіаційний університет, Київ

ЗАСТОСУВАННЯ СИСТЕМ ДИСПЕТЧЕРИЗАЦІЇ ДЛЯ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ РЕАЛЬНОГО ЧАСУ

Система диспетчеризації дозволяє спостерігати за роботою системи в реальному часі. Диспетчеризація дозволяє контролювати різні процеси, що відбуваються на віддалених об'єктах, змінювати параметри пристроїв, які обслуговують ці об'єкти, а також переглядати протоколи їх роботи.

Для збору і подальшої обробки даних використовуються програмовані контролери, що підтримують різноманітні стандарти передачі даних. Такі контролери працюють в двох режимах: незалежному, без зовнішнього управління і залежному, спільно з центральним пультом управління [3]. Для здійснення автоматизації виробничих процесів необхідно, щоб керування ними відбувалося без участі людини. Таке управління називають автоматичним. Для автоматичного уравління застосовують різноманітні технічні та програмні засоби, які утворюють автоматичний управляючий пристрій. Якщо такий пристрій приставити до машини або механізму, які виконують технологічні операції, то цю машину або механізм називають управляючим об'єктом. Управляючий об'єкт і автоматичний управляючий пристрій становлять автоматизовану систему управління (АСУ).

Частина системи, що виконує відповідну функцію, називається блоком. Залежно від виконуваних функцій в автоматичному управляючому пристрої блок може бути сприймаючим, задавальним, запам'ятовуючим, управляючим і виконавчим. Сприймальний блок приймає дії із зовні. Задавальний блок встановлює заданий порядок роботи і значення заданої величини. Запам'ятовуючий блок (блок пам'яті або фіксації) фіксує на відповідний проміжок часу значення дії. Упаравляючий блок перетворює дію, прийняту від інших блоків, і передає її на виконавчий блок. Виконавчий блок надає управляючі дії для об'єкта [1].

Кожна система, пристрій і блок мають вхід і вихід. Вхід – це частина системи, пристрою або блока, на яку безпосередньо подається дія. Вихід – це та частина, яка безпосередньо діє на іншу частину системи. Залежно від характеру управляючої дії АСУ бувають стабілізуючі, програмні і слідкуючі.

Стабілізуюча автоматична система здатна тривалий час підтримувати управляючу величину постійною (наприклад, підтримування заданої швидкості обертання вала, рівня рідини в резервуарі, тиску та ін.).

Програмна автоматична система змінює управляючу величину відповідно з наперед заданою послідовністю змін. Таку систему застосовують у сушильних камерах, в яких температура і вологість повітря мають змінюватись відповідно до заданого режиму сушіння. Програма може бути задана перфорованими стрічками і картами, магнітним записом, кіноплівкою, кнопковими пристроями та ін.

Слідкуюча автоматична система замінює управляючу величину залежно від значення невідомої раніше змінної величини на вході автоматичної системи. Така

система здатна слідкувати за змінами, що відбуваються в будь-якому процесі. В цю систему можуть входити навіть лічильно-обчислювальні пристрої.

АСУ з розімкнутим ланцюгом дії називається така система, в якої вхідними є тільки зовнішні дії управляючого пристрою. Ці дії визначені раніше і не залежать від дійсного стану управляючого об'єкта або процесу. Така система використовується тільки для управління простими процесами, які відбуваються в одних і тих самих умовах і у визначеному порядку.

АСУ із замкнутим ланцюгом дії називають таку систему, в якій вхідними для управляючого пристрою є як зовнішні, так і внутрішні (контролюючі) дії. Прикладом замкнутої системи може бути автоматична система регулювання. В ній керуючі дії виробляються внаслідок порівняння дійсного значення управляючої величини з наперед заданою.

АСУ широко застосовуються в усіх галузях промисловості не тільки для управління машинами, верстатами, лініями та іншими транспортними об'єктами, а й для контролю якості обробки деталей та сортування їх.

Для запобігання несправностей, які можуть призвести до аварій, поломки інструментів і устаткування в автоматичних лініях, застосовують засоби автоматичної сигналізації і захисту, які в будь-який час можуть зупинити лінію чи інший об'єкт.

Автоматизація – один з напрямів науково-технічного прогресу, спрямований на застосування саморегульованих технічних засобів, економіко-математичних методів і систем управління, що звільняють людину від участі в процесах отримання, перетворення, передачі і використання енергії, матеріалів чи інформації, істотно зменшують міру цієї участі чи трудомісткість виконуваних операцій [2]. Разом з терміном автоматичний, використовується поняття автоматизований, що підкреслює відносно великий ступінь участі людини в процесі.

Автоматизація, окрім об'єкта управління вимагає додаткового застосування датчиків (сенсорів), управляючих пристроїв (контролерів із засобами вводу-виводу), виконавчих механізмів та у переважній більшості базується на основі використання електронної техніки, та методів обчислень, що іноді копіюють нервові і розумові функції людини.

Вищою формою автоматизації є роботизація. При роботизації технологічні операції виконують машини-роботи, які уподібнюють рухи людини, але ще з більшою точністю. Виділено класифікацію автоматизованих систем управління. Для програмування АСУ в реальному часі використовують системи диспетчеризації, які в даний час є актуальними для сучасного промислового підприємства, бізнес-центрів та інших об'єктів підвищеної відповідальності.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием – М.: "Вильямс", 2009. – 720 с.:ил..

2. Джон Парк, Стив Маккей, Эдвин Райт. Передача данных в системах контроля и управления – СПб.:Группа ИДТ, 2007. – 480 с.: ил.

3. Нестеров А.Л. Проектирование АСУТП. Методическое пособие. Книга 1. – СПб.: Издательство ДЕАН, 2006. – 240 с.

УДК 004.912

В. В. Гудь,
Ю. Є. Боярінова, к.т.н.
Національний технічний університет України "КПІ", Київ

НЕЧІТКИЙ ТЕКСТОВИЙ ПОШУК З ВИКОРИСТАННЯМ НЕПОВНИХ МНОЖИН ВИДАЛЕНЬ

Збільшення кількості даних незмінно веде до збільшення кількості помилок. Тому для задач спеціалізованого повнотекстового пошуку важливе врахування можливості виникнення помилок як на стороні даних, так і на стороні пошукового запиту. Існуючі техніки пошуку на базі інвертованих індексів не можуть забезпечити інтерактивний час (менше 100 мілісекунд) при вирішенні задачі нечіткого повнотекстового пошуку по великих об'ємах даних (понад 10 гігабайт).

В якості базового алгоритму ефективним є класичний метод Мора-Френкеля [1]. Спочатку формують множину-окіл з комбінаціями помилок для кожного слова вхідного словника. Для цього до слова застосовують певну кількість помилок, послідовно видаляючи з нього букви і формуючи всі можливі підпослідовності. Об'єднання таких множин підпослідовностей формує пошуковий індекс. Над пошуковим запитом виконують аналогічні операції, після чого здійснюють пошук співпадінь між елементами індексу та множини видалень, сформованої на основі слів запиту. На даний момент цей клас алгоритмів є одним з найшвидших [2], але його експоненційна складність по використанню пам'яті робить його застосування в класичному вигляді неможливим на практиці.

Проведено значну оптимізацію по зменшенню кількості пам'яті, необхідної для розміщення індексу, шляхом обмеження довжини слів, які проходять індексацію і використання інвертованого індексу з порядковими ідентифікаторами слів вхідного словника замість повного об'єднання множин видалень. Формування обмеженого індексу не впливає на коректність роботи алгоритму, а лише збільшує кількість слів, для яких необхідно здійснити перевірку схожості по відстані Левенштейна. Використавши швидку бітово-паралельну версію динамічного алгоритму Маєрса [3] для перевірки кандидатів на співпадіння можна забезпечити швидкодію як у класичного алгоритму, але з уникненням експоненційного використання пам'яті для розміщення пошукового індексу.

Результуючий алгоритм дозволяє виконати пошук по повному набору статей англійської версії ресурсу Wikipedia.org (3.7 мільйони статей, 21 гігабайт текстових даних) з межею помилки в 2 символи за час в середньому 90 мілісекунд і з використанням лише 4 гігабайт пам'яті для зберігання всього індексу. Для порівняння, пошуковий фреймворк Apache Lucene виконує аналогічний пошук в середньому за 20 секунд, а гібридний алгоритм Лі - за 6 секунд.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Mor, M., Fraenkel A. S. A hash code method for detecting and correcting spelling error, – Communications of the ACM 25, 1982. – 955 pages.

2. Boytsov L. M. Indexing methods for approximate dictionary searching: Comparative analysis, – Journal of Experimental Algorithmics 16, 2011. – 91 pages.

УДК 004.056.53 (043.2)

М. М. Гузій, к.т.н.,
І. А. Жуков, д.т.н.,
Ю. М. Мінаєв, д.т.н.
Національний авіаційний університет, Київ

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В КОМПЬЮТЕРНІ МЕРЕЖІ

Проблема виявлення та попередження вторгнень в комп'ютерні мережі (КМ) останнім часом отримала серйозну увагу з боку фахівців, що пояснюється складністю проблеми та її прикладним значенням. В [1] наводиться аналіз інженерних принципів, методик та алгоритмів виявлення аномалій, які можуть бути корисні для побудови перспективних систем попередження вторгнень в КМ. Проблема виявлення вторгнень в мережах TCP/IP зводиться до задач розпізнавання і практично вирішується на основі аналізу наступних параметрів трафіку КМ:

– структурних ознак (сигнатур) відомих типів атак;

– інваріантних ознак структури коректних обчислювальних процесів;

– кореляційних ознак нормального функціонування

– розподілених обчислювальних систем.

Розпізнавання аномалій передбачає вирішення наступного комплексу завдань:

– формування безлічі еталонів інваріантів нормального

– розвитку обчислювальних процесів в умовах апріорної невизначеності впливів зовнішнього і внутрішнього середовища;

– вибір шкал вимірювання ознак еталонів або інваріантів;

– обґрунтування достатнього числа інформативних ознак, що характеризують інваріанти;

– формування системи правил для розпізнавання аномалій.

Авторами запропонована універсальна методика виявлення аномалій на основі інваріантів подоби шляхом порівняння значень інваріантів подоби реальних обчислювальних процесів з еталонними значеннями інваріантів, що дозволяє розробити повністю автоматичний детермінований алгоритм виявлення аномалій. Для дослідження комп'ютерних мереж отримали широке застосування методи інтелектуального аналізу даних, які дозволяють з представлених наборів даних витягати знання у вигляді системи правил. Ухвалення рішення про виявлення атаки або вторгнення здійснюється на основі застосування ряду методів до даних, отриманих від програмних мережевих сенсорів, в тому числі:

– методу виявлення вторгнень, заснованого на методах штучного інтелекту і використанні бази знань, що виконує виявлення розподілених атак;

– методу виявлення аномалій, що виконує виявлення відхилень в роботі системи і ґрунтується на профілюванні користувачів;

– методу виявлення атак відмови в обслуговуванні.

Модуль прийняття рішення має два рівня класифікації для виявлення аномальної мережевої активності. На першому рівні знаходиться класифікатор, що розділяє мережеві записи на два класи: «норму» і «підозра на вторгнення». На

другому рівні мережеві записи, віднесені до другого класу, далі обробляються комітетом класифікаторів на основі методу опорних векторів для розпізнавання класів атак. В [2] запропонована інтелектуальна технологія ідентифікації атак на КМ, що базується на тензорному поданні трафіку КМ. Інваріанти тензор-трафіку дозволяють отримати нове знання і досить достовірно визначити наявність атаки на мережу.

Аналіз трафіку, представленого у вигляді тензора, дозволяє отримати додаткові знання, що дозволяє враховувати значення власних векторів. У тензорному полі, подібно критичним точкам векторних полів, існують деформовані точки, де кілька власних значень рівні. Ці точки поділяють тензорне поле на області, відповідно до топологічної структури. Аналіз поведінки власного вектора біля цих точок визначає топологію тензоного поля.

Проведені дослідження показали ефективність застосування тензорною методології для обліку умов невизначеності при аналізі трафіку [3].

На рис. наведені графічні відображення тензор-трафіку «атака - відсутність атаки» і їх векторні аналоги, побудовані на базі систем ортогональних інваріантів (sigma,tau), які показують високу ефективне використання векторних аналогів тензор-трафіка для ідентифікації аномальних режимів КМ.

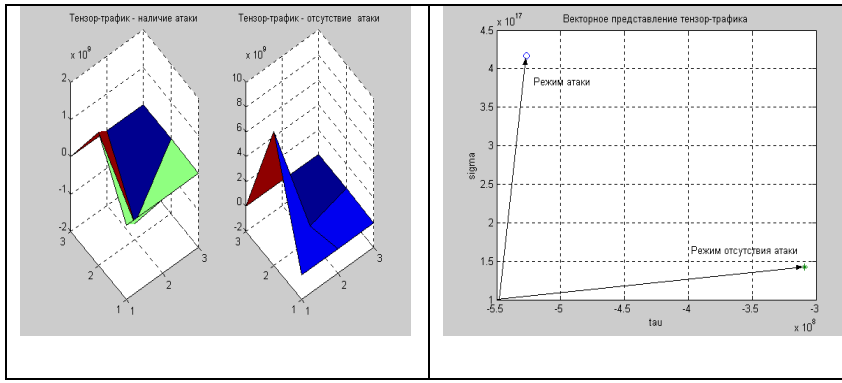

Рис. Ідентифікація аномального трафіку КМ

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Jiang D., Qin W., NieL. etal. Time-frequency detection algorithm of network traffic anomalies. Intern. Conf. on innovation and information management (ICIIM IPCSIT). — 2012. — Vol. 36. — IACSIT Press, Singapore. — P. 110—116.

2. Ю.Н.Минаев, О.Ю.Филимонова, Н.Н.Гузий. Интеллектуальные технологии в системах идентификации и прогнозирования атак на компьютерные сети. Электронное моделирование, – Т.27. – №6. 2005. – С. 37–52.

3. Ю.Н. Минаев, О.Ю. Филимонова, Ю.И. Минаева. Идентификация аномалий трафика компьютерных систем на основе методики структурирования многомерного трафика. Электронное моделирование, – Т. 35. – № 4. 2013. – С. 73 – 91.

УДК 681.518 (043.2)

О. О. Жолдаков, к.т.н.,
А. О. Жолдаков
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕКСПЕРТНИХ ОЦІНОК В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Досвід розробки автоматизованих систем (АС) на основі математичного моделювання технологічних процесів та систем із значним обсягом фактографічної інформації щодо складу і зв'язків між елементами системи приводить до висновку, що строго формалізовані методи прогнозування, планування та управління виявляються неспроможними у цілому ряді ситуацій.

Навіть такі строго регламентовані процеси як технічне обслуговування складних апаратів і систем у процесі свого розвитку і все більш повної інформатизації приходять до дисбалансу між програмно-технічними можливостями і усталеними формами обслуговування. Якщо взяти АС технічного обслуговування літальних апаратів, то навіть найпростіший літак має більш як шість мільйонів деталей, згрупованих у компоненти, що обслуговуються відповідними спеціалістами. Побудова графіків обслуговування в умовах наперед не визначеного технічного стану та зміни зовнішніх умов не може бути повністю заформалізованою, без урахування експертних прогнозних оцінок. На перший погляд подолання проблеми невизначеності може бути цілком здійснене за рахунок привнесення в процеси управління можливостей сучасних інформаційних технологій, резерв яких здається невичерпним. Проте, слідування відомому кібернетичному принципу "достатнього різноманіття" призводить до ускладнення системи управління настільки, що складність стає не сумірною із можливостями людини, що приймає кінцеве рішення.

Виявлення такого роду проблем призводить до необхідності взаємодії двох типів суб'єктів проведення дослідження та синтезу АС управління технологічними процесами і системами. До перших відносяться особи, зацікавлені у виявлені проблемної ситуації, що потребує прогнозних оцінок; другі – є джерелом інформації щодо об'єкту керування – експертами в даній проблемній області.

Методи експертного оцінювання суттєво відрізняються від методів обробки фактографічної інформації, а саме: генератором прогнозної інформації виступає спеціаліст (або група спеціалістів) у даній предметній області; інформація щодо об'єкту і параметрів управління представляється звичайно і якісному форматі.

Експертне оцінювання – це формалізована якісна або кількісна оцінка експертами характеристик із їх наступним порівнянням.

У якості типових задач, пов'язаних із необхідністю прогнозування розвитку подій у керованій системі можна виділити такі смислові постановки:

– визначення очікуваних подій із оцінкою ймовірності їх виникнення;
– визначення поточних цілей управління технологічним процесом з упорядкуванням за ступенем пріоритетності;
– визначення альтернативних варіантів розв'язання задач (стратегій реалізації)

із оцінкою їх переваги;

– визначення альтернативних варіантів розподілу обмежених ресурсів.

У свою чергу проблеми, що виникають у слабко структурованих задачах, діляться на два класи: такі, у відношенні до яких у експерта є достатньо стійкі уявлення та такі, у відношенні до яких нема "достатнього інформаційного потенціалу". У останньому випадку важливими стають евристичні процедури виявлення і обробки інформації із урахуванням якісного складу групи експертів.

На перший план виходить теза щодо "мудрості натовпу" у порівняні із оцінками навіть "найкращого" експерта.

При проведенні експертизи прийнято виділяти наступні етапи:

– організаційний етап, коли створюється керівництво експертами;

– підбір і формування групи експертів разом із вибором методичного забезпечення;

– визначення технології форм і методів проведення експертизи;

– реалізація системного підходу до проведення експертизи із урахуванням можливості набуття додаткових (уточнених) знань в процесі повторних експертиз із оцінкою їх достовірності.

До математичних методів експертного оцінювання відносять, як правило, метод прогнозного графа, аналіз на проблемних мережах, метод перехресної взаємодії та інші.

Наступною проблемою є обґрунтування способів представлення експертної інформації.

За характером експертна інформація поділяється на якісну та кількісну. Типи шкал вимірів експертної інформації розділяються: для якісної – іменована (номінальна) шкала та порядкова: для кількісної – інтервальна, відносна, абсолютна.

Вищевказані оцінки називаються оцінками першого роду, тоді як оцінки, що складаються із двох частин, де перша містить твердження, а друга – відображає степінь упевненості експерта, називаються оцінками другого роду. Самі оцінки розділяються на вербальні, групові, парні, процедурні, векторні, бальні, інтервальні, точкові, багато точкові, функціональні.

Можливість використання різних методів оцінювання зумовлюється наявною інформацією щодо об'єкту. Проте, вони приводять до близьких результатів при розв'язанні аналогічних задач.

Обґрунтування якісного та кількісного складу експертної групи може відбуватися за формалізованими процедурами відбору – алгебраїчною і статистичною.

Статистичний підхід можна застосовувати лише тоді, коли оцінки різних експертів можна вважати рівноправними, тоді як алгебраїчний підхід допускає суттєву різницю між окремими та середньою оцінками.

Ключовим моментом проведення експертного оцінювання являється обробка результатів проведення експертного оцінювання альтернативних прогнозів. Саме від цього залежить якість кінцевого результатах оцінювання. Три основних переділи обробки результатів опитування експертів включають попередній аналіз індивідуальних оцінок, обчислення групової оцінки та визначення якості групової експертної оцінки. Кінцевим етапом експертного оцінювання являється визначення якості прогнозу на основі групової експертної оцінки.

УДК 004.272:004.383(043.2)

И. А. Жуков, д.т.н.,
Н. А. Ковалев, к.т.н.
Национальный авиационный университет, Киев

РЕАЛИЗАЦИЯ ИНТЕГРАЛЬНЫХ ВЫЧИСЛЕНИЙ

Развитие современных элементных баз и вычислительных платформ, микропроцессоров (МП), цифровых сигнальных процессоров, графических ускорителей, ПЛИС, усложняет выбор из них для реализации различных вычислений в реальном масштабе времени. В ряде работ проведен сравнительный анализ [1, 2]. В основном оценивается быстродействие при решении узкого круга специфических и синтетических задач, а результаты сравнений иногда противоречивы.

Объектом разработок часто выступают однородные вычислительные среды, в частности, цифровые интегрирующие структуры (ЦИС) [3, 4]. Выполняя численное интегрирование по Стилтьесу систем уравнений Шеннона (СУШ), они эффективно применяются для решения широкого круга математических задач моделирования и управления. Поэтому целесообразно комплексно сравнить некоторые упомянутые базисы и платформы при реализации ЦИС на их основе.

Аппаратная и программная реализации решения актуальной для многих бортовых систем управления (БСУ) баллистической задачи встречи позволило провести такое сравнение. Получена СУШ, эквивалентная системе дифференциальных уравнений внешней баллистики, вида:

$$\begin{cases} dz_1 = -z_{24}dt;\ dz_2 = z_3dz_5;\ dz_3 = -z_2dz_5;\ dz_4 = 2z_1dz_1;\ dz_5 = (z_8 - k_3k_4)dt; \\ dz_6 = -z_6dz_7;\ dz_7 = z_6dz_1;\ dz_8 = dz_3(k_5z_1 - k_1z_6) + z_3(k_5dz_1 - k_1dz_6);\ dz_9 = z_{14}dt; \\ dz_{10} = k_8z_{15}dt;\ dz_{11} = z_3dz_1 + z_1dz_3;\ dz_{12} = -z_{12}dz_{13};\ dz_{13} = z_{12}dz_{11}; \\ dz_{14} = (k_6z_{10}dz_5 - k_7)dz_{12} + k_6z_{12}(dz_{10}dz_5 + z_{10}d^2z_5);\ dz_{15} = z_1dz_{10} + z_{10}dz_1;\ dz_{16} = z_{21}dt; \\ dz_{17} = z_{22}dt;\ dz_{18} = z_{23}dt;\ dz_{19} = z_{20}dz_9;\ dz_{20} = -z_{19}dz_9;\ dz_{21} = z_{20}dz_{11} + z_{11}dz_{20}; \\ dz_{22} = z_{19}dz_{11} + z_{11}dz_{19};\ dz_{23} = z_2dz_1 + z_2dz_1;\ dz_{24} = k_1dz_2 + k_2k_3dz_4. \end{cases}$$

Для решения задачи встречи выполнялось 4-5 итераций интегрирования СУШ по Стилтьесу, каждое из которых моделирует более точный полет снаряда к цели длительностью примерно 5 с. Численное интегрирование выполняется по формуле квадратичных парабол с шагом dt=0,0025c.

Для реализации ЦИС могут применяться ПЛИС типа *FPGA*. Это обусловлено их архитектурными особенностями, связанными с большой степенью интеграции функциональных элементов, высоким быстродействием, возможностью реализации максимального параллелизма, присущего задаче. Кроме того, СУШ содержит лишь мультипликативные и аддитивные операции, а современные семейства *FPGA* имеют в своем составе большое количество встроенных умножителей (*Embedded Multiplier*, *DSP blocks*), позволяющие эффективно реализовать операции умножения, сложения, накопления и их комбинации. На базе МС *FPGA Cyclone IV EP*4*CGX*22*BF*, *Stratix IV EP*4*SGX*110*F*29*C*4, а также

ASIC Hardcopy IV HC4E25FF484 с использованием САПР *Quartus* II фирмы *Altera* и *ModelSim AE* фирмы *Modeltech* разработаны соответствующие экстраполяционные параллельные ЦИС. Их структура непосредственно следует из СУШ (1). Длительность шага интегрирования составляет 5 тактов. Описание схем выполнено на языке *VHDL*.

Программное решение производилось с применением среды визуального программирования *Embarcadero RAD Studio* 2010, многоядерных МП и технологии параллельного программирования [5] на базе библиотеки *TPL* (*Task Parallel Library*) платформы программирования *Microsoft .NET Framework* 4.

В таблице приведены некоторые из полученных характеристик схемных и программных решений: времена решения задачи *Tmin*, максимальные частоты тактирования f_{max}, мощности энергопотребления *Pmax* и стоимости МС. При этом аппаратные решения предполагают обработку 24-разрядных данных с фиксированной точкой, а программное решение – с плавающей запятой одинарной точности (эквивалентны по точности интегральных вычислений).

Полученные характеристики реализаций интегральных вычислений

	МП *AMD Phenom II X3* 740	*FPGA Cyclone IV EP4CGX22BF*	*FPGA Stratix IV EP4SGX110F29C4*	*ASIC Hardcopy IV HC4E25FF484*
f_{max}	2,8 ГГц	140 МГц	154 МГц	214 МГц
Tmin, мс	11,527	0,71	0,65	0,47
Стоим. МС, у.е.	80	40	800	-
Pmax, Вт	95	1,2	2,7	-

Проведенные исследования показали, что скорость решения подобных практических задач на базе *FPGA* и *ASIC* на порядок превосходит скорость их программного решения. По соотношению быстродействия, энергопотребления, сложности разработки, массогабаритных параметров и стоимости интенсивные вычисления в реальном масштабе времени оптимально реализовывать в бюджетных МС *FPGA*. При этом аппаратные затраты позволяют дополнительно реализовать другие цифровые устройства, повышая тактико-технические и технико-экономические характеристики БСУ в целом.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Vestias Mario, Neto Horacio. Trends of CPU, GPU and FPGA for high-performance computing // Field Programmable Logic and Applications (FPL), 2014 24th International Conference on, 2-4 Sept. 2014, Munich, Germany. – P. 1-6.*

2. *Chey Shuai, Liz Jie, W. Sheaffery Jeremy, Skadrony Kevin, Lach John. Accelerating Compute-Intensive Applications with GPUs and FPGAs // Application Specific Processors SASP 2008. Symposium on, 8-9 June 2008, Anaheim, CA. – P. 101-107.*

3. *Пат. 91258 Україна, МПК[6] G06F 7/60, G06F 7/64, G06F 7/57. Цифровий інтегро-арифметичний пристрій / Жуков І.А., Ковальов М.О., Кубицький В.І. – и 2014 01106; заявл. 06.02.2014; опубл. 25.06.2014, Бюл. № 12. — 10 с.*

4. *Беспалов Д.А., Гузик В.Ф. Некоторые аспекты разработки современных цифровых интегрирующих вычислительных систем // Известия ЮФУ. Технические науки. – 2015. – № 3. – С. 6-16.*

5. *Жуков І.А., Корочкін О.В. Паралельні та розподілені обчислення: навч. пос. –К.: Корнійчук, 2005. – 226 с.*

УДК 004.273:004.457 (043.2)

С. В. Журавель
Національний авіаційний університет, Київ

ВПРОВАДЖЕННЯ СТІЛЬНИКОВИХ МЕРЕЖ ЧЕТВЕРТОГО ПОКОЛІННЯ

Бурхливий розвиток різних технологій зв'язку, як фіксованої, так і мобільної, викликано, у першу чергу, підвищеним інтересом людей до мережі Інтернет. Величезна роль мережі Інтернет у сучасному світі обміну інформації незаперечна й не має потреби в підтвердженні. За допомогою глобальної мережі люди мають можливість працювати, вчитися, спілкуватися, обмінюватися даними, переглядати потокові відеофайли, прослуховувати аудіозаписи, а також користуватися в режимі онлайн усілякими послугами комерційних компаній і державних установ.

LTE (від англ. Long Term Evolution - еволюція в довгостроковій перспективі) - технологія побудови мереж бездротового зв'язку, створена в рамках проекту співробітництва в створенні мереж третього покоління 3GPP (3G Partnership Project). Основними цілями розробки технології LTE є: зниження вартості передачі даних, збільшення швидкості передачі даних, можливість надання більшого спектра послуг по більше низькій ціні, підвищення гнучкості мережі й використання вже існуючих систем мобільного зв'язку. Головна відмінність стандарту LTE від інших технологій мобільного зв'язку полягає в повній побудові мережі на базі IP-технологій. Радіоінтерфейс LTE забезпечує поліпшені технічні характеристики, включаючи максимальну швидкість передачі даних більше 300 Мбіт/с, час затримки пересилання пакетів менш 5 мс, а також значно більше високу спектральну ефективність у порівнянні з існуючими стандартами бездротового мобільного доступу третього покоління (3G). На сьогоднішній день мережі стандарту LTE розгорнуті в більш ніж 80 країнах світу і їхнє число швидко збільшується.

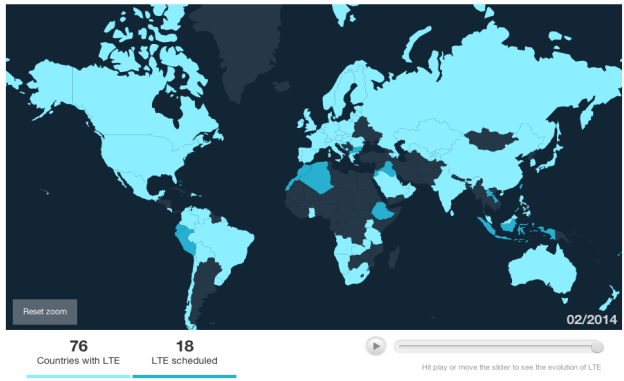

Рис. Карта впровадження технології *LTE* в світі

В Україні поширення доступу до мережі Інтернет викликає труднощі, у першу чергу, через просторість території. У містах нашої країни до глобальної мережі

може підключитися будь-який бажаючий, виходячи зі своїх потреб, вибравши задовольняючий його тариф. При чому в міського жителя є вибір між провідним і бездротовим доступом. Недоліком бездротовим доступів з використанням мереж мобільних операторів є швидкість. Забезпечення населення високошвидкісним виходом у мережу Інтернет є однією з причин роботи над цією тематикою.

Для рішення цієї проблеми можна піти різними шляхами. Можна використати для доступу в мережу Інтернет супутниковий зв'язок, організувати доступ за допомогою провідних ліній зв'язку або за допомогою мобільного зв'язку. Супутниковий доступ не задовольняє швидкістю й занадто дорогий. Доступ за допомогою провідних ліній можливий тільки при наявності на селі цифрових АТС, але за даними служби державної статистики за осінь 2013 року цифровізація сільської місцевості країни склала не більше 63% і просувається повільними темпами. Доступ за допомогою мобільного зв'язку став можливий із приходом стандартів *EDGE*/*GSM* й *UMTS*/*HSPA*, але швидкість першого занадто мала для комфортної роботи в мережі Інтернет, а дія другого найчастіше не поширюється на сільську місцевість по двох причинах: по-перше, мобільні оператори, у першу чергу, намагаються охопити міську місцевість й, по-друге, дальність дії сигналу в діапазоні 1920-2100 Мгц не висока, тому, щоб охопити більші території потрібно будувати величезну кількість базових станцій, що економічно не вигідно.

Одним з перспективних варіантів забезпечення населення високошвидкісним доступом у мережу Інтернет - це побудова мереж стільникового рухливого радіозв'язку четвертого покоління (4*G*). Самим підходящим стандартом 4*G* для рішення цього завдання є технологія бездротового доступу *LTE*.

Розвиток бездротових технологій зв'язку за останні десять років зробив величезний стрибок уперед. Швидкість надання бездротового доступу зросла в десятки разів. Широкий спектр послуг, висока якість обслуговування, досить висока мобільність - от чим відрізняються сучасні бездротові мережі зв'язку. Розробка технології *LTE*, я вважаю, зробила перший крок на шляху до повної відмови від фіксованого зв'язку в будь-якій місцевості.

Проведено аналіз надання послуг зв'язку в різних країнах світу. Визначено основні складові якості та розглянуто методи їх підвищення.

Проведено дослідження основних проблем надання послуг зв’язку, приведено основні способи їх вирішення, а саме:

1.Правильне направлення базових станцій для покриття зон мобільних абонентів.

2.Нахил діаграми направленості до землі, що дозволяє вирішити проблеми зв’язку в низинах та інших закритих областях.

3.Ефективний план хопінгу для мереж *LTE.*

Будівництво мережі *LTE* в Україні дозволить стати найбільшим оператором, що надає послуги бездротового доступу, а також заощадити значні кошти, тому що в майбутньому відпаде необхідність у модернізації мережі фіксованого зв'язку.

УДК 004.942 (043.2)

О. М. Зудов, к.т.н.
Національний авіаційний університет, Київ

МОДЕЛЮВАННЯ ПОВЕДІНКИ СУЗІР'Я ШТУЧНИХ СУПУТНИКІВ ЗЕМЛІ СИСТЕМИ СУПУТНИКОВОЇ МОБІЛЬНОЇ ТЕЛЕФОНІЇ

З використанням оптимізаційних методів і комп'ютерного моделювання було розглянуто проблему взаємного розташування штучних супутників Землі, які використовуються у телекомунікаційних системах супутникового мобільного зв'язку.

Реалізація супутникової мобільної телефонії пов'язано з відомими труднощами. Якщо висота супутників дуже велика, то потужність сигналу мала, оскільки вона обмежена потужністю мобільних телефонів. З іншого боку, зі зменшенням висоти зменшується зона покриття кожного супутника.

Було отримано аналітичний вигляд умови видимості супутників з конкретної точки на поверхні Землі. Ця умова має вигляд:

$$sin(\varphi_1)\times sin(\varphi_2)+cos(\varphi_1)\times cos(\varphi_2)\times cos(\lambda_1-\lambda_2)\le 1-\frac{h\times(2R+h)}{(R+h)^2} \qquad (1)$$

де ($\lambda 1$, $\varphi 1$) - картографічні координати точки на поверхні Землі (широта і довгота);

($\lambda 2$, $\varphi 2$) - картографічні координати проекції супутника на поверхню Землі (ефемериди);

R - радіус Землі;

h - висота супутника над рівнем моря.

Використовуючи даний вираз, можна отримати карту покриття поверхні Землі системою супутників (так званим сузір'ям). Вибравши певну висоту супутника над поверхнею Землі, яка зумовлена потужністю мобільного пристрою, можна обчислити необхідно мінімальну кількість супутників для покриття заданої площі на поверхні Землі в конкретний момент часу. Але виникає ще одна проблема: в інший момент часу площа покриття буде іншою. Це пояснюється тим фактом, що супутники не можуть рухатися паралельно на орбітах, що мають однаковий радіус.

Отже, виникає необхідність у знайденні оптимального взаємного розташування орбіт і положень супутників на орбіті. Критерієм оптимальності є максимально можлива площа покриття протягом усього періоду обертання супутників навколо Землі.

Цільовою функцією даної задачі оптимізації є площа покриття, а параметрами - положення орбіт, їхні кути нахилу, а також початкове положення кожного конкретного супутника на орбіті. Також було розглянуто можливість надання кожній ділянці площі на поверхні Землі певних вагових коефіцієнтів. Оскільки супутникова мобільна телефонія має найбільше значення для віддалених районів Землі з нерозвиненою телекомунікаційною інфраструктурою (пустелі, високогірні райони, джунглі тощо), а також поверхня океанів, то ці райони землі можуть

отримати більші вагові коефіцієнти в порівнянні з іншими районами, в яких актуальність супутникової мобільної телефонії менша.

Кількість змінних параметрів даної задачі дуже велика, а цільова функція багатоекстремальна, тому її розв'язання вимагає спеціальних комп'ютерних методів.

Було запропоновано декілька методик для оптимізації орбітального руху штучних супутників Землі при проектуванні системи супутникової телефонії.

Перша методика ґрунтується на методі Монте-Карло. Геометричні параметри орбіт, а також початкове положення супутників вибираються за допомогою генераторів випадкових чисел. Для кожної випадкової системи параметрів обчислюється площа покриття; далі процес багатократно повторюється і накопичується статистика про зону покриття. Зменшити кількість повторень даному стохастичному пошуку можна за допомогою відомого алгоритму імітації відпалу [1].

Другий підхід є реалізацією еволюційної глобальної оптимізації і носить назву генетичного алгоритму [2]. Пошук оптимального розташування орбіт і супутників на них у цьому випадку більш цілеспрямований. Оскільки цільова функція даної задачі гладка, то для вирішення задачі оптимізації ефективно застосовується запропонований модифікований генетичний алгоритм [3].

Початкові положення супутників, очевидно, треба вибирати, максимізуючи попарні відстані між ними. Це зводиться до відомої задачі про розташування точкових електричних зарядів на поверхні сфери (задача Томсона), чисельні розв’язки для якої знайдені для великої кількості точок [4].

Таким чином, запропонований підхід поділяється на дві стадії: вибір початкового положення групи супутників і комп’ютерне моделювання їх орбітального руху із визначенням зони загального покриття в залежності від вибраних параметрів даного руху.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Левитин А. В. Алгоритмы: введение в разработку и анализ. Пер. с англ. — М. : Издательский дом "Вильямс", 2006. — 576 с.

2. Курейчик В.М., Родзин С.И. Эволюционные алгоритмы: генетическое программирование // Известия АН. Сер.: Теория и системы управления.— 2002.— №1.— С. 127-137.

3. Зудов О.М., Васильєв О.С. Метод градієнтного схрещування у генетичних алгоритмах неперервного коду // Електроніка та системи управління. - 2010.- №3(25).- С.143-148.

4. Андреев Н.Н., Юдин В.А. Экстремальные расположения точек на сфере // Математическое просвещение. – 1997. – Сер.3, Вып.1. – С.115-125

УДК 004.056.5:004.7 (043.2)

Р. В. Зюбіна, аспірант
О. М. Весельська,
Національний авіаційний університет, Київ
О. В. Фролов

МЕТОДИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНОЇ СКЛАДОВОЇ В АУДІОСИГНАЛАХ

Спроби приховати факт передачі інформації мають довгу історію і безліч прикладів. Наукою про приховану передачу інформації шляхом збереження в таємниці самого факту передачі є стеганографія. Ця задача вирішується за допомогою впровадження інформації, в середину різних документів і файлів, що називаються контейнерами, передача яких є звичайною справою та не визиває підозри.

Особливий розвиток отримали стеганографічні методи приховування інформації у аудіосередовищі. Базова модель вбудовування повідомлення в аудіо контейнер приведена на рис. 1.

Рис. 1. Базова модель аудіо стеганографії

Розглянемо основні методи стеганографічного захисту інформації з використанням аудіо контейнера.

1) *Кодування найменш значущих бітів (часова область).*

Даний метод є найпростішим серед методів приховування даних у аудіосигналах. Його суть полягає у заміні НЗБ у кожній точці вибірки із сигналу, представленого у двійковій послідовності. Використання даного методу обумовлює високу пропускну здатність каналу, платою за що є добре чутний низькочастотний шум. Дану проблему можна вирішити використанням записів, на яких і так присутній певний шум, наприклад, звук стадіону на живому концерті. Але, заповнені контейнери є вразливими до сторонніх впливів окрім випадків, коли секретна інформація вбудована із внесенням надлишковості. Однак, останнє при збільшенні стійкості каналу зменшує швидкість передачі даних.

2) *Метод фазового кодування (частотна область).*

Основною ідеєю методу фазового кодування є заміна фази вихідного звукового сегменту на деяку опорну фазу, характер зміни якої і відражає повідомлення, яке необхідно приховати. При правильному використанні даний метод є найефективнішим для приховування даних у аудіосигналах, оскільки, доки модифікація фази достатньо мала, наявність повідомлення може бути абсолютно не відчутно на слух. Але при збільшенні пропускної здатності

знижується стійкість, підвищується спотворення контейнера і підвищується складність обчислювання.

3) *Метод розширення спектра (часова область).*

Даний метод майже ідентичний до методу приховування даних у нерухомих зображеннях шляхом розширення спектру. Тобто, секретне повідомлення розподіляється по частотам несучого сигналу рівномірно, так щоб співвідношення сигнал(повідомлення)/шум у каналі було дуже низьким і не виникало підозр щодо наявності повідомлення. Потрібно зазначити, що на відміну від метода LSB, метод розширення спектра може бути більш ефективним, тому що він більш стійкий до методів видалення та має середню швидкість вбудовування. Крім того, метод розширення спектру досить стійкий до сторонніх шумів, що забезпечує більшу ймовірність отримання цілісного повідомлення. Однак даний метод має значний недолік, він може спотворювати сигнал, шляхом додавання шумової складової.

4) *Приховування даних із використанням ехо-сигналу.*

Ехо-методи використовуються в цифровій стеганографії і використовують проміжки між ехо-сигналами. Даний метод вбудовує повідомлення у аудіосигнал-контейнер шляхом введення у нього ехо-сигналу. Дані приховуються зміною параметрів ехо-сигналу: початкової амплітуди, швидкості затухання та зсуву. Для деяких звукових сигналів неможливо отримати достатню кількість правильно витягнутих біт впровадженого повідомлення Воно значною мірою залежить від якості початкового сигналу і, само собою, від слухача. Даний метод досить стійкий до амплітудних та частотних атак, однак до часових атак цей метод не стійкий. Особливістю даного методу є те, що контейнер можна передавати не тільки у вигляді окремого файлу, а ще й використовуючи високоякісний радіоканал, для прикладу FM діапазон. Після запису аудіо з ефіру можна отримати приховане повідомлення шляхом використання спектроаналізатора.

Переваги та недоліки розглянутих стеганографічних методів приховування інформації у аудіо середовищі представлені у таблиці 1.

Таблиця 1.

Метод	Переваги	Недоліки
Кодування найменш значущих бітів (часова область)	• простота програмної реалізації методу; • можливість застосування шифрування.	• чутливість до спотворень контейнера; • низька скритність повідомлення.
Метод фазового кодування (частотна область)	• висока стійкість до більшості відомих атак; • дозволяє вбудовувати велику кількість повідомлень в контейнер	• низька пропускна здатність.
Метод розширення спектра	• стійкий до несанкціонованого вилучення і спотворення.	• низька пропускна здатність • середня швидкість вбудовування
Приховування даних із використанням ехо-сигналу	• стійкість до амплітудних і частотних атак; • передача повідомлення у режимі реального часу	• нестійкий до атак за часом • важкий у реалізації

УДК 623.618 + 621.391

Н. П. Кадет,
Національний авіаційний університет, Київ)
О. М. Башкиров,
М. В. Зірка
Центральний науково-дослідний інститут
озброєння та військової техніки
Збройних Сил України, Київ

ПРИНЦИПИ ПРОЕКТУВАННЯ СУЧАСНИХ АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ І РИЗИКИ ЇХ СТВОРЕННЯ

Метою доповіді є формулювання загальносистемних принципів проектування сучасних систем автоматизації управління та інформатизації, а також аналіз найбільш значущих на цей час проблемних питань і ризиків створення автоматизованих та інформаційних систем (АІС) вітчизняного виробництва. Як показує історичний досвід Європи останніх років, цілковита залежність держав від іноземного постачальника життєво важливої продукції не тільки потребує надмірних фінансових витрат, але й призводить до жорсткої залежності навіть в політичній сфері. На сьогоднішній день однієї з актуальних проблем створення сучасних АІС є відсутність вітчизняних операційних систем реального часу та загального програмного забезпечення взагалі, мікропроцесорної техніки та інших обчислювальних пристроїв на власній елементній базі. В зв'язку з цим визначення принципових вимог до створюваного вітчизняного науково-технічного продукту є важливим і своєчасним науковим завданням. Внаслідок вищесказаного в доповіді розглядаються сучасні тенденції розвитку АІС, які повинні відображати концептуальні напрями розвитку телекомунікаційних засобів та комп'ютерних технологій, закладені провідними світовими компаніями, які орієнтовані на випуск інноваційної стандартоутворюючої продукції.

Враховуючи еволюцію розвитку засобів автоматизації в останні роки, можна зробити висновок, що сучасна тенденція створення АІС полягає у поглибленні інтеграції різнотипних засобів і впровадженні мережецентричного принципу управління шляхом комплексування систем різного функціонального призначення: моніторингу, телекомунікації, обчислювальних засобів, навігації, виконавчих пристроїв, засобів та сил оперативного забезпечення та логістики. Така система забезпечуватиме єдність сприйняття обстановки та передачу команд управління усім елементам, що входять до складу АІС.

Пропонується в основу практичної реалізації сучасної парадигми мережецентричного управління в єдиному інформаційному і комунікаційному просторі і створення на її підґрунті автоматизованої системи управління покласти поступовий перехід від старої системи управління ієрархічної деревовидної структури, побудованої на старому парку засобів зв'язку і автоматизації, до сучасної комплексної системи автоматизації і управління [1]. Даний підхід, на наш погляд, дозволить забезпечити для учасників процесів взаємодії в ході управління надання реальної оперативної обізнаності в усьому спектрі можливих умов його здійснення. Для чіткої синхронізації у часі роботи органів і об'єктів управління

пропонується інтегрувати окремі засоби і системи моніторингу, передачі даних, оброблення і активного впливу в програмно-апаратні засоби (модулі), що об'єднані в єдину систему на основі спільної мережі зв'язку. Застосування мережецентричних підходів потребує змін в принципах управління: особа, що приймає рішення може знаходитися не на вершині ієрархічної піраміди, як колись, а в будь-якому місці на будь-якому АРМі, в цьому сенсі змінюється сенс поняття «централізоване управління». Системоутворюючими елементами даної мережі зв'язку повинні бути комплексні апаратні засоби зв'язку. Саме вони повинні забезпечувати створення єдиного комунікаційного простору, інформаційної взаємодії пунктів і об'єктів управління, маршрутизацію повідомлень, організацію IP-телефонії та підключення елементів пунктів управління до необхідних каналоутворюючих засобів [2]. Практична реалізація перелічених заходів дозволить досягти таких результатів:

забезпечити комплексність збору і обробки інформації, уяви начальниками і посадовими особами різних рівнів даних про обстановку, положення, стан і характер дій своїх підлеглих;

надати всім посадовим особам можливості ситуаційної обізнаності про можливий характер дій;

організувати тісний взаємозв'язок підлеглих підрозділів із силами і засобами сусідів та підрозділами інших формувань, з якими потрібно організувати взаємодію.

Основними загальносистемними принципами побудови автоматизованих та інформаційних систем є принципи системності, відкритості (розвитку), сумісності, стандартизації (уніфікації), адаптивності та ефективності [3].

Загальносистемні принципи можуть бути поширені на підсистеми й елементи, що складають АІС. Розходження можуть полягати лише в значимості (вазі) того або іншого принципу стосовно до тої або іншої підсистеми. Розглянуті принципи вимоги повинні бути враховані в процесі проектування, створення і модернізації перспективних автоматизованих та інформаційних систем. засобів інформаційно-телекомунікаційних систем, автоматизації управління та інформатизації діяльності посадових осіб.

Крім цього, в доповіді проводиться класифікація і аналіз особливостей різних за своїм характером ризиків, які потрібно враховувати під час проектування автоматизованих та інформаційних систем і які можуть суттєво вплинути на час і вартість розробок.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Синявский В.К. Влияние содержания и принципов «сетецентрической войны» на процессы управления войсками (силами) // Наука и военная безопасность. – 2010. – № 4.

2. Електронний ресурс: http: // rosrep.ru / news / index.php? ELEMENT_ID=7041 & SECTION_ID=17.

3. M. Olson, M.D. Abrams, Computer Access Policy Choices, Computer& Security, V/ 9(1990), № 8, p.p.699-714.

УДК 681.51 (043.2)

Н. В. Кірхар, к.т.н.
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ АПАРАТНО-ОБЧИСЛЮВАЛЬНОЇ ПЛАТФОРМИ ДЛЯ СИСТЕМ ДИСПЕТЧЕРИЗАЦІЇ

У сучасних системах диспетчеризації інженерних систем широко використовуються інформаційні технології. Інформація про все приєднане до системи диспетчеризації обладнання виводиться в режимі реального часу на екрани моніторів. Комп'ютеризація систем диспетчеризації дозволяє інтегрувати системи безпеки, зв'язку та інженерні системи в єдиний комплекс, в якому моніторинг всього обладнання, об'єднаного системою диспетчеризації, відбувається в режимі реального часу [2].

Для програмування систем диспетчеризації доцільно використовувати апаратно-обчислювальну платформу, наприклад Arduino.

Arduino – апаратно-обчислювальна платформа, основними компонентами якої є плата вводу/виводу та середовище розробки на мові Processing/Wiring. Arduino може використовуватися як для створення автономних інтерактивних об'єктів, так і підключатися до програмного забезпечення, яке виконується на комп'ютері (наприклад: Adobe Flash, Processing, Max/MSP, Pure Data, SuperCollider). Інформація про плату (рисунок друкованої плати) знаходиться у відкритому доступі і може бути використана тими, хто вважає за краще збирати плати самостійно [1].

Плата Arduino складається з мікроконтролера Atmel AVR, а також елементів обв’язкових для програмування та інтеграції з іншими пристроями. На багатьох платах наявний лінійний стабілізатор напруги +5В або +3,3В. Тактування здійснюється на частоті 16 або 8 МГц кварцовим резонатором. У мікроконтролер записаний завантажувач (bootloader), тому зовнішній програматор не потрібен.

На концептуальному рівні усі плати програмуються через RS-232 (послідовне з’єднання), але реалізація даного способу різниться від версії до версії. Новіші плати програмуються через USB, що можливо завдяки мікросхемі конвертера USB-to-Serial FTDI FT232R. У версії платформи Arduino Uno в якості конвертера використовується контролер Atmega8 у SMD-корпусі. Дане рішення дозволяє програмувати конвертер таким чином, щоб платформа відразу розпізнавалася як мишка, джойстик чи інший пристрій за вибором розробника зі всіма необхідними додатковими сигналами керування. У деяких варіантах, таких як Arduino Mini або неофіційній Boarduino, для програмування потрібно підключити до контролера окрему плату USB-to-Serial або кабель.

Плати Arduino дозволяють використовувати значну кількість I/O виводів мікроконтролера у зовнішніх схемах. Наприклад, у платі Decimila доступно 14 цифрових входів/виходів, 6 із яких можуть видавати ШІМ сигнал, і 6 аналогових входів. Ці сигнали доступні на платі через контактні площадки або штирові роз’єми. Також існує декілька видів зовнішніх плат розширення, які називаються "shields" ("щити"), які приєднуються до плати Arduino через штирові роз’єми [3].

Програмне забезпечення. Інтегроване середовище розробки Arduino це багатоплатформовий додаток на Java, що включає в себе редактор коду, компілятор і модуль передачі прошивки в плату. Середовище розробки засноване на мові програмування Processing та спроектована для програмування новачками, не знайомими близько з розробкою програмного забезпечення [3]. Мова програмування аналогічна мові Wiring. Строго кажучи, це C++, доповнений деякими бібліотеками. Програми обробляються за допомогою препроцесора, а потім компілюється за допомогою AVR-GCC. У табл. 1, наведено порівняльну характеристику моделей Arduino.

Таблиця 1

Порівняльна характеристика моделей Arduino

Arduino	Процесор	Флеш-пам'ять, КБ	EEPROM, КБ	Двійкові входи/ виходи	Аналогові входи
Diecimila	ATmega168	16	0.5	14	6
Due	ATMEL SAM3U	256	0	54	16
Duemilanove	ATmega168/328P	16/32	0.5/1	14	6
Ethernet	ATmega328	32	1	14	6
Leonardo	Atmega32u4	32	1	14	12
Mega	ATmega1280	128	4	54	16
Mega2560	ATmega2560	256	4	54	16
Nano	ATmega168 orAT mega328	16/32	0.5/1	14	8
Uno	ATmega328P	32	1	14	6

Завдяки простоті і доступності, Arduino була використана в тисячі різних проектах та додатках. Програмне забезпечення Arduino просте у використанні для новачків, але досить гнучке для досвідчених користувачів. Воно працює на Mac, Windows, Linux. Викладачі та студенти використовують його для створення дешевих наукових інструментів. Дизайнери та архітектори створюють інтерактивні прототипи. Музиканти і художники використовують його для налаштування і експериментування з новими музичними інструментами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Brian W. Evans: Arduino programming notebook: Пер. с англ.: Блокнот программиста Arduino– М.: "Вильямс", 2007. – 40 с.:ил..

2. Нестеров А.Л. Проектирование АСУТП. Методическое пособие. Книга 1. – СПб.: Издательство ДЕАН, 2006. – 240 с.

3. Улли Соммер, Программирование микроконтроллерных плат Arduino / Freeduino. – М.: БХВ, 2012. – 256 с.

УДК 004.074.34

І. А. Клименко, к.т.н.,
О. С. Головко,
М. О. Гілляка,
Я. І. Мицьо
Національний технічний університет України «КПІ»

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АПАРАТНИХ ПРИСКОРЮВАЧІВ НА ПЛІС ДЛЯ РІШЕННЯ ЗАДАЧ ВЕЛИКОЇ РОЗМІРНОСТІ

Актуальним напрямком підвищення ефективності обчислень в області високопродуктивних обчислювальних систем сьогодні є концепція створення обчислювальних систем на базі програмованих логічних інтегральних схем [1]. Реалізація перепрограмованих апаратних обчислювачів на базі ПЛІС дозволяє підвищити ефективність обчислень у порівнянні з традиційними технологіями паралельних обчислень. Збільшення складності обчислювальних алгоритмів та обсягу оброблюваних даних приводить до необхідності рішення задач великої розмірності. В роботі досліджено вплив розмірності апаратної задачі на швидкодію обчислювального процесу.

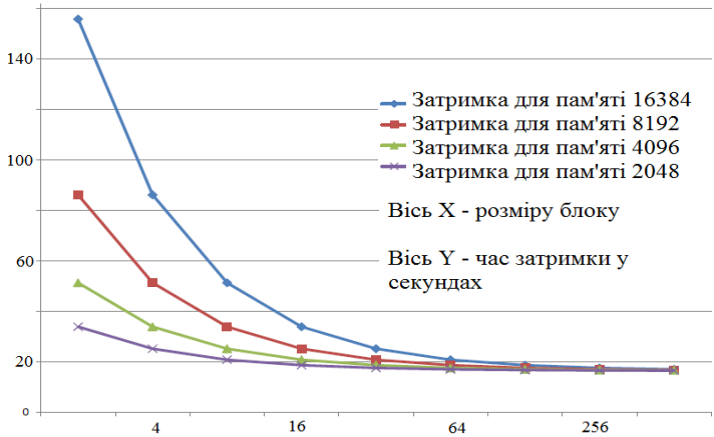

Рис. 1 Залежність часу затримки від розміру блоку

В рамках досліджень розроблена бібліотека апаратної реалізації матричних операцій. Апаратні задачі синтезовані на мові опису апаратури *Verilog*. Під час моделювання роботи обчислювальних пристроїв визначено, що одним з основних чинників, які впливають на ефективність обчислень є затримки за обміну інформацією між обчислювальними блоками та пам'яттю даних, які збільшуються зі збільшенням розмірності матриць. Час затримки визначається за наступною формулою: , де – час затримки, – час затримки передачі даних між блоками, – час пересилання блоку. На підставі експериментів з пам'яттю різних об'ємів та

різними розмірами обчислювальних блоків, отримано залежність часу затримки від розміру блоку, яка зображена на рис. 1.

З графіків видно, що час затримки обернено пропорційний розміру блоку даних, тобто чим більша кількість блоків, тим більший час передачі між цими блоками, та більший час затримки при пересилання кожного блоку. Так, розмір блоку 2 є не ефективним, оскільки значно збільшується загальна кількість блоків, а отже, збільшується загальний час передачі даних. З іншого боку, оптимальним розміром є 128 байт, оскільки подальше збільшення розміру блоку майже не впливає на час затримки.

Також досліджена залежність продуктивності обчислень на різних поколіннях кристалів ПЛІС Cyclone(I, II, III, IV) від розмірності матриць. Досліджена залежність частоти роботи схеми від розмірності матриці (рис. 2). Зроблений висновок, що зі збільшенням розмірності матриць зменшується максимальна частота роботи схеми. Це пов'язано зі збільшенням кількості використаних логічних блоків на кристалі і, відповідно, збільшенням міжкристальних шляхів проходження сигналу.

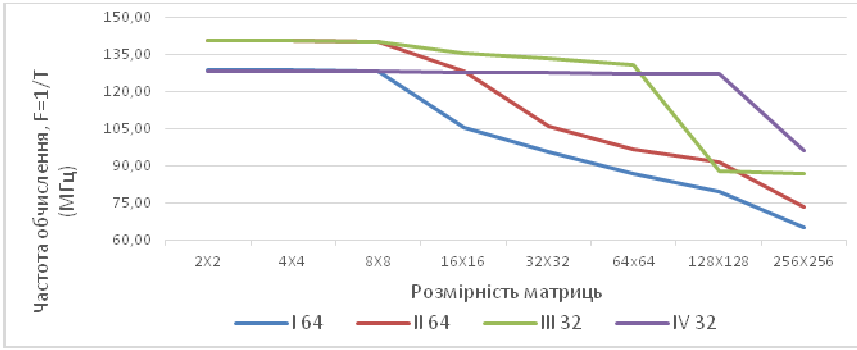

Рис. 2. Залежність продуктивності обчислення від розмірності задачі

Отже, зважаючи на актуальність реалізації обчислень надвеликої розмірності слід зробити висновок, що збільшення розмірів апаратних обчислювачів для виконання матричних операцій великої призводить до збільшення затримок під час обміну даними з пам’яттю, а також до зменшення частоти роботи обчислювальних блоків. Це значним чином впливає на швидкодію обчислень з використанням ПЛІС. Це дозволяє зробити висновок, що окрім збільшення потужностей обчислювальних засобів, виникає потреба в розробці нових методів і технологій оптимізації обчислень під час побудови апаратних засобів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Клименко І.А. Класифікація реконфігурованих обчислювальних систем І.А. Клименко, М.В. Рудницький // Інформаційні технології та комп’ютерна інженерія. – Вінниця: КІВЦ ВНТУ, 2014. – С. 120 – 128.

УДК 681.586.783(043.2)

О. Г. Коврижкин, д.т.н.
Национальный авиационный университет, Киев

КОМЛЕКСИРОВАНИЕ ИНФОРМАЦИИ ПРИ ОПРЕДЕЛЕНИИ УГЛОВОЙ ОРИНТАЦИИ БПЛА

Колоссальный рост (в конце XX, начале XXI в.в.) номенклатурного ряда выпускающихся в мире беспилотных летательных аппаратов (БПЛА) связан, главным образом, с миниатюризацией и удешевлением бортового оборудования управления и полезной нагрузки.

При наличии в составе оборудования GPS-приемника, измерение координат не представляет проблемы. И, соответственно, задачи траекторного управления решаются относительно просто давно известными методами. Принципиальную трудность продолжают составлять задачи точного управления угловым положением БПЛА. Так, в интересах выполнения задачи прицеливания (например, подсветка лазерным лучем малоразмерного объекта) необходимая точность составляет единицы миллирадиан. Для прецезионных целей проблема заключается в информационном обеспечении этой задачи.

Обеспечивающие приемлемую точность гировертикали, как правило, являются самым дорогим и сложным устройством бортового навигационного оборудования БПЛА. К сожалению, безплатформенные инерциальные системы (БИНС) на основе микродатчиков (MEMS-технологии), не содержащие гидровертикалей, обладают недостаточными характеристиками по так называемому "уходу" по времени автономной работы (десятки минут, часы). Основным чувствительным элементом таких систем являются датчики угловой скорости. Отметим, что традиционный гиродатчик на основе механического гироскопа при удовлетворительной точности обладает неприемлемыми массогабаритными характеристиками для БПЛА классов микро и мини.

Предлагается подход к построению системы коррекции углов пространственной ориентации БПЛА (в интересах БИНС) на основе комплексной обработки данных измерения земного магнитного поля и (при наличии) корреляционных устройств привязки к местности (геолокация, ТВ или ИК камеры и т.п.). Наиболее актуальной такая задача представляется для БПЛА классов микро и мини, где стоимость и вес оборудования имеет принципиальное значение. Предварительные расчеты и тестовые испытания, показывают, что погрешность определения углов может быть сведена к требуемой пока только на прямолинейных участках полета и режимах "висения". Впрочем, именно такие участки и предусматриваются основными для осуществления рассматриваемых задач.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Пупков К.А., Неусыпин К.А. Вопросы теории и реализации систем управления и навигации.– М.: Биоинформ, 2008.– 368 с.
2. Кузовков Н.Т., Салычев О.С. Инерциальная навигация и оптимальная фильтрация.– М.: Машиностроение, 1978.– 215 с.

УДК 004.056.53 (043.2)

Б. Я. Корнієнко, д.т.н.,
К. О. Тюртюбек
Національний авіаційний університет, Київ

ПОБУДОВА ПОЛІГОНУ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Висока вартість компонентів для побудови та тестування різних конфігурацій безпечної мережі, основаної на мережевому обладнанні Cisco, не дає змогу невеликим компаніям побудувати полігон кібернетичної безпеки, на якому можна протестувати конфігурацію мережного обладнання цієї компанії та політик безпеки на предмет їхньої вразливості щодо атак на комп'ютерну мережу [1].

Основною метою побудови полігону кібернетичної безпеки на основі програмного комплексу GNS3 є економія ресурсів компанії та можливість проведення оцінки ризиків при різних конфігураціях мережі, та різних реалізаціях політик безпеки. Актуальність полягає в можливості оцінити захищеність мережі при реалізації різних видів атак на неї, шляхом моніторингу і збирання статистики обладнання. На основі зібраної статистики можна робити підкріплені висновки щодо перекофігурації мережевого обладнання, необхідності заміни деяких компонентів, практично оцінити доцільність використання мережевого устаткування [2-3]. Для реалізації полігону обрано топологію з використанням одного брандмауера Cisco ASA 5520, який поділяє мережу компанії на демілітаризовану зону, внутрішню мережу та зовнішню мережу, реалізується також ще одна гілка, з прямим підключенням до зовнішньої мережі, яка дає можливість тестувати шляхом порівняння статистики ефективність використання програмно-апаратних засобів. Зональна модель є доволі гнучкою, інтерфейси присвоюються зонам, а політика перевірки – трафіку, що передається між зонами. У демілітаризованій зоні та внутрішній мережі використовуються віртуальні машини, за допомогою яких знімається статистика стосовно успішності чи неуспішності проведених атак. Використання різних серій маршрутизаторів у різних зонах дозволяє підвищити безпеку та знизити ймовірність зловмисника скористатись однією і тією ж вразливістю. Для тестування на проникність і аудиту безпеки мережі використовується дистрибутив Kali Linux, котрий містить близько 300 інструментів. Полігон кібернетичної безпеки реалізований на основі програмного комплексу GNS3, в якому побудована дана топологія та проведено налаштування мережевого устаткування, тобто підготовлений стенд для тестування мережі на проникність і проведення аудиту безпеки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Корнієнко Б.Я. Система інформаційної безпеки / Д.П. Галата, Б.Я. Корнієнко, Л.П. Галата // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – 2011. - Випуск 59. - С. 48 - 52.

2. Корнієнко Б.Я. Прикладні програми управління інформаційними ризиками / Б.Я. Корнієнко, Н.М. Марутовська, Ю.О. Максімов / Захист інформації. – 2012, № 4 (57). - С. 60 - 64.

3. Корнієнко Б.Я. Оцінка ризиків автоматизованої інформаційної системи / Б.Я. Корнієнко, О.К. Юдін, Г.В. Наконечна // Наукоємні технології. – 2012. - № 2 (14). - С. 69-73.

УДК 681.3.06

А. В. Корочкин, к.т.н.,
О. Р. Педоренко
Національний технічний університет України «КПІ», Київ

ОПТИМИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ ПОТОКОВ В ПАРАЛЕЛЬНИХ ПРОГРАМАХ

Разработка параллельных программ стала актуальной с появлением и массовым распространением многоядерных компьютерных систем. Языки и библиотеки параллельного программирования (ЯБПП) Java, C#, Ada, WinAPI, POSIX, OpenMP, MPI, PVM и др. обеспечивают различные реализации концепции потоков, позволяя использовать преимущества многоядерных процессоров. Важной задачей параллельного программирования является решение двух взаимосвязанных проблем: минимизации времени выполнения программы и загрузки всех ядер процессора. Анализ структуры параллельной программы показывает, что значительная ее часть связана с организацией взаимодействия потоков. Поэтому сокращение времени выполнения параллельной программы может быть основано на использовании методов и средств, позволяющих оптимизировать взаимодействие потоков, путем уменьшения времени их взаимодействия.

Взаимодействие потоков. С организацией взаимодействием потоков связаны основные трудности параллельного программирования. Различают два вида взаимодействия потоков: *коммуникацию* и *синхронизацию.* Коммуникация – передача данных от одного потока к другому, синхронизация - согласование поведения потоков. Обе формы взаимодействия связаны, так как отдельные виды коммуникации требуют синхронизации, а синхронизация в свою очередь требует передачи определенной информации. Поведение параллельной программы критически зависимо от обеих форм взаимодействия потоков.

В работе выполнен анализ и сравнение реализации существующих моделей взаимодействия потоков:

- модели, основанной на общих переменных (shared variable–based synchronization and communication);
- модели посылки сообщений (message-based synchronization and communication).

Выбор модели определяется видом используемой параллельной компьютерной системы (с общей или с распределенной памятью).

Источником потерь времени при взаимодействии потоков в этих моделях являются операции, приводящие к блокированию потоков. Они являются также и причиной возникновения тупиковых ситуаций - важнейшей проблемой многопотокового программирования. Отсюда возможны два подхода к оптимизации взаимодействия потоков: минимизация количества блокирующих операций и времени блокирования или переход к неблокирующим операциям.

Модель общих переменных. Временные затраты, связанные с взаимодействием потоков в первой модели, определяются потерями времени на решение задач синхронизации и взаимного исключения.

Синхронизация потоков основывается на цепочке действий: *событие - сигнал*

о событии - ожидание события. Наряду с синхронизацией двух потоков (точка-точка) имеет место множественная (групповая) синхронизация: один поток ждет сигнала от нескольких; несколько потоков ждут сигнал от одного потока; каждый поток ждет сигналы от всех остальных.

Потери времени здесь связаны с возможным блокированием потока (потоков), ждущего сигнала (сигналов) о событии (событиях). Синхронизация точка-точка поддерживается в ЯБПП с помощью двоичных семафоров, событий, мониторов. Для оптимизации групповой синхронизации возможно применение множественных семафоров, событий с ручным сбросом (manual reset), барьеров.

Решение задачи взаимного исключения обеспечивает взаимоисключающий доступ потоков к общим ресурсам (ОР). ЯБПП поддерживают решение задачи взаимного исключения с помощью семафоров, мютексов, критических секций (замков), мониторов. Оптимизация в этом случае может базироваться на сокращении времени использования общих ресурсов (ОР). В случае использования ОР, которые не изменяются потоками (копирование ОР), оптимизация может быть обеспечена одновременным (параллельным) копированием. Такой поход реализован, например, в защищенных модулях языка Ада. При этом возможно размещением копий в кэш-памяти ядер процессора. Современные ЯБПП характеризуются появлением в них готовых модулей (классов) для решения определенных задач взаимного исключения.

Атомарные переменные, описываемые модификаторами типа atomic или volatile обеспечивают синхронизированный доступ к ОР, выполнение операций над ними выполняется непосредственно в памяти без использования регистров. Кроме того, такие переменные не перемещаются в кэш-память.

На атомарных переменных реализованы неблокирующие операции, поддерживающие взаимодействие потоков и реализующие вида синхронизации тип obstruction-free, lock-free, и wait-free. При этом неблокирующие алгоритмы строятся на атомарных операциях, таких как CAS, RCU. Примером реализации неблокирующих операций являются в Java классы типа AtomicInteger.

Модель посылки сообщений. Временные затраты, связанные с взаимодействием потоков в модели, определяются потерями на передачу данных. Передача сообщений концептуально базируется на примитивах типа Send/Receive. Так как основные потери времени здесь связаны с передачей сообщений, то на этапе планирования взаимодействия следует минимизировать объемы передаваемых данных, а при реализации передачи сообщений использовать преимущества групповых операций, таких как Bcast, Gather, Scatter в MPI.

Оптимизировать передачу данных также можно с помощью неблокирующих операций, таких как ISend/IReceive в MPI. Кроме того, поток, ожидающий прием (передачу) сообщения, может не блокироваться, а выполнять некоторое альтернативное действие. Такой подход реализован, например, в механизме рандеву языка Ада с помощью оператора select.

Выводы. В работе приведены результаты практического исследования эффективности многопотоковых программ, в которых реализованы предлагаемые подходы к оптимизации взаимодействия потоков. Рассматривались различные средства организации взаимодействия потоков, реализованные в современных ЯБПП. Показано что в ряде случаев достигается увеличение коэффициента ускорения до 10-15%.

УДК 004.728.4(043.2)

А. Б. Коцюр
Національний авіаційний університет, Київ

ЦЕНТРАЛІЗОВАНА СИСТЕМА ОБРОБКИ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

Централізована система обробки інформації (ЦСОІ) є основою інформаційної інфраструктури, і надає можливості ефективної роботи мережевих сервісів в мережі підприємства, а так само взаємодію між внутрішньою мережею і зовнішніми інформаційними ресурсами.

Використання ЦСОІ у підприємстві це грамотний спосіб побудови його інформаційної системи, вона забезпечує централізацію апаратних, програмних і керуючих ресурсів. У порівнянні з децентралізованою інформаційною системою впровадження ЦСОІ дозволяє знизити ризики втрати даних в результаті аварій або помилок персоналу. При цьому значно полегшується необхідність забезпечення заходів щодо інформаційної та фізичний захист даних.

Розробка і впровадження даної системи забезпечить автоматизацію роботи компанії, дозволить підвищити точність і оперативність роботи з інформацією.

ЦСОІ забезпечить можливість роботи наступних сервісів інформаційної інфраструктури підприємства:

− файлові сервіси для зберігання інформаційних баз і документів компанії, з можливістю доступу до інформації, як з внутрішньої мережі компанії, так і з мережі Інтернет;

− служба каталогів для зручного централізованого управління обліковими записами користувачів і пов'язаними мережевими ресурсами;

− HTTP-сервер для публікації відкритої інформації на інформаційному порталі підприємства;

− сервіси термінального доступу, для роботи користувачів компанії з внутрішньою інформацією з будь-якої точки світу, за умови доступності мережі Інтернет;

− внутрішня мережа захищена від вторгнень із зовнішньої мережі;

− сервіси резервного копіювання дозволять регулярно зберігати важливу інформацію користувачів в спеціальному сховищі.

Надійність і безперервність роботи даної інформаційної системи обумовлена наявністю відмовостійких систем зберігання даних і мережевих вузлів, наявністю резервного каналу в Інтернет, доступністю мережевих сервісів, підсистеми резервного живлення від джерел безперебійного живлення.

Базові структури ЦСОІ повинні бути захищені від загрози випадкових або навмисних шкідливих дій користувачів, а так само загрози впливу шкідливого програмного забезпечення шляхом прозорої ізоляції від призначеного для користувача сегменту мережі.

У разі зростання підприємства дана інформаційна система дозволить гнучко і ефективно нарощувати обчислювальні потужності, і пропускну здатність мережевих каналів без зупинки роботи і простоїв мережевих сервісів, що особливо актуально для активно зростаючих і розвиваючих підприємств. ЦСОІ повинен забезпечувати ефективну роботу необхідних сервісів, автоматичне відновлення

роботи сервісів в разі апаратних або програмних збоїв, зменшити кількість непродуктивної роботи серверного обладнання.

Для вирішення цих завдань слід також проаналізувати можливість впровадження рішень віртуалізації. Програмне забезпечення для віртуалізації має бути з відкритим вихідним кодом.

Підсистема доступу до зовнішніх мереж (Інтернет) повинна забезпечувати приховування внутрішньої структури мережі, контрольований доступ як локальної мережі в мережу Інтернет, так і користувачів Інтернет і обраним ресурсам централізованої системи обробки інформації. Підсистема повинна забезпечувати гнучку фільтрацію трафіку, захист локальної мережі від зовнішніх мережевих загроз, можливості для управління перенаправленням трафіку в разі зростання підприємства і збільшення кількості зовнішніх мережевих сервісів. Так само підсистема повинна надавати можливості налаштування маршрутизації. Для вирішення цих завдань має бути реалізовано гнучке і зручне управління шлюзом і фаєрволом.

Планування мережної архітектури ЦСОІ здійснюється виходячи з сервісного навантаження ЦСОІ.

При проектуванні обчислювальної мережі ЦСОІ повинні бути виконані вимоги до відмовостійкості на рівні мережевих вузлів, комутації, взаємодії сервісів, сегментації і можливостей масштабування.

Для забезпечення можливості автоматичного відновлення працездатності цих сервісів в разі апаратних або програмних збоїв повинна бути надмірність серверного обладнання.

Збільшення ефективності використання серверного обладнання здійснюється за рахунок застосування рішень віртуалізації. Кластер віртуалізації це безліч систем віртуалізації, що мають загальну систему управління, єдине сховище даних і загальні мережеві ресурси.

Для реалізації можливості створення кластера має бути використано як мінімум два фізичних сервера, що мають відповідну продуктивність і можливості для забезпечення роботи всіх сервісів на одному з них, у разі апаратного або програмного збою іншого сервера. [1-5]

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Дрововозов В.І. Розвиток корпоративної мережі центру високопродуктивної обробки даних / В.І. Дрововозов, М.М. Дидар // Проблеми інформатизації та управління: зб. наук. праць.– К.: НАУ, 2014. – Вип. 1(45). – С. 42- 46.

2. Гоменюк А.Р. Строим центр обработки данных / А.Р. Гоменюк, С.И. Сопенко //Корпоративные системы К. – 2007. – №5. – С.6–11.

3. Медянников М.В. ЦОД в современных условиях / М.В.Медянников // Программные продукты и системы. – М.: ЮНИТИ. - 2002. - 223 с.

4. Басистый Д.А., Кусакин Д.Н.. ЦОД, создаваемый по всем правилам./ Корпоративные системы, №3 (213), 2010.

5. Don Williams, Will Urban. Best Practices when implementing VMware vSphere in a Dell EqualLogic PS Series SAN Environment, [Електрон. ресурс]. – Dell Inc., 2013.

УДК 681.325.59

О. С. Лелека
Національний технічний університет України «КПІ», Київ

ОБЧИСЛЕННЯ ОЦІНОК САМОКОРЕКЦІЇ НА ОКРЕМИХ ВИХОДАХ СУМАТОРА

Проблема достовірності і надійності комп'ютерних обчислень є однією з найважливіших проблем прикладної математики, особливо з урахуванням неминучої обмеженої точності будь-яких вихідних даних. В роботі [1] дається визначення самокорекції як явища, яке полягає у формуванні операційним пристроєм правильних сигналів за умови дії на вхід операндів з детермінованими спотвореннями. Методика оцінки та порівняння самокоригуючих властивостей представлена в роботах [1-2].

В роботі [3] показано можливість зменшення складності обчислень за рахунок використання внутрішньої реалізації логічної мережі при обчисленні достовірності функціонування. Згідно з [1] складність обчислення оцінки автокорекції для комбінаційної схеми, яка сама працює без спотворень, експоненціально залежить від кількості її входів. Тому для кожного виходу суматора n-розрядних чисел вона становитиме 4^{2n} множень з плаваючою комою. Припустимо що вказаний суматор реалізований як два суматори з n і n+1 входом, де розряд переносу від першого суматора подано на вхід до другого. Отримані оцінки достовірності функціонування відповідних розрядів результату будуть такими ж, як і в початковому варіанті, а складність їх обчислення для кожного розряду становитиме 4^n+4^{n+1}. Аналогічні перетворення для нових суматорів не вплинуть на значення автокорецї результату, а складність її оцінки буде змінюватись логарифмічно і врешті після k ітерацій становитиме:

$$\lim_{k\to \log n} 2^k \cdot 4^{\frac{n}{2^k}+1} = 2^{\log n} \cdot 4^{\frac{n}{n}+1} = 16n$$

Теоретично доведено і практично підтверджено, що оцінки достовірності функціонування не залежать від реалізації суматора, тому можна обчислювати ці оцінки для варіанту реалізації, який має найменшу обчислювальну складність. Це твердження стосується складності обчислень довільної комбінаційної схеми.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Тарасенко В.П., Тарасенко-Клятченко О.В. Метод оценки автокорректирующих свойств поразрядных логических операций // Радиоэлектроника и информатика. – 2001. - № 1 (14). – С. 83-86.

2. Тарасенко В. П., Тарасенко-Клятченко О. В. Автокоригуючі властивості логічних операцій / Хмельницький, Вимірювальна та обчислювальна техніка в технологіних процесах, 2001, № 8. – с. 334–337.

3. Клятченко Я.М., О.В. Тарасенко-Клятченко, В.П. Тарасенко, О.К. Тесленко. Достовірність функціонування логічних мереж в умовах дії детермінованих вхідних спотворень// Міжвузівський збірник "Ком'ютерно-інтегровані технології: освіта, наука, виробництво". Луцьк, 2012, №8. – С. 47-52.

УДК 681.142 (043.2)

В. В. Лукашенко, к.т.н.
Национальный авиационный университет, Киев

МЕТОДЫ ПОВЫШЕНИЯ ЭНЕРГОЭФФЕКТИВНОСТИ СЕТИ С ТОЛЕРАНТНОСТЬЮ К ЗАДЕРЖКАМ ДЛЯ ПРИМЕНЕНИЯ В СИСТЕМАХ ДАЛЬНЕЙ КОСМИЧЕСКОЙ СВЯЗИ

Основными тенденциями развития систем дальней космической связи являются [1]:

– рациональное использование частотного ресурса;

– энергосберегающие технологии доставки данных потребителям;

– обеспечение требуемого уровня помехозащищенности и электромагнитной совместимости по мере увеличения количества одновременно работающих космических аппаратов.

Перечисленные задачи являются все более актуальными по мере усложнения программ исследования дальнего космоса, повышения требований к скорости передачи данных при соблюдении безусловных гарантий доставки. В работе [2] рассчитаны характеристики обнаружения сигналов в системе дальней космической связи, построенной по принципу "Межпланетного Интернета". Выражение для отношения сигнал/шум имеет следующий вид:

$$\frac{P_{\text{ï ðì}}}{N_{\text{ø}}} = \frac{P_{\Sigma} G_{\Sigma} G_{\text{ï ðì}} \lambda^2}{\left(4\pi r\right)^2 k_B T_0 \Delta f \cdot k_{\text{ø}} L_s}, \qquad (1)$$

где $k_B = 1{,}38 \cdot 10^{-23}$ (Вт/Гц)·°К – постоянная Больцмана; T – абсолютная температура источника излучения, °К; $k_{\text{ø}} = \frac{P_{\text{ï ðì}} / k_B T \Delta f}{\left(P_{\text{ï ðì}} / N_{\text{ø}}\right)_0}$ – коэффициент шума приемника; Δf – эквивалентная шумовая полоса пропускания приемника; $P_{\text{ï ðì}} / N_{\text{ø}}$ – отношение мощности сигнала, вычисляемой по формуле $P_{\text{ï ðì}} = \frac{P_{\Sigma} G_{\Sigma} G_{\text{ï ðì}} \lambda^2}{\left(4\pi r\right)^2}$, к мощности шума, приведенной ко входу приемника; L – множитель потерь для системы связи в целом.

Выражение (1) имеет простую и удобную форму для анализа затрат частотного и информационного ресурса. При передаче большого объема разнородных данных измерений и экспериментов с орбитальных станций и космических спутников, включая, в том числе, Интернет-трафик, наблюдаются существенные задержки во времени прохождения сигнала от передающего устройства спутниковой станции до принимающего устройства на Земле. Кроме того, общий разнородный трафик уже не может быть описан моделями Пуассона или Эрланга. Он обладает выраженными самоподобными свойствами [3]. На рис. 1 изображены графики зависимости вероятности обнаружения от квадрата дальности для сигнала с гауссовским распределением и сигнала с распределением Парето. Для наглядности те же графики изображены на рис. 2 в логарифмической шкале.

Видно, что при увеличении дальности вероятность обнаружения сигнала с распределением Парето убывает медленнее, чем сигнала с нормальным (гауссовским) распределением.

Введем нормализованную дальность $r_{\text{norm}} = r/r_{\max} = m^{-0,5}$, где переменную m можно рассматривать как отношение текущей и максимальной мощностей сигнала на соответствующих дальностях. Величина r_{norm} может рассматриваться как коэффициент, учитывающий уменьшение дальности связи по сравнению с максимальной вследствие вероятностного характера процесса связи.

Видно, что при передаче самоподобного сетевого трафика вероятность обнаружения сигнала убывает медленнее, чем при передаче пуассоновского трафика. Однако расход частотного ресурса сети при передаче самоподобного трафика, естественно, будет выше.

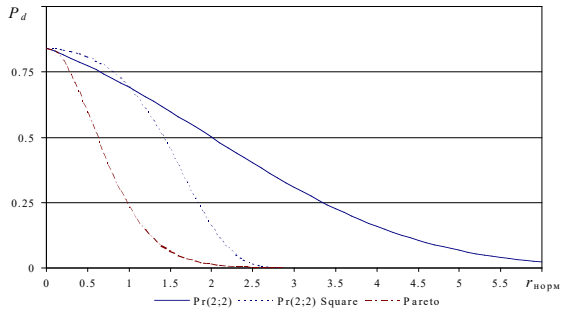

Рис. 1 Зависимости вероятности обнаружения от квадрата нормализованной дальности. Отношение сигнал/шум по мощности равно 4

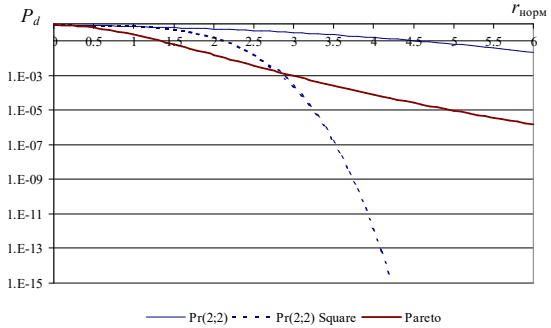

Рис. 2 Зависимости вероятности обнаружения от квадрата нормализованной дальности (логарифмическая шкала). Отношение сигнал/шум по мощности равно 4

Используя приведенные выше формулы, уравнения и графики, можно рассчитывать потребную мощность передающих устройств, число и чувствительность приемных устройств, при которых обеспечивается требуемая вероятность доставки сообщений.

УДК 621.395.7 (043.2)

V. I. Nadtochiy, Candidate of Technical Science
National Aviation University, Kyiv

INTERNATIONAL CONFERENCE ON THE DESIGN OF RELIABLE COMMUNICATION NETWORKS

The International Conference on Design of Reliable Communication Networks (DRCN) is a forum for presenting excellent results and new challenges facing the field of the reliability and availability of communication networks and services. It brings together experts from industry, governments and academia, experienced in engineering, design and research.

DRCN is an event that has been set up to provide a forum of presentations and discussions of recent developments and future trends in communication networks and network subsystems, focusing on all aspects of network reliability.

The conference has been held since 1998, in the beginning biannually, and more recently annually. Over the past eighteen years, DRCN has developed into a well established conference covering topics from equipment and technology for survivability to network management and public policy; through theory and techniques for the design, management and operation of survivable and robust networks. The 12th DRCN has been held in Paris.

The DRCN conferences is technically sponsored by the IEEE Communications Society. It is endorsed by many IEEE ComSoc Technical Committees (Internet, Communications Quality and Reliability, Optical Networking, Networks and Operations Management, Transmission Access and Optical Systems) and the International Teletraffic Congress.

Prospective authors are invited to submit original technical papers by the deadline Conference Proceedings and for oral presentation during the conference. The IEEE reserves the right to exclude a paper from distribution after the conference if the paper is not presented at the conference.

Papers are reviewed on the basis that they do not contain plagiarized material and have not been submitted to any other conference at the same time (double submission). These matters are taken very seriously and the IEEE Communications Society will take action against any author who has engaged in either practice.

The DRCN conference offers a rich program, including keynote talks, regular papers and panels, together with free state-of-the-art tutorials. Conference needs author's contribution and participation to make it a successful event and the best paper award will be granted.

Disasters can strike anywhere at any time and may strike your company or the community you live. Disasters may be man-made such as terrorist attacks potentially through large security system attacks or may be technological such as power grid blackouts, dam failures, nuclear accidents, etc. Disasters may be natural phenomenon (hurricanes, earthquakes, tsunami, tornados, floods, forest fires, or even pandemics). Disasters can affect thousands of people, multiple communities, entire countries, or just one company. When a catastrophic disaster happens in a region, the population can lose completely their means to communicate - wireless and wireline - until the telecom

networks can be restored. That isolation can put lives and livelihoods at risk especially under disaster conditions.

The panel objective is to address how the recent advances in network control and system recovery can support the management of "Disasters" within network contingency planning and can restore user communications following massive network infrastructure destructions. The discussion will try to provide a comprehensive state of the art in network systems, control and management architectures, security, standardization and regulation for Network Disaster Management and Recovery.

The items that can be addressed are and are not limited to:

What are the needs of network infrastructure emergency preparedness for global recovery? Which essential actions are needed to be properly prepared for emergency?

How the recent advances in elastic optical network systems (spectrally and/or spatially flexible systems) can overcome complete communication outages?

Are programmatic transport networks (SDN) and network virtualization (NFV) able to integrate the control application of the network disasters and their recovery? How these recovery procedures can synergize for safe wireless and wireline ad-hoc network infrastructures?

What are the security requirements from large institutions e.g. governments, multi-national business organizations, to small and mid-size enterprises, the Telecom network infrastructures must face to?

What is the impact on the required maintenance of Emergency Network Operations Centers to recover from Network Disasters? What are the efforts to maintain such network disaster plans?

How are governments and public institutions organized to manage and recover from Telecom Network Disasters? What are the agreements that must be in place to overcome network disasters?

How are the members of standard bodies organized to address network disaster recovery? Are recent network control architectures considering the challenges of disaster recovery plans?

New approach to disaster management and network design to minimize probability of encountering disasters to avoid dynamically forecasted disasters.

Unpredictability is a fact of life. Whether terrorist attacks, cataclysmic weather, networks never know when their operations may be threatened.

Network Modeling allows multiple Virtual Networks to coexist on a single physical substrate in isolation from each other, i.e., without security or performance interferences. It has been propounded as a diversifying attribute of the future inter-networking paradigm that can enable seamless integration of new features resulting in a more rapid evolution of the Internet architecture.

Riverbed Network Modeling Complex provides disaster management and network design, end-user support, application and network performance management and centralized control. Using network models drastically reduces the time and effort required to develop, deploy, and ensure network application performance and assessment of Design Reliability of Communication Networks. Network Modeling allows multiple Virtual Networks to coexist on a single physical substrate in isolation from each other, i.e., without security or performance interferences.

УДК 004.274

В. М. Опанасенко, д.т.н.
Институтут кибернетики НАН Украины, Киев,
Э. Э. Эсонов, к.т.н.
Ташкентский государственный технический университет, Узбекистан

РЕАЛИЗАЦИЯ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ С КОМПЛЕКСНЫМИ ЧИСЛАМИ НА FPGA

Решение широкого круга задач требует использования арифметических операций над комплексными числами [1], для аппаратной реализации которых в настоящее время используются кристаллы типа FPGA (Field Programmable Gate Array) [2]. Аппаратные реализации представляются функциональными IP-блоками, которые можно встраивать в новые проекты и они, как правило, независимы от технологии изготовления FPGA [3].

Предложена и рассмотрена структурная организация IP-блоков, реализующих арифметические операции над комплексными числами (16- и 32-разрядные), построенных на основе кристаллов FPGA серии Virtex–5 (XC5VLX30-3FF676).

IP-блок сложения/вычитания двух комплексных чисел одновременно формирует результат действительной и мнимой части и реализован на основе модуля LUT (Look-Up-Table).

IP-блок для реализации операций умножения и деления использует модули DSP48E с одновременным получением результата действительной и мнимой части на двух выходах.

Аппаратные (количество Slices, триггеров (FF) и LUT) и частотные оценки (тактовая частота) IP-блоков арифметических операций над комплексными числами приведены в таблице.

Таблица. Аппаратные и частотные оценки блоков арифметических операций

Тип операции	Разрядность операндов, бит	Количество модулей, шт				Частота, МГц
		DSP48E	Slices	FF	LUT	
сложение/ вычитание	16	2	24	96	32	525
	32	8	56	192	64	455
умножение	16	3	30	64	48	147
	32	12	88	256	224	90
деление	16	6	360	398	964	180
	32	28	1232	806	1230	120

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Акушский И.Я., Амербаев В.М., Пак И.Т. Основы машинной арифметики комплексных чисел. – Алма-Ата: Наука, 1973. – 192 с.

2. Palagin A.V., Opanasenko V.N. Reconfigurable computing technology— «Journal Cybernetics and Systems Analysis», №5, 2007. pp. 675–686.

3. Palagin A.V., Opanasenko V.N. Design and application of the PLD-based reconfigurable devices //In: Design of Digital Systems and Devices, vol. 79. Springer, Verlag, Berlin, Heidelberg, 2011. – pp. 59–91.

UDC 519.852.35:004.7 (043.2)

N. K. Pechurin, doctor of science
National Aviation University, Kiev,
L. P. Kondratova,candidate of science
National Technical University of Ukraine "KPI", Kiev,
S. N. Pechurin, candidate of science

THE MODEL DISTRIBUTING COMPUTER RESOURCES IN A WIRELESS NETWORK

When exchanging computing resources via computer networks, using the airwaves as communication media, having limited capacity, a special place belongs to the function calculating the effective plan of the local computing resource allocation. The traditional ISO model of network management system implies the ability to manage data flows in the network, with the increase of the effectiveness of management procedures is achieved due to the services of the performance management, configuration management, account management, fault tolerance management, failure-free operation [1]. Here, as the criteria there are used to prevent the reduction in efficiency due to network congestion buffering tools, forcible reduction of the data rate, the introduction of windows, "prescribed" at the lower levels of OSI/ISO model, which correspond to the maximum network components bandwidth, the minimum value of the average time of reaction to the request network and a similar [2]. To reduce the criterial gap in a multilevel hierarchical model there is proposed the complex model to distribute the computing resources based on the classical formalizations of flow distribution in an abstract networks. There is considered a network presented as the bi-oriented graph of $G=(V,E)$ with V node set of basic computing resources localization. The set of V is complemented by the workstations representing pairs of $s_i,t_i \in V$sources and sinks, and a workstation, representing a common source of s_0 to transmit the computational resources to s_i nodes. The basic and working network stations are connected by arcs of E set with weights characterizing buffering and window technology parameters for flow control, the channel capacity, the cost to transport protocol data unit. The objective is to plan for calculating the distribution of computational resources between nodes of $s_0,s_i \in V$ with minimizing the cost of the flow transmit, maximizing the flow in the network. The method resolving flow problems is based on to reduce them to the problems described by the linear programming model with using the block programming tools of Danzig-Wolfe [3]. Plan computing resource allocation on the basis of mathematical programming universal tools increases the flexibility of the represented complex model.

REFERENCES

1. Руководство по технологиям объединённых сетей: Пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 1040с.

2. Рошан П., Лиэри Д. Основы построения локальных беспроводных сетей стандарта 802.11.:Пер. с англ.–М.:Изд. дом «Вильямс»,2004.– 304 с.

3. Marco E.Lübbecke, Jacques Desrosiers. Selected Topics in Column Generation // Operations Research. – 2005. - Vol. 53, No. 6.- P. 1007–1023.

УДК 004.05

В. А. Романкевич, к.т.н
А. Л. Дейнеко
Национальный технический университет Украины "КПИ", Киев

МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ НЕСТАНДАРТНЫХ МНОГОПРОЦЕССОРНЫХ СИСТЕМ В ПОТОКЕ ОТКАЗОВ

Отказоустойчивые многопроцессорные системы (ОМС) с каждым годом получают все большее распространение. Это связано с расширяющейся областью их применения, в первую очередь в системах управления сложными и ответственными объектами (самолеты, ракеты, космические объекты, сложные технологические процессы, финансовые расчеты и др). При этом для вычислительных систем характерны большое количество процессоров и регулярность их структуры. Для систем управления характерно сравнительно меньшее количество процессоров (десятки, сотни, иногда тысячи) и относительная нерегулярность структуры, что связано, как правило, с большим количеством источников информации различного типа (датчиков) и разнотипностью процессоров. Последнее усложняет задачу расчета параметров системы, в частности, надежности. Различают ОМС базовые (устойчивые к любым отказам, кратность которых не превышает заданной величины) и небазовые. Отметим, что задачу расчета надежности ОМС нельзя назвать простой, хотя бы потому, что широко распространенные методы расчета надежности к ним неприемлемы: система может отказать при появлении i отказов и, в то же время, быть работоспособной при появлении j отказов, где $j>i$. Для базовых ОМС методы расчета вероятности безотказной работы известны. Однако реально встречающиеся системы далеко не всегда являются базовыми. Более того, во многих случаях разработчик вынужден использовать разные процессоры, которые не всегда могут заменять друг друга, не могут брать на себя функции управления отказавшего процессора, что весьма серьезно усложняет задачу реконфигурации системы. Для них применяются статистические методы, основанные на выполнении экспериментов с моделями, отражающими реакцию ОМС на появление отказов. В качестве таких моделей, то есть моделей поведения ОМС в потоке отказов используются GL-модели, отличающиеся универсальностью. GL-модель представляет собой граф с булевыми функциями, приписываемыми ребрам графа. Переменными функций являются состояния процессоров (отказал - работоспособен). Если функция принимает нулевое значение, соответствующее ребро пропадает, а связность графа отражает состояние ОМС. В докладе описывается модель, которая позволяет учитывать, что не все процессоры взаимозаменяемы. Понятно, что она очень часто не является базовой, поскольку должна отражать поведение системы, которая по-разному может реагировать на появление отказов одинаковой кратности. Множество процессоров разбивается на подмножества, в каждом из которых все процессоры способны подхватывать функции отказавшего процессора, а также подмножества, куда входят процессоры, способные выполнять функции процессоров разных подмножеств. Предлагается способ построения GL-модели, отвечающей описанным условиям, которая состоит из нескольких подмоделей, и отмечаются ограничения для случаев, когда подмодели могут быть базовыми.

УДК 621.3

O. V. Rusanova
National Technical University of Ukraine "KPI", Kiev

SCHEDULING PROBLEMS FOR CLUSTERS - AN OVERWIEW

Today the supercomputers progress is connected with development of clusters. Analysis of the last 46th edition TOP -500 shows that the increasing performance is achieved by using of multi-core nodes and growth the total cores number in the clusters. Thus, last year the average number of cores in the clusters increased on 12,308 (or 26.6%). This increase the cores number leads to significant complications solving the problem of efficient resources using in cluster systems. For example, the effectiveness of the most powerful systems in the world Tianhe-2 equals to 0.62. More efficient resources using associated with the improvement of scheduling methods.

The scheduling problem belongs to NP-complete class. Therefore we concentrate our activity on different heuristics. The main heuristics types, such as genetic, list, cluster and duplication are discussed and analyzed. Last effective scheduling methods use hybrid approaches that allows to combine the advantages of different algorithms. The most effective scheduling algorithms such as *HGAHS* [1] – hybrid of genetic and list approaches, *SHTSA* [2] – hybrid of duplication and list approaches, *SAMCS* [3] – hybrid of duplication and cluster approaches are discussed, compared and analyzed. These algorithms don't support different topologies of cluster systems. They can be used only for fully connected systems. More over, only *SAMCS* algorithm takes into account multi-core architecture of clusters.

The initial data, results and optimization criterion are discussed in this paper. All wellknown approaches use application model as a directed acyclic task graph. *HGAHS* and *SHTSA* approaches use also prosessors number while *SAMCS* algorithm use nodes number and their core quantity. As a result of scheduling all algorithms use Gantt Chart. All scheduling approaches use as a optimization criterion minimal scheduling length or makespan of a given application on clusters. We propose consider cluster as a hierarchical system with given topology that consists of multi-core nodes. A model of such a cluster system can be represented as a directed graph system. The vertexs of this graph correspond to nodes of the system, and edges - communication links between them (the topology of the system). Each vertex of the graph is characterized by number and cores quantity for the node of system. Graph edges are characterized by a weight that determines the throughput capacity for data transfer.

Results of our paper can be used in advanced scheduling approaches for multi-core clusters.

REFERENCES

1. *Kamaljit Kaur. Heuristics Based Genetic Algorithm for Scheduling Static Tasks in Homogeneous Parallel System // Department of Computer Science & Engineering, Guru Nanak Dev University, Amritsar- 143001, Punjab, India, IJCSS, vol.4, pp.183-198, 2010.*

2. *Yanyan Dai. A Synthesized Heuristic Task Scheduling Algorithm // Institute of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China, 2014. – P. 67.*

УДК 004.056.5 (043.2)

М. О. Семенюк
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СТЕГАНОГРАФІЇ У МЕРЕЖЕВІЙ ТЕХНОЛОГІЇ

Під мережевою стеганографією мається на увазі методи, в котрих стеганографічним контейнером є інформаційний пакет, що передається в мережі. Типові методи мережевої стеганографії включають в себе зміну властивостей одного з протоколів мережі. Ретрансмісія *TCP/IP* трафіку забезпечує надійну доставку інформаційних пакетів в разі їх спотворення або втрати. Одним з недоліків TCP протоколу є ресурсоємність.: *«трійний хендшейк»,* передача даних та відновлення сесії, постійний контроль над станом віртуального каналу даних, закриття сесії. Протокол TCP є більш придатним для реалізації стеганографічного каналу на транспортному рівні.

Метод мережевої стеганографії побудований на ретрансмісії протоколу TCP дозволяє реалізувати приховану передачу даних всередині пакетів протоколу, що, начебто, призначені для виправлення невдало переданих даних. Отримувач приймає початковий пакет та відправляє повідомлення про не вдалу доставку. Відправник відправляє той же пакет знову, замінюючи первинну інформацію інформацією призначеною для прихованої передачі. Так як цей пакет має той самий ідентифікатор, що і попередній, то системи, призначені для аналізу мережевого трафіку, вже не перевіряють повторний пакет. Повторно переданий пакет з секретними даними не відрізняється від початкового для всіх систем мережевого захисту. При отриманні повторно переданого пакету з нього вилучається секретна інформація.

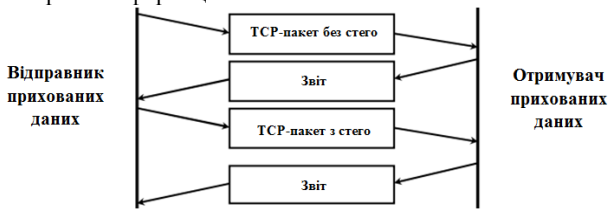

Рис. 1. Принцип функціонування ретрансмісії стеганографії.

Недоліком цього методу є мала пропускна спроможність, так як кількість ретрансмісій значно збільшується у порівнянні з середнім значенням для мережі, що сягає до 0,1% від усього трафіку. Коли доля ретрансмісія в мережі досягає 1-2% порушується коректне функціонування протоколу TCP. Потрібно володіти середньо-статичними характеристиками мережі для реалізації цього методу, що б вдало налаштувати механізм стеганографічної пересилки, не виділяючи з'єднання серед інших в мережі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Hiding Information in Retransmissions. Wojciech Mazurczyk, Milosz Smolarczyk, Krzysztof Szczypiorski. [Електронний ресурс] – Режим доступу: https://arxiv.org/ftp/arxiv/papers/0905/0905.0363.pdf

УДК 004.4:378.4 (043.2)

Ю. І. Сінько, к.пед.н.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ В ЗАКЛАДАХ ОСВІТИ

Опис проблеми

Сьогодні без використання сучасних інформаційних технологій не може ефективно працювати жодний освітній заклад. При цьому зміст і розвиток власної ІТ-інфраструктури при кожному освітньому центрі обходиться дуже дорого. З кожним роком рівень таких витрат все більше і більше зростає. Установи витрачають великі суми на комп'ютерну техніку, телекомунікаційне обладнання та програмне забезпечення. Крім вищевказаних витрат значні фінансові вкладення потрібні і для підтримки високого рівня професіоналізму цих співробітників.

"Хмарні обчислення" (Cloud computing) є хорошою альтернативою класичній моделі навчання. Головним її плюсом можна вважати істотну економію коштів освітньої установи, в якому вони використовуються. Адже в цьому випадку комп'ютерна інфраструктура і/або інформаційні сервіси надаються як послуги "хмарного" провайдера. Документи, електронні листи, програми та інші дані учасників освітнього процесу зберігаються на віддалених серверах провайдера. При цьому для установи немає необхідності утримувати власну дорогу ІТ-інфраструктуру і переплачувати за обчислювальні ресурси, які в більшості випадків не задіяні на повну потужність. Єдине, чим необхідно забезпечити викладачів і студентів з використанням хмарних технологій, - це доступ до мережі Інтернет.

Сьогодні є безліч постачальників хмарних рішень. Такі великі компанії як Amazon, Google, Microsoft та ін. пропонують значні знижки освітнім установам, за рахунок чого вони отримують доступ до хмарних сервісів практично безкоштовно.

Надійність, доступність і легке розповсюдження є ключовими перевагами хмарних технологій. Чи може все це означити, що незабаром більшість освітніх послуг надаватиметься на базі хмарних обчислень? Чи призведе це до повної відмови освітніх установ від власних громіздких ІТ-інфраструктур?

Тому є потреба поставити за мету розглянути і оцінити всі переваги і недоліки використання хмарних обчислень в сфері освіти, а також дати практичні рекомендації щодо застосування хмарних обчислень в процесі навчання як в школі, так і в ВНЗ.

Застосування хмарних обчислень в освіті

Однією з перших хмарних послуг, яку стали використовувати європейські освітні установи, стала електронна пошта. Забезпечення працездатності (аутсорсинг) сервісу електронної пошти - нескладне завдання, яке безумовно не відіграє ключової ролі в роботі освітнього закладу. Корпорації Google і Microsoft надають співробітникам і учням освітніх установ доступ до електронної пошти безкоштовно.

Крім послуг електронної пошти ці корпорації забезпечують можливість використовувати в хмарі функції стандартного офісного пакету для спільної роботи з електронними документами, таблицями та для створення презентацій. Хмарні сервіси для освітніх організацій Google Apps for Education і Microsoft Office 365 for education дозволяють використовувати вбудовані системи для обміну миттєвими повідомленнями, календарі для спільного планування та загальні адресні книги. Кожен користувач хмарних систем отримує значний дисковий простір для зберігання будь-якої інформації, яка була отримана в результаті роботи з хмарою.

Може здатися дивним, що ці послуги надаються освітнім установам безкоштовно, в той час як для комерційних організацій ціни на програмне забезпечення як були, так і залишаються традиційно високими. Така цінова політика пояснюється наступним чином. На сучасному ринку хмарних технологій зберігається висока конкуренція між постачальниками програмного забезпечення, тому вони намагаються надавати свої сервіси освітнім установам безкоштовно. Розрахунок іде на майбутніх випускників, які після отримання освіти влаштуються на роботу і зможуть переконати майбутніх роботодавців придбати програмний продукт, про переваги якого вони вже знають. Також це забезпечить прихильність і лояльність користувачів до продуктів певної марки і її впізнаваність і популярність.

Якщо для освітнього закладу безпека доступу до даних не є пріоритетним напрямком, тоді може виявитися вигідним використання низькорівневих IaaS-сервісів як систем зберігання даних, наприклад для відео- і аудіоматеріалів.

Для деяких освітніх установ може виявитися вигідним переміщення в "хмару" внутрішніх систем управління навчанням (LMS, Learning Management Systems). Це хороша можливість для таких установ, які не можуть дозволити собі покупку і підтримку дорогого устаткування і програмного забезпечення, що дозволяє оптимізувати витрати на IT-інфраструктуру в сучасних посткризових умовах.[1-2]

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Allen M.W. Designing Successful e-Learning. John Wiley & Sons Inc, 2008. – ISBN 978-0-7879-8299-7. – 240 p.

2. Chao L. Cloud Computing for Teaching and Learning: Strategies for Design and Implementation. University of Houston-Victoria, 2012. – ISBN 978-1-4666-0957-0. – 357 p.

УДК 004.056.3

І. А. Терейковський, д.т.н.
Національний технічний університет України «КПІ», Київ

ПРО РОЗПІЗНАВАНЯ КІБЕРАТАК НА ВЕБ-СЕРВЕР СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

Однією із найбільш відповідальних компонент захисту інформації веб-серверу системи дистанційного навчання (СДН) є системи виявлення кібератак багато з яких функціонують на основі шаблонів нормальної поведінки (ШНП) [3]. Важливим недоліком сучасних ШНП є недостатня пристосованість до складних нестаціонарних процесів зміни функціональних параметрів веб-серверів СДН [2]. Виправити ситуацію пропонується за рахунок розробки нестаціонарної марківської моделі (ММ) ШНП. Проведені дослідження вказують, що для досягнення достатньої точності оцінки параметрів достатньо використати ММ з двадцятьма станами в якій можливі переходи між трьома сусідніми станами. Для врахування не стаціонарності динаміки параметрів піддослідний часовий діапазон слід розділити на ряд стаціонарних інтервалів, кожен з яких можливо моделювати окремою стаціонарною ММ. Визначити межі вказаних стаціонарних інтервалів можливо застосувавши методи теорії вейвлет-перетворень [1]. Таким чином кожна окрема ММ буде моделювати або монотонно зростаючий, або монотонно спадаючий процес. При моделюванні зростаючого процесу в системі рівнянь Колмогорова-Чепмена слід використовувати рівняння виду (1), а при моделюванні спадаючого процесу рівняння виду (2).

$$P_k(t) = P_k(t-1) - \sum_{j=1}^{3} \left(P_k(t-1) p_{k,k+j}\right) + \sum_{i=1}^{3} \left(P_{k-i}(t-1) p_{k-i,k}\right), \quad (1)$$

$$P_k(t) = P_k(t-1) - \sum_{j=1}^{3} \left(P_k(t-1) \times p_{k,k-j}\right) + \sum_{i=1}^{3} \left(P_{k-i}(t-1) \times p_{k+i,k}\right), \quad (2)$$

де $P_k(t)$ – ймовірність перебування процесу в k–му стані в момент часу t,

$p_{k,j}$ – ймовірність переходу із k–го стану в j-ий стан за один крок процесу.

Результуючу нестаціонарну марківську модель можна представити як суперпозицію описаних ММ. Власне розпізнавання кібератаки здійснюється на основі допустимого відхилення реальної величини параметру від ШНП. Для цього можливо використати методи теорії нейронних мереж.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.Дьяконов В.П.Вейвлеты. От теории к практиве / В.П. Дьяконов. – М. : Солон, 2006. – 440 с.

2.Менаске Д. Производительность Web-служб. Анализ, оценка и планирование / Менаске Д., Виргилио А. ; пер. с англ. – СПб. : ДиаСофтЮп", 2003. – 480 с.

3. Терейковский И. А. Моделирование профилей нормального поведения компьютерных систем / И. А. Терейковский // Защита информации: сб. науч. трудов НАУ. – 2006. – Выпуск 13. – С. 103–108.

УДК 004.27

В. В. Ткаченко, к.т.н.,
О. В. Опанасюк,
М. В. Вакуленко
Національний технічний університет України «КПІ», Київ

ЗАСОБИ ПРИСКОРЕННЯ РЕКОНФІГУРАЦІЇ В РЕКОНФІГУРОВАНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Для реконфігурованих обчислювальних систем час виконання обчислень є критичним параметром зважаючи на його високу непродуктивну складову, що може бути порівняна у часі з апаратним прискоренням, зводячи нанівець весь позитивний ефект від здійснення реконфігурації архітектури [1]. Таким чином, зменшення накладних видатків часу реконфігурації є актуальною задачею, що вирішується в даній роботі. Розроблено програмну модель реалізації методу прискорення реконфігурації, що заснований на технології повторного використання ресурсів функціональних блоків апаратних задач.

Досліджені обчислювальні алгоритми, що відповідають моделі обчислень під управлінням потоку даних. В роботі реалізований алгоритм визначення критичного часу виконання алгоритма, запропонований в роботі [2]. На підставі аналізу потомків кожної вершини формується завчасна черга реконфігурації функціо-нальних блоків апаратних задач. Задачі, що були вже зконфігуровані на поверхні обчислювальної площини ПЛІС зберігаються для подальшого використання.

Алгоритм пошуку критичного шляху заснований на побудові матриці зв'язності графу. Нехай модель М-програми [2] подана графом $C=(V,E)$, де V – множина вершин, які є макрозадачами (М-задачами); E – множина дуг, при цьому дуга $e\in E$ поєднує М-задачі M_1 и M_2, якщо між ними є співвідношення за даними або за управління; v – кількість вершин графу C, w – кількість ярусів графу C; $W_j \mid (j=\overline{1,w})$ – поточний ярус; n_j – кількість вузлів на ярусі W_j.

Під час опису графу програми в вигляді матриці зв'язності M_C розмірності $(v\times v)$, рядки $M_C[g]\Big| g=\overline{1,v}$ відповідають виконуваним задачам. В стовпцях $M_C[k]\Big| k=\overline{1,v}$ кожного рядку $M_C[g]$ розміщується одиниця, якщо задача $Task_g$ готує дані для задач $Task_k$. Отримати множину всіх задач які готують дані для задачі $Task_k$, можна проаналізувавши елементи стовбця $M_C[k]$, в якому номери g елементів стовбця $M_C[g,k]$ вказують на номери задач $Task_g$, якщо $M_C[g,k]=1$. Алгоритм пошуку критичного маршруту маршруту для оцінки часу обчислень наведений далі:

```
for (g=0; g=v; g++) do                  / аналіз рядків матриці зв'язності
{for (k=0; k=v; k++) do                 / аналіз елементів рядку
   {if MD[g, k] = 1 do Qg:=MD[g, k]; / формування масиву нащадків
```

```
    T_i_max:= max{Q_g};          / нащадок з максимальним часом виконання
    W[k]:=i_max;                 / формування критичного шляху
    }
T_D:=T_D+T_i_max;                / розрахунок критичного часу виконання алгоритму
}
```

На рис.1. а, б зображені порівняльні залежності виконання обчислювального алгоритму без прискорення реконфігурації (Рис.1. а), а також із застосуванням технологій прискорення реконфігурації, таких як завчасна реконфігурація і видалення повторного заваттаження (Рис.2.а). За результатами експериментів отриманий усереднений показник прискорення близько 10%. Визначено, що ефективність розробленого алгоритму залежить від збільшення кількості повторень однотипних задач і від ширини графа алгоритму.

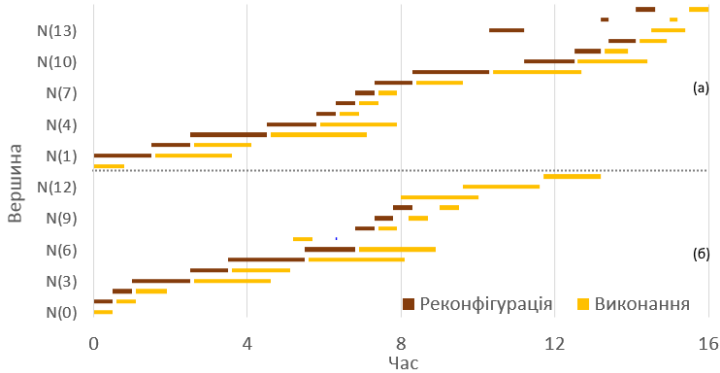

Рис. 1. Часова діаграма виконання обчислювального алгоритму

Таким чином в роботі досліджені засоби скорочення киритичного часу виконання обчислювального алгоритму, поданого потоковим графом. Досліджені механізми прискорення реконфігурації, які призводять до скорочення критичного шляху графу алгоритма. Визначено, що запропонований спосіб найбільш єфективний під час статичного аналізу графу алгорима, в той час як в динамічному режимі виникають непередбачені часові затримки, пов'язані з необхідністю аналізу всіх можливих шляхів графу алгоритму, в пошуку найкоротшего.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Клименко І.А. Класифікація реконфігурованих обчислювальних систем І.А. Клименко, М.В. Рудницький // Інформаційні технології та комп'ютерна інженерія. – Вінниця: КІВЦ ВНТУ, 2014. – №5 (116). – С. 120 – 128.

2. Луцький Г.М. Зменшення накладних видатків реконфігурації в реконфігурованих обчислювальних системах / Луцький Г.М. Клименко І.А. // Штучний інтелект. – К.: Наука і освіта, 2015. – №1 – 2(67 – 68). – Р. 146 – 156.

УДК 004.272.3

В. Ю. Ткаченко,
Р. Ю. Ткаченко
Національний технічний університет України «КПІ», Київ

СОЗДАНИЕ АЛИЗАТОРОВ ПРОГРАММНОГО КОДА .NET

При разработке программных продуктов часто возникает необходимость следить за качеством кода, находить потенциально опасные места, которые могут ухудшить производительность кода, или даже привести к сбоям работы вычислительной техники, например, по причине нехватки оперативной памяти.

Рассмотрим тему создание анализаторов программного кода на примере очень распространенной ошибки в C#, допускаемой разработчиками. В .Net настоятельно рекомендовано (но не обязательно) уничтожать объекты, которые реализуют интерфейс “IDisposable”, так как стандартный сборщик мусора делает это не сразу после выхода из метода, где этот объект был создан, а спустя какое-то время. И если такой объект имеет большой размер, и метод, где он создается вызывается много раз во время работы программы, непременно возникнут проблемы нехватки оперативной памяти на вычислительной машине. При написании кода многие разработчики не используют метод «Dispose» либо конструкцию «Using» для таких объектов, который «говорит» сборщику мусора заняться уничтожением объекта, когда будет достаточно ресурсов, чтоб совершить это действие. Часто на проектах проводят, так называемый, «рефакторинг» программного кода, когда опытный разработчик просматривает весь код, пытаясь найти ошибки подобные описанной выше. Но просматривать десятки, а то и сотни строк кода, задача сложная и требующая больших временных затрат. Поэтому существует огромное количество различных анализаторов кода, которые просматривают код и демонстрируют свои замечания к коду.

Анализатор кода – это программа, которая на входе принимает список файлов с программным кодом и список правил, которые необходимо проверить (применить), а на выходе получает список ошибок и координат этих ошибок в файлах программного кода. Список ошибок должен формироваться путем применения правил к коду. То есть правило – это метод, который принимает во входящих параметрах, например, файл с кодом и ищет в нем лексические, синтаксические или семантические ошибки. Нас интересуют только поиск семантических ошибок, так как с двумя первыми прекрасно справляется компилятор, но это не мешает нам писать правила, которые будут требовать, например, определенного оформления кода или написания комментариев.

Для .Net самые популярные - это FXCop [1] и StyleCop [2]. Эти анализаторы имеют большое количество списков правил для анализа кода, имеют возможности гибкой настройки использования этих правил. Также есть возможность дополнять списки правил, дописывая специальные компоненты. Возможность дополнять правила, очень актуальна, так как сейчас существует огромное количество сторонних библиотек, которые используются при разработке, содержащие классы которые должны быть использованы строго определенным образом, с определенной грамматикой для обеспечения их правильного функционирования.

FXCop и StyleCop не способны найти многие ошибки по причине отсутствия соответствующих правил, особенно для использования сторонних библиотек. Именно о создании анализаторов кода и правил для них и пойдет речь.

Но все же вернемся к нашему примеру. В библиотеке «Microsoft.Sharepoint» существуют два COM объекта «SPSite» и «SPWeb». Они имеют оболочку, написанную на C#, которая реализует интерфейс «IDisposable». Существует огромное количество ситуаций, когда эти объекты неявно создаются и программисты забывают их уничтожать [3]. Пока не существует работающего анализатора кода в открытом доступе, способного проанализировать эти ситуации. Поэтому было принято решение написать свой анализатор кода. Наиболее удобным вариантом использования анализатора кода является его вызов из среды разработки (в данном случае Visual Studio). Поэтому было написано расширение к Visual Studio, которое вызывается из контекстного меню и выводит ошибки и замечания в окно списка ошибок в Visual Studio.

В разработки правил для анализатора использовалась теория создания компиляторов. Из входящих данных в виде программного кода формируется дерево разбора, над которым проводиться семантический анализ. До недавних пор не существовало готового решения для того, чтобы получить дерево разбора .Net кода, так как это требовало бы огромных усилий. Но недавно Майкрософт разработали новый компилятор .Net, который находиться в открытом доступе, имеет открытый код, написанный на C# и называется «Roslyn» [4]. Используя компоненты «Roslyn» строиться дерево разбора над которым проводиться семантический анализ. В ходе семантического анализа проверяются синтаксические конструкции, называющиеся «Object creation statement» и другие, которые создают объекты классов «SPSite» и «SPWeb». В случае отсутствия синтаксических конструкций, уничтожающих экземпляры этих классов, список ошибок пополняется. То есть на базе компилятора .Net мы построили анализатор кода, проверяющий семантику использования классов сторонней библиотеки.

До появления «Roslyn» анализаторы кода, которые были разработаны, по сути являлись анализаторами текста, так как построить дерево разбора было невозможно. С появлением «Roslyn» для программистов отрылись огромные возможности изучения компилятора .Net и использования его компонентов для внесения своих изменений в него.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1.Static code analysis tool FxCop - https://en.wikipedia.org/wiki/FxCop

3.Static code analysis tool StyleCop - https://en.wikipedia.org/wiki/StyleCop

4.Best Coding Practices in SharePoint - http://adicodes.com/best-coding-practices-in-sharepoint-part1/

5..NET Compiler Platform ("Roslyn") - https://github.com/dotnet/roslyn

6.https://ru.wikipedia.org/wiki/Компилятор

7.Reza Alirezaei, Brendon Schwartz, Matt Ranlett, Scot Hillier, Brian Wilson, Jeff Fried, Paul Swider, 2013. Professional SharePoint 2013 Development. 1st ed.: John Wiley & Sons, Inc.

УДК 004.728.4 (043.2)

О. В. Толстікова, к.т.н.
Національний авіаційний університет, Київ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ СЕРВЕРНОГО ОБЛАДНАННЯ В ЦЕНТРАХ ОБРОБКИ ДАНИХ ЗАСТОСУВАННЯМ РІШЕНЬ ВІРТУАЛІЗАЦІЇ

Центр обробки даних (ЦОД) для управління виробництвом та організація його мережевого середовища дає можливість гнучко, ефективно та централізовано управляти обчислювальною мережею. Він зазвичай служить для взаємодії між собою облаштувань зберігання даних, підключених до одного або більше серверів. Впровадження інформаційної системи для здійснення можливості високопродуктивного функціонування необхідних мережних сервісів управління виробництвом, ефективної взаємодії внутрішніх інформаційних ресурсів виробництва і є метою використання ЦОД в системі управління виробництвом.

Рішення віртуалізації дозволяють зменшити витрати виробництва на апаратне забезпечення, а також підвищити доступність мережевих сервісів.

Ефективне розподілення сервісів центру обробки даних, зменшення кількості простоїв і непродуктивної роботи серверного обладнання можливо забезпечити використанням системи віртуалізації *VMware vSphere.*

VMware vSphere – це комплексна платформа віртуалізації серверів, що забезпечує підвищення коефіцієнта використання серверних ресурсів, скорочення капітальних і експлуатаційних витрат, високий коефіцієнт консолідації серверів. Ця система дозволяє виконати автоматичне відновлення працездатності сервісів у випадку апаратних або програмних збоїв серверів.

Віртуалізація сервісів ЦОД повинна відбуватися з урахуванням відсутності втрат функціональних якостей мережних сервісів. З урахуванням попереднього планування віртуального середовища недоліки систем віртуалізації можливо звести до мінімуму. Важливою вимогою до системи віртуалізації є підтримка операційних систем, які будуть використані для виконання необхідних сервісів. У структурі ЦОД можна віртуалізувати серверний сегмент вцілому.

У процесі застосування рішень віртуалізації забезпечується надання набору обчислювальних ресурсів або їх логічного об'єднання, абстраговане від апаратної реалізації, що й забезпечує при цьому логічну ізоляцію обчислювальних процесів, виконуваних на одному фізичному ресурсі.

За допомогою системи віртуалізації *VMware vSphere* можливо автоматичне відновлення працездатності сервісів у випадку апаратних або програмних збоїв серверів.

Для забезпечення цих можливостей необхідно використовувати як мінімум три фізичні сервери, однаковість мережного середовища в сегменті віртуалізації і єдине сховище для реалізації концепції кластера віртуалізації. При цьому, у випадку відмови одного сервера, потужності серверів, що залишилися, повинно бути достатньо для виконання всіх сервісів.

Також, важливо підкреслити, що грамотна організація серверного сегмента має на увазі підхід «один сервіс - один сервер». Дана концепція дозволяє

збільшити безпеку та керованість інформаційної системи. Реалізувати цей підхід дозволить застосування рішень віртуалізації.

Базовим обчислювальним елементом віртуальної інфраструктури є віртуальна машина – це програмний елемент під керуванням гіпервізора *VMware vSphere.* Інформація про конфігурацію та стан віртуальної машини, а також її дані інкапсульовані в наборі окремих файлів, які розміщені у сховищі даних. Інкапсуляція забезпечує зручність переносу, резервного копіювання та клонування віртуальних машин.

Кожна віртуальна машина має принаймні один віртуальний центральний процесор (ЦП), і їх число може бути збільшене до 64 при використанні технології симетричної багатопроцесорної обробки *vSphere* за назвою *VMware Virtual SMP*. При включенні віртуального процесора ядро *VMkernel* призначає йому доступний контекст виконання апаратного рівня (*hardware execution context*, *HEC*-контекст). Один *HEC*-контекст дає процесору може обробляти один потік керування й, таким чином, відповідає одному ядру ЦП або одному гіперпотоку (якщо ЦП підтримує технологію *Hyper-Threading*). Багатоядрові ЦП і ЦП із підтримкою технології *Hyper-Threading* надають два й більш *HEC*-контекстів, на яких можуть виконуватися віртуальні процесори.

При об'єднанні декількох віртуальних машин на одному фізичному сервері можна більш ефективно використовувати більші обсяги пам'яті даного фізичного сервера. Платформа *vSphere* використовує кілька технологій для забезпечення ефективного використання ОЗП та високих коефіцієнтів консолідації, включаючи прозоре спільне використання сторінок, звільнення пам'яті гостьовий ОС і стиснення умісту пам'яті.

Перенос працюючих віртуальних машин з одного фізичного сервера на інший без простоїв зі збереженням постійної доступності служб і повної цілісності транзакції забезпечується *VMware vSphere vMotion*.

Платформа *VMware vSphere* надає чотири види служб віртуалізації мережі для вузлів *VMware vSphere* і віртуальних машин. Ця платформа зв'язує віртуальні машини один з одним у межах одного вузла, підключає віртуальні машини до фізичної мережі, а також підключає служби *VMKernel* (такі як *NFS, iSCSI і VMware vSphere vMotion*) до фізичної мережі. Крім того, вона реалізує мережеві можливості для інтерфейсу керування [1-5].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Басистый Д.А., Кусакин Д.Н.*. ЦОД, создаваемый по всем правилам./ Корпоративные системы, №3 (213), 2010.

2. *David Davis. End Your Data Center Logging Chaos with VMware vCenter Log Insight*, [Електрон. ресурс]. – *VMware Inc*., 2013.

3. *Don Williams, Will Urban. Best Practices when implementing VMware vSphere in a Dell EqualLogic PS Series SAN Environment*, [Електрон. ресурс]. – *Dell Inc*., 2013.

4. *David Glynn. EqualLogic Virtual Storage Manager: Installation Considerations and Datastores Manager*, [Електрон. ресурс]. – *Dell Inc*., 2012.

5. *James Hutten, Barry Gruetzmacher. Power to Dell PowerEdge M1000e Blade Server Enclosures*, [Електрон. ресурс]. – *Dell Inc*., 2012.

УДК 004.056 (043.2)

Е. В. Толстикова, к.т.н.,
И. С. Мирошниченко
Национальный авиационный университет, Киев

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ МЕХАНИЗМА ЦИФРОВОГО АУДИО-ОТПЕЧАТКА ДЛЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

По мере развития компьютерных сетей и расширения сфер автоматизации ценность информации неуклонно возрастает. Популярность глобальной сети Интернет, с одной стороны, открывает огромные возможности для электронной коммерции, но, с другой стороны, создает потребность в более надежных средствах безопасности для защиты корпоративных данных от доступа извне. В настоящее время все больше компаний сталкиваются с необходимостью предотвращения несанкционированный доступ к своим системам и защите транзакции в электронном бизнесе. Одним из самых эффективных способов улучшения защиты являются биометрические системы аутентификации.

Биометрические системы аутентификации — системы аутентификации, использующие для удостоверения личности людей их биометрические данные, гарантируют более высокий уровень защиты, нежели стандартные средства.

Данный механизм функционирует следующим образом: в базе данных системы хранится цифровой биометрический образ заявленного пользователя. Клиенту, для получения доступа к компьютерной сети, с помощью микрофона, сканера отпечатков пальцев или других устройств необходимо ввести информацию о себе в систему. Поступившие данные сравниваются с образцом, хранимым в базе данных.

Следует обратить внимание на существенные преимущества биометрических систем аутентификации, а именно:

− уникальные человеческие качества сложно подделать;

− биометрические характеристики не могут быть забыты или утеряны.

Однако слабостью биометрической системы аутентификации является то, что данные могут быть похищены после их получения.

Первым шагом работы механизма цифрового аудио-отпечатка при распознавании образца цифрового аудио-отпечатка является процесс первоначального трансформирования вводимой информации для сокращения обрабатываемого объема и её дальнейшего анализа. Следующим этапом является спектральное представление речи, получаемое путем преобразования Фурье. Спектральное представление достигается использованием широко-частотного анализа записи. Затем определяются конечные выходные параметры для варьирования голоса, и производится нормализация для составления шкалы параметров, а также для определения ситуационного уровня речи. Вышеописанные измененные параметры используются затем для создания шаблона. Шаблон включается в словарь, который характеризует произнесение звуков при передаче информации говорящим при использования этой системы.

Далее в процессе распознавания новых речевых образцов (уже подвергшихся нормализации и получивших свои параметры), они сравниваются с шаблонами, уже имеющимися в базе, с учетом динамичного искажения и похожих метрических измерений.

Любой речевой сигнал можно представить как вектор в произвольном параметрическом пространстве. При этом данный вектор может быть запомнен в нейросети. Одна из моделей нейросети, обучающаяся без учителя – это самоорганизующаяся карта признаков Кохонена. В ней для множества входных сигналов формируются нейронные ансамбли, представляющие эти сигналы. Данный алгоритм обладает способностью к статистическому усреднению. Этим решается проблема с вариативностью речи. С помощью этого алгоритма (как и многих других нейросетевых алгоритмов), осуществляется параллельная обработка информации, поскольку осуществляется одновременная работа всех нейронов. Тем самым решается проблема со скоростью распознавания, так как обычно время работы нейросети составляет несколько итераций.

В связи с разнообразностью обрабатываемого сигнала (различия человеческих голосов, уровень речи говорящего, вариации в произношении, нормальное варьирование движения органов речи) можно разработать алгоритм сравнивания образцов, с помощью которого осуществляется поэтапная реализация следующих процессов:

− фильтрация шумов;
− спектральное преобразование сигнала;
− постфильтрация спектра;
− лифтеринг;
− наложение окна Кайзера;
− сравнение.

Таким образом, можно получить высокоточную самообучающуюся систему распознавания человеческой речи.

Механизм цифрового аудио-отпечатка является простым и надёжным средством безопасности для защиты информации от несанкционированного доступа. Данный метод более эффективен, чем стандартные методы идентификации (сетевой логин и пароль), но требует больше ресурсов. Однако, требуется оценка целесообразности использования данного механизма для защиты системы. Использование механизма цифрового аудио-отпечатка в комплексе со стандартными методами идентификации, является наиболее оптимальным способом защиты компьютерной сети. [1-4]

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Joseph Picone, Ruslan Popov. Методы моделирования сигнала в распознавании речи. Кемерово. − 2000.

2. Ф. Уоссермен. Нейрокомпьютерная техника: Теория и практика. − 1992.

3. Фланаган Дж. Анализ, синтез и восприятие речи. − М.: Связь. − 1968.

4. Плотников В.Н., Суханов В.А., Жигулевцев Ю.И. Речевой диалог в системах управления. − М.: Машиностроение, − 1988.

УДК 004.023 **О. А. Туровський**
Національний технічний університет України «КПІ», Київ

АНАЛІЗ МЕТОДІВ АВТОМАТИЧНОЇ КЛАСИФІКАЦІЇ ОНЛАЙН-КОНТЕНТУ

Метою даної роботи є порівняння методів класифікації текстів такі як методу словника та навчального методу з урахуванням мінімізації ресурсів та інтервалу часу, який потрібно витратити на підготовку до аналізу, та оцінка вартості цієї підготовки.

Для порівняння розглянутих методів використовуватимуться такі характеристики як час підготовки інформації для роботи алгоритму, вартість підготовки цієї інформації, складність алгоритму, швидкість виконання, кількість обчислювальних ресурсів, які потрібні для роботи алгоритмів. [1, 2] Нехай t_1,t_2 - час укладання словника та час кодування тексту для навчальних методів відповідно; c_1, c_2 - складність алгоритму методу словника та навчальних методів відповідно, і ця складність задана в кількості операцій алгоритму. Відомо, що для укладання словників потрібно закодувати однакову кількість текстів, як і для навчальних методів. Проте, після кодування потрібен час для створення власне словника. [1] Тому $t_1 > t_2$. Оскільки алгоритм роботи методу словника більш простий, ніж алгоритми навчальних методів, то $c_1 < c_2$. Нехай функція $f(t) = p$ – лінійна зростаюча функція, яка оцінює вартість роботи експерта, який складає словники та виконує кодування, а $g(c) = v$, а $h(c) = u$ - відповідно лінійна спадна та зростаюча функції швидкості роботи алгоритмів та кількості обчислювальних ресурсів для роботи алгоритму.[1] Тоді, p_1, p_2 - вартість підготовки інформації для метода словника, та для навчальних методів відповідно, v_1, u_1 - це швидкість роботи та об'єм обчислювальних ресурсів алгоритму метода словника, а v_2, u_2 - це швидкість роботи та об'єм обчислювальних ресурсів алгоритмів навчальних методів відповідно. Оскільки функція $f(t)$, $h(c)$ лінійно зростаючі, $g(c)$ – лінійно спадна, то вартість укладання словників більша ніж вартість просто кодування текстів, тобто $p_1 > p_2$, а швидкодія методів словника вища, і кількість обчислювальних ресурсів на їх реалізацію менша, тобто $v_2 > v_1$, $u_1 > u_2$. [1]

Проведені дослідження показують, що словникові методи можуть швидше класифікувати текст, і їм потрібні значно менші обчислювальні ресурси. Навчальні методи дають змогу зменшити витрату коштів, проте об'єм обчислювальних ресурсів залежить від складності алгоритму аналізу.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Grimmer. J. Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts [Електронний ресурс] / J. Grimmer, B.M. Stewart // Political Analysis. - 2013. - Volume 21, Issue 3. – Режим доступу: http://scholar.princeton.edu/sites/default/files/bstewart/files/tad2.pdf. – Назва з екрану. – Дата звернення: 17.12.2015.

2. Collingwood W. Tradeoffs in Accuracy and Efficiency in supervised Learning Methods / W. Collingwood, L. Collingwood, J. Collingwood // The Journal of Information Technology and Politics 2011. - P. 4.

УДК 681.51 (043.2)

Д. В. Ходаков, к.т.н.
Національний авіаційний університет, Київ

ОСНОВНІ АСПЕКТИ АРХІТЕКТУРНОГО ПРОЕКТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Програмні продукти – це основний елемент більшості сучасних високотехнологічних доменів (стільниковий зв'язок, відеотрансляції, охоронна діяльність, керування транспортним та іншими видами руху і т.д.), По суті, багато нововведень, які ми тепер сприймаємо як даність – в тому числі таких організацій, як eBay або Amazon – просто не існувало б, якби вони не були побудовані на програмному забезпеченні (ПЗ). На сьогоднішній день важко знайти організацію, яка хоч якимось чином була залучена в сферу програмного забезпечення.

Архітектура – це базова організація системи, втілена в її компонентах, їхні стосунки між собою і з оточенням, а також принципи, що визначають проектування і розвиток системи.

Для створення інформаційної архітектури необхідно володіти знаннями про вимоги до неї в проектуємій області.

Якісна підтримка і розвиток ПЗ, має на увазі розуміння того, що саме і яким чином треба розвивати, які раніше допущені помилки не слід повторювати, а що з минулого необхідно врахувати і використовувати зараз і в майбутньому. Архітектура визначає структуру. Так як з урахуванням поступово зростаючої кількості різнопланових запитів до якості інформаційних продуктів, що складається з безлічі різних компонентів, дозріло розуміння того, що архітектура програмних продуктів повинна бути результатом роботи не тільки програмістів, а і спеціальних груп широко-профільних фахівців. Ці групи повинні бути здатні з заданим рівнем якості створити повноцінну архітектуру, здатну охопити численні складові інформаційних продуктів. Тобто здійснений перехід від класичної схеми розгляду архітектурного проектування як технічної, інженерної дисципліни до розгляду взаємопов'язаного комплексу дисциплін знаходиться на стику задоволення комплексу потреб усіх зацікавлених осіб [4].

В рамках архітектури розглядаються не тільки внутрішні елементи системи, але і взаємодія системи із зовнішнім середовищем, включаючи призначену для користувача середовище і середовище розробки. Тільки так вдасться встановити причинно-наслідкові зв'язки і вибудувати оптимальну систему, на якій зможе бути спроектована архітектура будь-якої складності.

Архітектуру програмного забезпечення можна проілюструвати за допомогою кількох архітектурних уявлень. Кожне архітектурне уявлення пов'язане з деяким певним набором питань, що цікавлять учасників розробки: користувачів, проектувальників, менеджерів, технічних фахівців, обслуговуючий персонал і так далі. Архітектура повинна врівноважувати потреби зацікавлених осіб і втілювати рішення на основі логічного обгрунтування[3].

Проблема ще в тому, що класичні інженерні практики, не настільки ефективні, для непостійних вимог, мінливих умов. Шаблони проектування не є конкретними. Архітектурні рішення – це завжди компроміси між різними інтересами, зовнішніми силами, принципами та відповідними силами, так що цей баланс унікальний для кожного проектувальника і проектного середовища. Шаблони проектування можна умовно розділити на три типи[2].

1. Розробка архітектури відбувається перед початком роботи над кодом. Використання шаблону реалізується від початку і до кінця при кодуванні відповідної функціональності. Інвестується більше часу і ресурсів на ранній стадії з тим, щоб отримати велику економію при супроводі та доопрацювання.
2. Еволюційно використання шаблонів, направлено на більш рівномірний розподіл ресурсів за стадіями проектів. Зменшуються інвестиції на початку проекту, швидше виходять перші результати у вигляді функціональності, проте потрібні разові інвестиції на впровадження шаблону при переході на супровід / доопрацювання. При такому підході на ранніх стадіях проекту функціональність реалізується повністю або частково без використання шаблону, створюються тести. На етапі ж виправлення помилок, доопрацювання функціональності або вдосконалення системи (як правило, перед початком розробки нової функціональності або удосконалення старої) за допомогою рефакторінга код перетвориться до потрібного шаблоном проектування.
3. Невикористання шаблонів в деяких випадках виявляється виправданим. Наприклад, при роботі над старим кодом, в разі вкрай обмежених ресурсів, або термінів в поєднанні з невисокими вимогами до якості, або супроводу продукту.

Вибір відповідного стилю використання шаблонів робиться на підставі політики, ресурсів і вимог, і вибір цей часто робиться архітектором на підставі неповних даних про майбутнє проекту, що робить його дуже людино-залежним[1].

Проектування архітектури в проектах із розробки програмного забезпечення має першочергове значення як для технічного, так і для маркетингового успіху проекту, характеристики людей мають першочергове значення для процесу розробки ПЗ в цілому і проектування архітектури зокрема.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Scott Millett, Nick Tune: Patterns, Principles, and Practices of Domain-Driven Design. –“ Wrox ”, 2015. – 795 с.

2. Эрик Фримен, Элизабет Фримен, Паттерны проектирования. – СПб.: Питер, 2011. – 565 с.

3. Len Bass, Paul Clements, and Rick Kazman: Software Architecture in Practice, Second Edition. “ Addison Wesley”, 2003. – 40 с.:ил.

4. Майкл Нейгард: Release it! Проектирование и дизайн ПО для тех, кому не все равно. – СПб.: “Питер”, 2016. . – 320 с.

УДК 004.3

О. А. Чемерис, к.т.н.
Інституту проблем моделювання в енергетиці
ім. Г.Є.Пухова НАН України, Київ

ЕНЕРГОСПОЖИВАННЯ МІКРОПРОЦЕСОРНИХ СИСТЕМ

З ростом поширення використання мікропроцесорних систем, мобільних пристроїв та вимірювальної апаратури, такий параметр, як енергоспоживання, набуває великого значення. Нажаль розвиток пристроїв живлення не відповідає темпам росту нових приладів. Важливим також є ті факти, що при низькому енергоспоживанні значно легше створити малогабаритний пристрій, легше запроектувати схеми живлення та зменшити рівень випромінювання пристрою [1].

Переважна більшість сучасних цифрових систем виробляються за допомогою КМОН (комплементарний метал-оксид-напівпровідник) технології. Для КМОН-схем існують чотири складових споживання енергії: а) розсіювання енергії, викликане струмами короткого замикання; б) розсіювання енергії, викликане паразитними струмами витоку; в) статичний розсіювання енергії; г) динамічне розсіювання енергії [1]. Відомо, що динамічна складова складає приблизно 80% від загального об'єму споживання і визначається за формулою (1) [2].

$$P_{dyn} = C \cdot V_{dd}^{\ 2} \cdot \alpha \cdot f \ , \qquad (1)$$

де C - сумарна ємність в вузлах схеми, V_{dd} - величина напруги живлення, f - частота перемикань, α - коефіцієнт активності [3].

Чим вище рівень абстракції, на якому виконується оптимізація енергоспоживання, тим вище буде значення ефекту від втілення того чи іншого рішення [4]. Коефіцієнт активності α – це той параметр, на який впливає виконання програм в системі. Таким чином, при зменшенні пересилок процесор-пам'ять, при оптимізації обчислень чи операцій вводу-виводу, можна зменшити активність ланцюгів мікросхем і отримати зменшення енергоспоживання.

Циклічні частини в програмах є тією ланкою, де втілено найбільш значний об'єм програми. Сучасні програми вимагають багато пам'яті, яка, як відомо, надзвичайно енергоємним. Пересилки в пам'яті витрачають багато енергії. Наприклад, передача з зовнішньої пам'яті споживає в 33 рази більше, ніж додавання 16-ти бітних чисел [7]. Очевидно, що обсяг пам'яті і кількість передач пам'яті повинно бути зведене до мінімуму, так що опис програми повинен бути оптимізованим [5].

Для зменшення активності елементів мікропроцесорної системи пропонується додаткова обробка тексту програми, яка планується до виконання на в даній системі. Так, проводиться аналіз тексту, виявляються оператори циклів, будується множина залежностей виходячи з умови збереження синхронізації обчислень, виконується трансформація циклу і генерується модифікований код програми. Таким чином, на виході даного перетворення отримаємо програму на мові вищого рівня, яку можна обробляти далі стандартними засобами.

Алгоритм, що виконується на мікропроцесорній системі, може бути представлений як орієнтований граф, де вершинами є оператори алгоритму, які зв'язані ребрами, що відповідають залежностям в алгоритмі.

В регістрах процесора и кэш-пам'яті кількість чарунок, які необхідно для зберігання даних, що відносяться до конкретного оператора програми, визначається вагою (w_e) всіх вихідних ребер (e) відповідної вершини графу (u). З цією метою вводиться поняття ціни вершини, яке визначається як максимальна вага ребер, що виходять з даної вершини

$$C_u = \max_{e=(u,v)\in E} w_e \quad \left(u \xrightarrow{e} v\right) \tag{2}$$

де v – вершина графу, E - множина всіх ребер графу.

Якщо V - множество всех вершин графа, то кількість чарунок швидкої пам'яті (кеш процесора, регістри даних, тощо) для циклу буде визначатися виразом (3).

$$Cost(G) = \sum_{u\in V} C_u \tag{3}$$

Мінімізують величину $Cost(G)$, використовуючи метод ресинхронізації, для чого кожній вершині u ставиться у відповідність параметр синхронізації r_u (цілочисельна величина). Даний параметр є величиною зміни ваги ребра графу. Для ресінхронізованого графу вага ребра записується у вигляді (4).

$$w_{r,e} = w_e + r_v - r_u\ ,\ \left(u \xrightarrow{e} v\right),\ w_{r,e} \geq 0, \forall e \in E \tag{4}$$

Задачу мінімізації $Cost(G)$ зводимо до задачі цілочисельного лінійного програмування:

$$\min \sum_{u\in V} C_u\ ,\ w_{r,e} \geq 0, \quad C_u \geq w_{r,e}\ ,\ \forall e \in E \tag{5}$$

Таким чином, виконання такої трансформації вихідного коду програми на високому рівні дає можливість зменшити кількість пересилань даних процесор-пам'ять. Тим самим зменшується активність елементів системи і, відтак, зменшується енергоспоживання мікропроцесорної системи. Експерименти, що були проведено на системі C8051F064-EK показують можливість зменшення енергоспоживання шляхом модифікації програми на 5-7%. Як тестовий приклад було розглянуто програму виявлення на зображеннях контурів об'єктів, що актуально для приладів зондування оптично непрозорих середовищ.

ВИКОРИСТАНІ ДЖЕРЕЛА

[1]. Chandrakasan A.P. Low power CMOS digital design / A.P. Chandrakasan, S. Sheng, R.W. Brodersen // IEEE Journal of Solid State Circuits. – 1992. - Vol. 27. - P. 473-484.

[2]. H.J.M. Veendrick, Deep-Submicron CMOS ICs. From Basics to ASICs. Kluwer academic publishers, 2000.

[3]. Low Power Design Guide [Електроний ресурс] / F. Poppen // OFFIS Research Institute - 2000. - P. 18. – URL: http://www.informatik.uni-oldenburg.de/~pipsoft/lpdesignguide.pdf, вільний. - Title of screen. - Lang. eng. - (use date: 03.04.2016).

[4]. J. Sproch, High Level Power Analysis and Optimization. Tutorial. In Proc. 1997 International Symposium on Low Power Electronics and Design. 1997.

[5]. A. Fraboulet, K. Kodary, and A. Mignotte, Loop fusion for memory space optimization. In Proc. 14th International Symposium on System Synthesis, 2001, Proceedings, pp. 95-100, 2001

[6]. F. Catthoor, F. Franssen, S. Wuytack, L. Nachtergaele, H. De Man, Global communication and memory optimizing transformations for low power signal processing systems. Workshop on VLSI Signal Processing, VII, pp. 178 - 187, Oct. 1994.

УДК 004.738

Г. В. Щербакова

Національний технічний університет України «КПІ», Київ

ПОРІВНЯННЯ СПОСОБІВ ШИФРУВАННЯ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

У сьогоденні проблема захисту ресурсів комп'ютерних мереж має велике значення. Одним з необхідних, але не єдиним, методом захисту є шифрування. Воно існує двох типів – симетричне та асиметричне. Метою цієї роботи є порівняння цих двох методів та виявлення переваг і недоліків.

При симетричному шифруванні використовується один ключ. За допомогою ключа проводиться як шифрування, так і розшифрування. Ключ повинен залишатися у таємниці. Цей метод також називають методологією з таємним ключем [1].

При асиметричному шифруванні створюються два взаємопов'язаних асиметричних ключа. Один повинен бути безпечно переданий його власнику, а інший - тій особі, яка відповідає за зберігання цих ключів, до початку їх використання. Незважаючи на те, що ключі створюються разом, вони різні [2]. У таблиці 1 наведено порівняння симетричного та асиметричного методів шифрування.

Таблиця 1

Показник	Симетричний метод	Асиметричний метод
Ключі	Один ключ, використовується двома, або більше, користувачами	Один відкритий ключ, інший – таємний, який відповідає відкритому
Обмін ключами	Захищеним каналом	Відкритий ключ передається загальнодоступним каналом, а таємний зберігає власник не розголошуючи
Швидкість	Метод шифрування має меншу складність, а тому швидкий	Метод складний, а тому повільний
Спосіб використання	Комплексне шифрування (шифрування файлів та комунікаційних каналів)	Розповсюдження ключів та цифровий підпис

Порівняльний аналіз алгоритмів шифрування показує, що асиметричне шифрування передбачає більш складні процедури, що призводить до значних часових затрат. Симетричне шифрування призводить до значно менших витрат часу, що особливо відчутно при збільшенні об'єму переданих даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2002. — 816 с.

2. Гатчин Ю.А.Основы криптографических алгоритмов. Учебное пособие / Коробейников А.Г. - СПб.: СПбГИТМО(ТУ), 2002. – 29 с.

О. К. Юдін, *д.т.н.*
Національний авіаційний університет, Київ,
С. С. Бучик, *к.т.н.*
Житомирський військовий інститут ім. С.П.Корольова, Житомир,
О. В. Фролов

МЕТОДИ АНАЛІЗУ РИЗИКІВ ДЕРЕВА ІДЕНТИФІКАТОРІВ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Метою даної доповіді є викладення методів аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів, запропонованих в оригінальній авторській інтерпретації.

Виклад методів аналізу ризиків представляє собою сукупність запропонованих авторами двох методів, при цьому вихідні дані першого методу є вхідними даними для другого, таким чином ми можемо говорити про методологію аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів.

І. Метод визначення рівня ризику застосування певних контрзаходів щодо визначених ресурсів (з урахуванням визначених атак та уразливостей ресурсів).

Визначимо для здійснення аналізу ризиків дерева ідентифікаторів ДІР наступні чотири складові: AS (assets) – активи, в ролі яких виступають ДІР; V (vulnerability) – уразливості ДІР; AT (attacks) – атаки на ДІР; D (decisions or counter-measures) – контрзаходи щодо зменшення впливу на ДІР атак через їх уразливості (засоби захисту, способи та методи захисту). Визначення даних складових лежить в рамках тієї теорії, що описана вище і не суперечить загальноприйнятим підходам до визначення складових ризику.

У відповідності до запропонованої авторами «методології подвійної трійки захисту», представимо дані складові у вигляді наступних множин.

1. Множина активів ДІР $AS = \{AS_{nps}, AS_{ors}, AS_{its}\}$, де AS_{nps}, AS_{ors}, AS_{its} множина ДІР в яких їх захист направлений за відповідними спрямуваннями: нормативно-правовим (НорПС) – nps ; організаційним (ОргС) – ors ; інженерно-технічним (ІнжТС) – its ;

2. Множина уразливостей ДІР $V = \{V_{nps}, V_{ors}, V_{its}\}$, де V_{nps}, V_{ors}, V_{its}, – множина уразливостей ДІР НорПС, ОргС та ІнжТС, які реалізуються через загрози ДІР;

3. Множина контрзаходів $D = \{D_{nps}, D_{ors}, D_{its}\}$, де $D_{nps}, D_{ors}, D_{its}$ – множина контрзаходів НорПС, ОргС та ІнжТС, направлених на захист відповідних ресурсів від уразливостей;

4. Множина атак $AT = \sum_{z=1}^{N} \bigcup_{k \in \{1,\dots,card(AT)\}} at_k(V_z)$, де $card(AT)$ потужність множини атак, N – кількість спрямувань загроз ДІР (НорПС, ОргС, ІнжТС), $at_k(V_z)$ – функція залежності k - ої атаки від уразливості ДІР за z - им спрямуванням. Необхідність введення даної залежності полягає у тому, що за рахунок зміни коефіцієнтів матриці V_z ми можемо впливати на атаку.

Позначимо матрицю контрзаходів як C. Її розмір визначається як $card(D) \times card(AS)$.

Таким чином, спираючись на визначення матриці C та попередніх міркувань, задача аналізу ризиків дерева ідентифікаторів ДІР зводиметься до знаходження такої матриці C^*, яка б оптимально задовольняла використанню за вартістю засобів захисту від атак на ДІР.

За допомогою операторів $*$ та $\cdot$, які визначають поелементне та класичне множення, функції, які описують оптимізацію процесу аналізу ризику, можуть бути представлені наступним чином:

$$f_1(C) = \left\| \mathbf{I_П} \cdot (\mathbf{П} * \mathbf{M}) \right\|, \quad (1)$$

$$f_2(C) = \left\| \mathbf{I_I} \cdot (\mathbf{I} * \mathbf{M}) \right\|, \quad (2)$$

$$f_3(C) = \left\| C * \mathbf{Г} \right\|, \quad (3)$$

II. Метод кластеризації ризиків на основі транзитивного замикання бінарного відношення активів.

У відповідності з першим методом ми отримали рівні ризику застосування певних контрзаходів щодо визначених ресурсів (з урахуванням визначених атак та уразливостей ресурсів), тобто вихідна матриця має розмір $card(D) \times card(AS)$.

Визначимо отриману матрицю, як матрицю об'єктів-ознак, де в якості об'єктів виступають ресурси (активи) AS, а в якості ознак – розподілені по ресурсам контрзаходи D.

В результаті отримання відповідних α - рівнів ми отримуємо кластери ДІР, які згруповані за рівнями ризику. В результаті цього є можливість прослідкувати порядок об'єднання у кластери ДІР для подальшого їх аналізу. Використавши алгоритм, який представлено автором в попередніх дослідженнях, отримуємо оптимальний α - рівень, нижче якого ризик є допустимим.

В доповіді не ставилось за мету проведення економізації вартості рішень у сфері розробки систем захисту інформації на базі ризикового підходу та адаптації законодавчої бази захисту інформації в Україні до міжнародних стандартів серії ISO 2700x. Основним результатом автори вважають формування системи стандартизації ДІР власної оригінальної методології, що зрозуміло не протирічить міжнародним стандартам, використовуючи особистий досвід та результати наукових досліджень представлених в серії статей та монографій групи науковців та викладення теоретичних основ оптимізації системи захисту ДІР.

Наведений механізм, на думку авторів, є з одного боку максимально доступним і простим, з іншого – втілює все краще, що реалізовано у міжнародних стандартах.

В подальшому автори бачить динамічний розвиток даної теорії у розрізі її практичного застосування в органах державного управління.

Наукове видання

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
IX МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2016)

21–23 квітня 2016 року

Тези доповідей надруковані в авторській редакції однією із трьох робочих мов конференції: українською, російською, англійською

Підп. до друку 14.04.15. Формат 60х84/16. Папір офс.
Офс. друк. Ум. друк. арк. 4,8. Обл.-вид. арк. 5,1
Тираж 100 пр. Замовлення № 111-1

Видавець і виготівник
Національний авіаційний університет
03680. Київ-68, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002

Для нотаток