МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Національний авіаційний університет
Інститут комп'ютерних інформаційних технологій

ЗБІРНИК ТЕЗ

VIII МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2015)

16–18 квітня 2015 року

Київ 2015

УДК 004.7(043.2)

Збірник тез VIII Міжнародної науково-технічної конференції «Комп'ютерні системи і мережні технології» (CSNT-2015), м. Київ, 16–18 квітня 2015 р. Національний авіаційний університет. – К.: НАУ, 2015. – 72 с.

У збірнику тез представлені доповіді, які були представлені на конференції «Комп'ютерні системи і мережні технології» (CSNT-2015). У доповідях розглянуті наукові, технічні та технологічні проблеми побудови, проектування сучасних комп'ютерних систем, засоби і методи моделювання комп'ютерних мереж, проблеми захисту ресурсів в інформаційних систмах, технології підготовки авіаційних фахівців.

Затверджено вченою радою Інституту комп'ютерних інформаційних технологій Національного авіаційного університету (протокол № 3 від 14 квітня 2015 р.).

Редакція не обов'язково поділяє думку автора. Відповідальність за достовірність фактів, цитат власних імен та іншої інформації несуть автори публікацій.

ЗМІСТ

УДК 681:513.54

Азарсков В.Н., д.т.н.,
(Национальный авиационный университет, Украина)
Курганский А.Ю.,
(Авиационный научно-технический комплекс «Антонов» , Украина)
Рудюк Г.И., к.т.н.,
(Авиационный научно-технический комплекс «Антонов» , Украина)

МОДЕЛИ НЕШТАТНЫХ СИТУАЦИЙ В ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ КОМПЛЕКСАХ АВИАЦИОННОЙ И КОСМИЧЕСКОЙ ТЕХНИКИ

Для синтеза устойчивых к отказам алгоритмов фильтрации, управления в информационно-управляющих комплексах (ИУК), а также для анализа их точности при возникновении отказов (появления нештатных, аварийных, катастрофических ситуаций), следует задаться математической моделью, адекватно описывающей эти состояния сложных систем управления. [1] Под отказом (нештатной, аварийной, катастрофической ситуацией) будем понимтаь скачкообразные изменения параметров или структуры сложной системы управления, происходящие в случайные моменты времени. Поэтому для описания ИУК, в которых необходимо учитывать возможность появления отказов, введем случайный неизвестный вектор появления параметров $\gamma(k)$, характеризующий на данный момент структуру и параметры ИУК. Появление нештатной ситуации приводит к скачкообразному изменению этого вектора. Уравнения состояния и наблюдения ИУК оказываются в этом случае зависящими от изменяющегося в случайные моменты времени вектора $\gamma(k)$ и в общем виде могут быть записаны следующим образом

$$X(k+1) = F\left[X(k)\gamma(k)U(k)W(k)\right]; \quad (1)$$

$$Y(k) = h\left[X(k)\gamma(k)V(k)\right], \gamma(k) = \Omega, \quad (2)$$

где F и h – известные функции; Ω – пространство возможных значений $\gamma(k)$; $X(k)$ – n-мерный вектор состояния системы; $Y(k)$ – матрица наблюдений системы; $U(k)$ – m-мерный вектор управления; $W(k)$ – случайный r-мерный вектор гауссовских возмущений с нулевым средним и корреляционной матрицей $M\left[W(k)W^T\right] = Q(k)\delta(kj)$; $\delta(kj)$ – символ Кронкера; $V(k)$ – p-мерный случайный вектор гауссовских погрешностей измерений с нулевым средним и корреляционной матрицей $M\left[V(k)V^T(j)\right] = R(k)\delta(kj)$. При этом уравнение состояния характеризует динамику системы, а уравнение наблюдений определяет механизм образования данных доступных измерению.

Однако, не конкретизируя статистические характеристики случайного вектора параметров $\gamma(k)$, трудно получить какие-либо теоретические результаты. Поэтому представляется целесообразным провести классификацию этих характеристик и на ее основе определить более конкретно математические модели, используемые в дальнейшем для синтеза отказоустойчивых алгоритмов фильтрации и анализа точности ИУК, подтвержденных отказом.

Прежде всего, следует задать структуру пространства возможных значений вектора $\gamma(k)$. Если это пространство непрерывное, то вектор $\gamma(k)$ может принимать бесконечное множество значений в заданной области, если дискретное – то число значений конечно. В последнем случае все значения вектора $\gamma(k)$ можно пронумеровать произвольным образом – $\gamma_i(k), i=\overline{1,N}$, и рассматривать индекс i как номер структуры, в которой в данный момент находится ИУК.

Рассмотрим класс моделей нештатных ситуаций в ИУК, который характеризуется однократным изменением структуры или параметров, когда статистические характеристики моментов возникновения нештатных ситуаций являются неизвестными. В общем случае для этих моделей уравнения состояния и наблюдения можно записать в виде

$$X(k+1)=\left[\Phi(k+1,k)+\Delta\Phi 1(k,m_1)\right]X(k)+W(k)+\Delta\Phi 1(k,m_2)\,; \qquad (3)$$

$$Y(k)=\left[H(k)+\Delta H 1(k,m_3)\right]X(k)+V(k)+\Delta V 1(k,m_4)\,, \qquad (4)$$

где $\Delta\Phi$, ΔW, ΔH, ΔV – приращения соответствующих матриц и векторов, возникающие за счет отказов; $1(k,m_i)$ – единичная ступенчатая функция; $m_i=(m=1,4)$ – неизвестный момент возникновения отказа.

Уравнения (3), (4) могут описывать такие нештатные ситуации, как внезапные отказы в ИУК (в измерительной и управляющей части).

Для исследования моделей данного вида эффективными оказываются идеи метода обобщенного отношения правдоподобия, позволяющего произвести оценку момента возникновения отказа, указать место его появления и оценить его влияние на безопасность и эффективность объекта исследования и принять «решение» на вывод объекта управления из нештатной ситуации.

Если предположить, что в процессе реализации алгоритмов оценивания и управления вычислительная система ИУК функционирует без сбоев, то ошибки оценивания будут определяться только характеристиками самих алгоритмов. Однако на практике при работе ИУК в реальном масштабе времени приходится считаться с возможностью возникновения сбоев в ЭВМ. Проявление сбоев может привести к существенному увеличению ошибок оценивания.

Предполагается проведение анализа влияния сбоев на точность алгоритмов фильтрации для тех случаев, когда за счет сбоев искажается содержимое ячеек запоминающего устройства, хранящих матричный коэффициент усиления, а также текущие и экстраполированные оценки. В результате такого анализа можно будет определить наиболее чувствительные к сбоям параметры алгоритмов ИИУ, выработать рекомендации по организации вычислительного процесса, обладающего повышенной устойчивостью к сбоям, обоснованно подойти к заданию количественных характеристик надежности хранения данных.

Предлагаемые математические модели предполагается использовать при моделировании сложных систем управления, так и при создании функционально-устойчивых информационно-управляющих комплексов авиационной и космической техники.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Азарсков В.М. Ідентифікація нештатних ситуацій у бортових інформаційно-керуючих комплексах. Вісник ЦНТЦ Транспортної академії України. – 2007. – № 10. – С. 73-76.

УДК 517.91

Антонов В.К., д.т.н.
(Национальный авиационный университет, Украина)

АДАПТИВНАЯ УСТОЙЧИВОСТЬ ДИНАМИЧЕСКИХ СИСТЕМ

Ослабим требования к поведению функции Ляпунова. Допустим возможность ее положительных производных, но на всех траекториях производная должна оставаться отрицательной в среднем. Поэтому до некоторого момента времени t_ε условие $\|x(t)\| < \varepsilon$ в нашем случае может нарушаться. До этого момента времени траектория может выходить за окрестность ε. Но при условии $t > t_\varepsilon$ она должна оставаться внутри области ε.

Определение устойчивости в нашем случае сформулируем следующим образом. Решение дифференциальной системы адаптивно устойчиво, если для любой окрестности ε существуют такие δ и t_ε, что при условии $\|x(0)\| < \delta$ и $t > t_\varepsilon$ выполняется условие $\|x(t)\| < \varepsilon$.

Функция $V(t,x)$ дифференцируема по времени и фазовому вектору, и имеет наименьшую высшую грань равную нулю в начале фазового пространства, т.е. существует функция $W(x)$ большая или равная нулю, такая, что $W(x) < V(t,x)$, если $\|x\| > 0$, и $W(0) = 0$.

Покажем, что для его выполнения достаточно, чтобы в среднем производная по времени от функции Ляпунова была отрицательна, т.е. чтобы для любого начального момента времени t_0, такого, что $0 \le t_0 < \infty$, выполнялось неравенство $\int_{t_0}^{\infty} \dot{V}(t,x)\big|_\Sigma dt < 0$. Символ $\big|_\Sigma$ означает определение полной производной в силу исследуемой системы.

Подобно доказательству теоремы Ляпунова исследуем поведение функции Ляпунова на траекториях исследуемой системы. Поверхность области ε является компактным множеством, и согласно теореме Вейерштрасса функция W имеет на нем наименьшую высшую грань. Ее значение обозначим через α. Из условия непрерывности функции Ляпунова по фазовому вектору и условия равенства ее в начале фазового пространства нулю следует существование области $\|x\| < \delta < \varepsilon$, такой, что в ней $V(0,x) < \alpha$. Докажем, что траектория решения, начинающегося в этой области, целиком остается внутри сферы S_ε при условии $t_\varepsilon < t < \infty$. Для этого предположим, что существует некоторое время, равное t_ε, такое, что если $t > t_\varepsilon$, то траектория навсегда остается вне сферы S_ε, то есть против условия устойчивости это время последнего покидания сферы, по истечении которого траектория обратно в сферу никогда не возвращается. Идея доказательства состоит в том, что в этом противоречащем условию устойчивости случае

должно выполняться неравенство, которое в первом приближении выглядит следующим образом

$$\int_0^{t_\varepsilon} \dot{V}(t,x)\big|_\Sigma dt + c_1 \; > \; -\int_{t\varepsilon}^{\infty} \dot{V}(t,x)\big|_\Sigma dt + c_2 .$$

Его смысл состоит в том, что вопреки условию устойчивости на начальном отрезке времени $[0, t_\varepsilon]$ функция Ляпунова возрастает более интенсивно, чем затем уменьшается на всей остальной части траектории. Запишем неравенство более точно, учитывая значения постоянных интегрирования в левой и правой частях неравенства - c_1 и c_2.

$$\int_0^{t_\varepsilon} \dot{V}(t,x)\big|_\Sigma dt + \alpha_1 \; > \; -\int_{t\varepsilon}^{\infty} \dot{V}(t,x)\big|_\Sigma dt + \alpha_2 \quad ,$$

где $\alpha_1 < \alpha$ постоянная интегрирования в левой части неравенства, равная значению функции Ляпунова в начальной точке траектории (в области δ, как и в случае теоремы Ляпунова, значение функции Ляпунова меньше α). В правой части постоянной интегрирования является левая часть неравенства, то есть значение функции Ляпунова на момент времени t_ε. Ее значение на сфере S_ε $\alpha_2 > \alpha_1$, т.к. $V(t_\varepsilon, x)\big|_\Sigma$ непрерывная функция, ограниченная снизу функцией $W(x)$, так что выполняется и неравенство $\alpha_2 > \alpha$. Получаем противоречащее условию теоремы неравенство

$$\int_0^{t_\varepsilon} \dot{V}(t,x)\big|_\Sigma dt + \int_{t\varepsilon}^{\infty} \dot{V}(t,x)\big|_\Sigma dt \; > \alpha_2 - \alpha_1 > 0 , \text{ или } \quad \int_0^{\infty} \dot{V}(t,x)\big|_\Sigma dt \; > 0 .$$

Таким образом, из противоречащего условию теоремы предположения получено противоречащее ее условию неравенство. Условия адаптивной устойчивости применимы к системам, работающим в режиме максимального быстродействия. Также они применимы к системам, имеющим параметрические регуляторы, параметры которых изменяются в процессе работы.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Б.П.Демидович Лекции по математической теории устойчивости, М., Наука, 1967, 472 с.

УДК 004.75

Балакин С.В.
(Национальный авиационный университет, Украина)

МЕТОДЫ И СРЕДСТВА ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ИДЕНТИФИКАЦИИ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ И АТАК В КОМПЬЮТЕРНОЙ СЕТИ

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

Предложена модель повышения достоверности идентификации воздействий и атак в компьютерной сети, а также разработана модель работы данной системы в режиме предотвращения и обнаружения.

Сформированы требования к системам которые предстоят модернизации и внедрению данных методов. Модуль идентификации построен с помощью расчетов статистики Байеса [1]. Алгоритм вычисления вторжений позволил проводить не только обнаружение, но в некоторых случаях и предотвращение вторжений [2].

Предложена и рассмотрена реальная модель повышения идентификации атак, которая позволяет обезопасить систему от атак в самой системе так и проникновения в нее извне.

Предложенная модель предназначена как для моделирования ситуаций связанных с атаками на сеть, так и для разработки готового программного продукта не только для повышения достоверности идентификации вторжений, но и для других бизнес-приложений, для защиты информации в корпоративных системах и т.п. Выделены основные развивающиеся направления использования идентификации атак [3].

Для получения данных о количестве вторжений и атак была использована формула Байеса:

$$\frac{P(I|A_1,A_2,\dots,A_k)}{P(\bar{I}|A_1,A_2,\dots,A_k)} = \frac{P(I)\prod_{i=1}^{n} P(A_i|I)}{P(\bar{I})\prod_{i=1}^{n} P(A_i|\bar{I})}$$

С ее помощью мы определили вероятность вторжения, используя значения измерений аномалий, вероятность вторжения и вероятности появления каждого из измерений аномальности, которые наблюдали ранее во время вторжений.

В работе предложен метод не только отслеживания несанкционированных действий в сети, но и выявление слабых узлов. С помощью метода можно отслеживать вторжения и определять какие из систем нужно модернизировать для предотвращения потери информации.

В результате процесса мониторинга анализируется и обрабатывается информация о деятельности защищенной системы. Правила мониторинга разрабатывают после рассмотрения таких вопросов, как:

• Раннее выявление;
• Конфиденциальность полученной информации;
• Обработка возможностей системы;

Информация о системе, за которой ведется наблюдение, поступает в виде отчетов. Безопасность системы и защита инфраструктуры могут быть встроены в систему мониторинга или быть отдельным элементом.

Концепция достоверности идентификации воздействий и атак в компьютерных сетях открывает ряд вопросов изучения безопасности, и открывает перспективу расширения набора решаемых функциональных задач, а также является средством всестороннего усовершенствования сети.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Хей Дж. Введение в методы байесовского статистического вывода, — ФИЗМАТЛИТ, 2006. - 816 с

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

3 Корченко О. Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / О. Г. Корченко. — К. : МК-Пресс, 2006. — 320 с.

УДК 621.327:681.5

Бойко Ю.П.
(Національний авіаційний університет, Україна)

МЕТОД КОМПРЕСІЇ ЗОБРАЖЕНЬ З ПОПЕРЕДНІМ КВАНТУВАННЯМ КОМПОНЕНТ ТРАНСФОРМАНТ ДИСКРЕТНОГО КОСИНУСНОГО ПЕРЕТВОРЕННЯ

На сьогоднішній день для зниження обсягів відеоінформації використовуються технології компресії зображень, однак характеристик, які забезпечуються існуючими методами, недостатньо для їх обробки в режимі реального часу. Отже, розробка методу компресії зображень для зниження їх обсягів при збереженні заданої якості візуалізації є актуальною задачею. Метою роботи є розробка методу компресії зображень з попереднім квантуванням компонент трансформант дискретного косинусного перетворення.

Запропонований метод стиснення містить в собі шість етапів.

Етап 1. Перетворення зображення з моделі кольорового опису RGB в кольороворізносне перетворення YUV.

Етап 2. На даному етапі виконується ДКП. Завдяки властивості подільності ядра базисної функції дискретне косинусне перетворення виконується в два кроки. Спочатку здійснюється одномірне ДКП для стовпців масиву вихідного зображення, потім виконується одномірне ДКП для рядків масиву.

Етап 3. Бінарний опис квантованих компонент трансформант на основі їх двійкового подання, дозволяє враховувати особливості розподілу нульових областей в бітовому описі трансформант (БОТ), а саме враховувати особливості розміщення та довжини областей нульових елементів для різних позицій бінарного опису трансформанти

Етап 4. Формування масивів довжин серій двійкових елементів в напрямку бітових площин БОТ, що дозволяє сформувати найбільш довгі серії нульових елементів.

Етап 5. Адаптивно-одноосновне кодування адаптивних одноосновних позиційних (АОП) чисел, утворених для стовпців масиву довжин серій двійкових елементів.

Етап 6. Побудова кодограми стислого представлення трансформанти на основі послідовності кодових слів, що містять інформацію про код АОП чисел.

В результаті досліджень одержала подальшого розвитку технологія стиснення зображень із втратами якості на основі їх попереднього трансформування. Відмінності від відомих методів полягають у тому, що: для побудови масивів довжин серій ДЕ використовується індексний принцип позиціонування елементів на основі їх координати в загальній послідовності, що дозволяє скоротити час формування масиву довжин серій; використання адаптивно-одноосновного кодування позиційних чисел дозволяє скоротити часові затримки на обробку та скоротити надмірність, обумовлену особливостями розподілу довжин серій двійкових елементів у бінарному описі трансформанти без використання додаткової службової інформації. Структура кодограми стислого представлення визначається за дворівневим принципом: на рівні грубої оцінки визначається кількість кодових слів, а на рівні уточнення забезпечується скорочення кодової надмірності, що дозволяє виключити переповнення машинного слова і скоротити кількість кодової надмірності.

УДК 004.023

Вікулов П.О.
(Національний авіаційний університет, Україна)

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ХМАРНИХ ТЕХНОЛОГІЙ ТА МЕТОДИ ЇХ ЗАХИСТУ

Актуальність. Розвиток комп'ютерних мереж ставить перед захистом інформації нові завдання. З появою хмарних технологій почалася масова міграція систем на віртуалізовані машини, що в свою чергу розширило спектр завдань захисту інформації. На сьогоднішній день вже відомо досить багато загроз безпеці користувацьких даних і створені методи для протидії цим загрозам, однак питання реалізації цих методів у віртуалізованих системах досить залишається відкритим.

Мета – розгляд основних загроз, які притаманні хмарним технологіям та пошук ефективних методів протидії цим загрозам.

Однією з основних проблем при використанні віртуалізованих систем є – забезпечення належного контролю та керування даними. Неможливо гарантувати, що усі ресурси хмарного сервісу враховані, а віртуальні машини перебувають під повним контролем. Такі загрози відносяться до високорівневих, адже охоплюють усю систему керування віртуалізованою системою. Захист від даного типу загроз реалізується шляхом індивідуального проектування системи безпеки хмарного сервісу, що потребує використання моделі керування ризиками.

Основна перевага віртуальних сервісів – динамічність. Можна легко створити нову віртуальну машину, керувати її станом або перемістити на інший фізичний сервер. Однак, це призводить до того, що вразливості систем та додатків розповсюджуються по мережі хаотично і можуть бути виявлені лише після певного проміжку часу. Тому актуальним методом протидії є фіксація стану системи безпеки незалежно від її стану та місцезнаходження.

Окрім загальних та зовнішніх загроз, існують також внутрішні загрози безпеці хмарного сервісу. Хмарні та локальні сервери використовують одні і ті ж операційні системи та додатки. Це означає, що існує загроза віддаленого злому або зараження хакерським програмним забезпеченням усього віртуалізованого сервісу.

При розширенні віртуалізованого сервісу периметр мережі вже не є досить чітким, і загальний рівень безпеки системи визначається по найменш захищеній частині мережі, що в свою чергу веде до появи потенційних загроз безпеці усього хмарного сервісу. Захист забезпечується створенням індивідуальної системи безпеки, яка переміщує мережний периметр до віртуальної машини.

Висновки. Для захисту хмарних технологій повинен використовуватися комплексний підхід з урахуванням особливості кожного проекту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Карр Н. Великий переход. Революция облачных технологий, — Москва 2013. — 272 с.

2. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — 379 p.

УДК 004.056.53(044)

Галата Л.П., Козюберда О.В.
(Національний авіаційний університет, Україна)

МОДЕЛЮВАННЯ БЕЗПЕКИ КОМП'ЮТЕРНОЇ СИСТЕМИ

В наш час швидкими темпами розвиваються інформаційні технології, вони проникають в усі сфери людської діяльності, тому дуже гостро постає питання інформаційної безпеки. З кожним днем технології обробки інформації удосконалюються, а разом з цим підвищуються вимоги до практичних методів забезпечення безпеки.

Звичайно, не існує універсальних методів для забезпечення безпеки, адже кожна комп'ютерна система має свої особливості. Тому перш ніж створювати модель безпеки для певної комп'ютерної системи необхідно зробити повний її аналіз.

Моделі безпеки грають важливу роль в процесах розробки і дослідження захищених комп'ютерних систем, адже вони забезпечують системотехнічний підхід.

Проблеми безпеки в комп'ютерній системі розглядаються з точки зору аналізу і дослідження умов, правил, порядку, запитів на доступ, при яких система, спочатку знаходячись в безпечному стані, за кінцеве число переходів перейде також в безпечний стан.

Існують три складові і, відповідно, три, хоча і взаємозв'язаних, але різних напрямів захисту комп'ютерної інформації - забезпечення конфіденційності інформації, забезпечення цілісності даних, забезпечення збереження і працездатності даних.

Перш за все моделі безпеки комп'ютерних систем, що забезпечують ті чи інші, з трьох складових, безпеки інформації, а саме технології і протоколи парольної автентифікації, криптографічні методи та засоби захисту інформації і т.п..

Конкретна модель безпеки деталізує і формалізує загальний принцип розмежування доступу на основі однієї з політик безпеки, а іноді деякій їх сукупності.

У конкретній комп'ютерній системі будуються і реалізуються оригінальні програмно-технічні рішення, що утілюють моделі безпеки, у тому числі структуру, функції, програмно-технічне втілення монітора безпеки.

Детальніше зупинимося на методах забезпечення інформаційної безпеки.

Існують:

Теоретичні:

1) формалізація процесів зв'язаних із забезпеченням інформаційної безпеки;

2) обгрунтування коректності і адекватності систем забезпечення інформаційної безпеки.

Організаційні:

1) управління інформаційної безпеки на підприємстві.

Сервіси мережевої безпеки:

1) ідентифікація і автентифікація;

2) розмежування доступу;

3) протоколювання і аудит;

4) засоби захисту периметра;

5) криптографічні засоби захисту.

Інженерно-технічні методи:

1) захист інформації від витоку по технічних каналах.

Правові методи:

1) відповідальність;

2) робота з державною таємницею;

3) захист авторських прав;

4) ліцензування і сертифікація.

Таким чином, можна зробити висновок, що основними задачами, які вирішує модель політики безпеки комп'ютерної системи є: вибір і обґрунтування базових принципів архітектури захищених комп'ютерних систем; підтвердження властивостей (захищеності) систем; складання формальної специфікації політики безпеки. У конкретній комп'ютерній системі розробники мають будувати і реалізувати оригінальні програмно-технічні рішення, що утілюють моделі безпеки, у тому числі структуру, функції, програмно-технічне втілення монітора безпеки. Для кожної комп'ютерної системи моделювання безпеки індивідуальне, адже кожна комп'ютерна система має свої особливості, які необхідно враховувати при розробці моделі безпеки.

УДК 004.724

Гетьманенко О.В.
(Національний технічний університет України "КПІ", Україна)

МАРШРУТИЗАЦІЯ НА ОСНОВІ МОДИФІКОВАНОГО АЛГОРИТМУ ДЕЙКСТРИ

У сучасних мобільних мережах значення показників якості обслуговування багато в чому залежить від ефективності рішення задач маршрутизації.

Одним із напрямків розвитку сучасних протоколів маршрутизації є розподілення навантаження. Реалізація технологій балансування навантаження на практиці дозволяє оптимізувати рішення задачі маршрутизації і ефективно використовувати ресурси мережі, в результаті чого покращуються значення показників якості обслуговування.

Удосконалення протоколів маршрутизації обумовлені переглядом математичних моделей і методів, покладених в їх основу. Виходячи з цього актуальною науковою і прикладною задачею являється здійснення відомих чи розвиток нових моделей маршрутизації з балансованим завантаженням.

На сьогоднішній день існує достатньо велика кількість множин математичних моделей маршрутизації. В комп'ютерних мережах теоретично можуть використовуватися різноманітні методи (алгоритми) маршрутизації, що забезпечують різні властивості і залежать від структурно-функціональних особливостей мережі і вимог, що пред'являються до якості її функціонування. На рисунку 1 представлена одна із можливих класифікацій методів багатошляхової маршрутизації за типом математичного підходу, які можна розбити на 2 групи:

- потоково-орієнтовані;
- графокомбінаторні.

Рисунок 1. Методи маршрутизації за типом математичного підходу

Як показав аналіз, протоколи маршрутизації спираються здебільшого на графові моделі. Вони являються статичними і забезпечують початкове резервування каналів. В основу графокомбінаторних алгоритмів покладено математичний опис мобільних мереж у вигляді орієнтованого чи неорієнтованого графа з наступним використанням комбінаторних алгоритмів пошуку множини найкоротших шляхів між заданими парами вузлів мережі.

Найпоширенішим є застосування алгоритму Дейкстри, який вирішує задачу пошуку найкоротшого шляху у зваженому орієнтованому графі в тому випадку, коли ваги ребер невід'ємні. Час роботи алгоритму становить:

$$O(N^2 + M),$$

де: N – кількість вершин;

M – кількість ребер.

При застосуванні класичного алгоритму для пошуку шляхів, що не перетинаються, послідовність дій має наступний вигляд:

1. пошук найкоротшого шляху по всьому графі;
2. пошук другого маршруту (вузли знайденого першого - відкидаються);
3. пошук наступних шляхів (відкидаємо вершини використані у попередніх маршрутах).

Загальна формула для знаходження складності k шляхів, що не перетинаються, обраховується наступним чином:

$$O\left(\sum_{j=1}^{k}\left(N_{V_j}\right)^2\right),$$

де: N – загальна кількість вершин мережі;

k – кількість шляхів, що не перетинаються;

N_{V_j} – кількість пройдених вершин для знаходження шляху L_j, якщо $N_{V_j} = L_j \rightarrow N_{V_j} = 0.$

Тобто ми бачимо циклічний процес пошуку з відкиданням попередньо знайдених шляхів (використаних вузлів у маршрутах). Було запропоновано модифікацію даного алгоритму для зменшення часової складності (збільшення швидкості роботи):

1. знайти найкоротший шлях звичайним алгоритмом Дейкстри;
2. розбити граф на дві множини (попередньо знайденим шляхом);
3. відкинути сусідні вузли, що межують зі знайденим попереднім шляхом;
4. здійснювати пошук класичним алгоритмом Дейкстри у сформованих незалежних областях.

У цьому випадку розрахунок часової складності проводиться за наступною формулою:

$$O\left(N^2 + \sum_{i=2}^{k}\left(N - \sum_{j=1}^{k-1} N_{L_j}\right)^2\right),$$

де: N – загальна кількість вершин мережі;

k – кількість шляхів, що не перетинаються;

N_{L_j} – кількість вершин шляху L_j .

Саме розбиття графа на дві незалежні області призводить до значно кращого результату і швидкості роботи.

Запропонована модель маршрутизації проаналізована для графу розмірністю 30 вершин. Розрахункові дані представлено у вигляді графіка (АД – алгоритм Дейкстри).

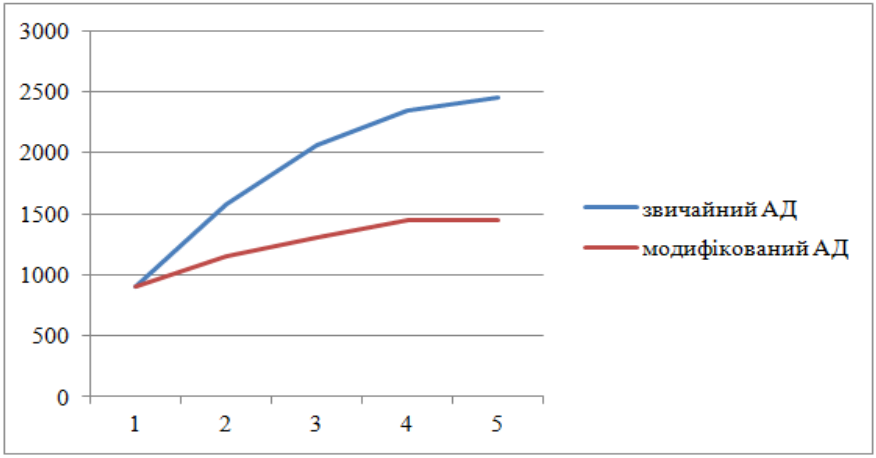


Рисунок 2. – Порівняння часової складності двох алгоритмів

Порівняння рішення задач маршрутизації в рамках запропонованої моделі зі звичайною моделлю (без використання розбиття) свідчить про доцільність застосування модифікованого методу, оскільки він дозволяє скоротити час пошуку вдвічі.

Отож, розробка все нових і нових методів багатошляхової маршрутизації має значний прикладний і теоретичний інтерес. Про це свідчить кількість робіт і публікацій, які присвячені оптимізації мобільних систем.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Mrs Soumyashree Sahoo. Secure Routing in Wireless Sensor Networks / Mrs Soumyashree Sahoo, Mr Pradipta Kumar Mishra, Prof. Dr. Rabi Narayan Satpathy // IJCSI International Journal of Computer Science Issues .- 2012.-Vol.9, №1.- P.189-191.*
2. *Кулаков Ю.А. Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности / Кулаков Ю.А., Лукашенко В.В., Левчук А.В. // Науково-Практичний Журнал «Захист Інформації».- 2011.-Т.2, №51.-С.5-10.*
3. *Кулаков Ю.А. Разработка и моделирование процесса безопасной многопутевой передачи информации в мобильных сетях / Кулаков Ю.А., Коган А.В., Пирогов А.А. // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: збірник наукових праць. – К.: Век+, 2011. – № 54. – С. 145-149.*
4. *Шувалов В.П. Классификация методов многопутевой маршрутизации / Шувалов В.П., Варакснна И.Ю // Т-Comm. 2014. №1. – С. 29-32.*

УДК 681.3.07

Глінський Б.В., Павлов В.Г., к.т.н.
(Національний авіаційний університет, Україна)

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ЗА ДОПОМОГОЮ МЕТОДУ “SAAS”

Відносини у сфері інтелектуальної діяльності регулюються цілою низкою актів цивільного законодавства України. Оскільки програми теж є результатом творчої діяльності людей, то на них також поширюються права інтелектуальної власності. Але крім законодавчих заходів програми повинні мати надійний захист від неліцензійного використання, яке, на жаль, дуже поширено у світі, зокрема, в Україні.

Розглянутий ряд заходів та засобів захисту програмного забезпечення (ПЗ) від несанкціонованого використання. Більшість з захисних механізмів реалізовано у вигляді вбудованого програмного коду. Це обмежує можливість неліцензійного використання ПЗ, але не обмежує доступу до самих програм. Тому врешті – решт цей захисний механізм зламується або відключається. Використання ПЗ з дистанційним інтерфейсом виключає безпосередній контакт користувача с програмним кодом, що значно посилює захищеність програм. Тому варто більш детально розглянути методи “SaaS” (software as a service).

Досліджено та проаналізовано моделі хмарного розміщення: приватна, публічна, громадська, гібридна. Здійснено огляд основних їх властивостей, серед яких самообслуговування на вимогу, широкий мережевий доступ, об'єднання ресурсів у пули, миттєва еластичність, вимірювані сервіси.

Застосована класифікація “хмар” відповідно рівнів: програмне забезпечення як послуга, обладнання як послуга, комп'ютер як послуга, робоче оточення як послуга, дані як послуга, комунікація як послуга, моніторинг як послуга, інфраструктура як послуга, платформа як послуга, безпека як послуга, все як послуга.

Також визначені основні атаки на даний метод захисту. Серед них: функціональні атаки на елементи “хмари”, традиційні атаки на ПЗ, атаки на клієнта, загрози віртуалізації, віток персональних даних, втрата даних, викрадення трафіку, “зловживання” можливостями хмар.

Здійснено огляд методів захисту “Saas” технології, визначено основні напрями: фізичний захист, авторизація, автентифікація, адміністрування, зберігання даних, управління вразливостями, безпека системи, шифрування, управління змінами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. J. Brodkin. 5 problems with Saas Security. – http://www.networkworld.com/article/2219462/saas/5-problems-with-saas-security.html

2. Mark O'Neill, Vordel. SaaS, PaaS, and IaaS: A security checklist for cloud models. – http://www.csoonline.com/article/2126885/cloud-security/saas--paas--and-iaas--a-security-checklist-for-cloud-models.html

УДК 004.056

Гулак Н.К., к.т.н., Маленовський О.Ю.
(Національний авіаційний університет, Україна)

АВТЕНТИФІКАЦІЯ ТА РОЗПІЗНАВАННЯ ЗА РАЙДУЖНОЮ ОБОЛОНКОЮ

Метод ідентифікації особи за райдужною оболонкою є одним з найбільш точних серед біометричних методів, тому що райдужна оболонка ока є унікальною характеристикою людини. Розглянемо переваги та недоліки цього методу.

Час первинної обробки зображення в сучасних системах приблизно 300 - 500мс, швидкість порівняння отриманого зображення з базою має рівень 50000-150000 порівнянь в секунду на звичайному персональному комп'ютері. Така швидкість порівняння не накладає обмежень на застосування методу у великих організаціях при використанні в системах доступу.

Розрізняють активні і пасивні системи розпізнавання [1]. У системах першого типу користувач повинен сам налаштувати камеру. Пасивні системи простіше у використанні, оскільки камера в них налаштовується автоматично. Висока надійність цього обладнання дозволяє застосовувати його навіть у виправних установах.

Переваги методу. Статистична надійність алгоритму. Захоплення зображення райдужної оболонки можна проводити на відстані від декількох сантиметрів до декількох метрів. Райдужна оболонка захищена від пошкоджень і майже не змінюється в часі. Так само, можливо використовувати високу кількість методів, що захищають від підробки.

Недоліки методу. Ціна системи, заснованої на райдужній оболонці вище ціни системи, заснованої на розпізнаванні пальця або на розпізнаванні особи. Низька доступність готових рішень [2].

З появою нового і більш потужного апаратного забезпечення і більш досконалих програм цілком можно очікувати , що біометрія стане основним інструментом ідентифікації особи.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Моніч К.І. Новий підхід до побудови коду райдужної оболонки ока /К.І. Моніч //Искусственный интеллект. - №3. – 2010. – С. 356-362.

2. Роберт Т. Кэррол. Иридодиагностика //Энциклопедия заблуждений: собрание невероятных фактов, удивительных открытий и опасных поверий. — М.: «Диалектика», 2005. — С. 212-214.

УДК 004.056.5

Гулак Н.К., к.т.н.;Топал О.О.
(Національний авіаційний університет, Україна)

МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Системи виявлення мережевих вторгнень і виявлення ознак атак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем. Найбільш ефективним профілактичним заходом щодо захисту комп'ютера є раннє виявлення мережевих атак або проактивні засоби захисту [2].

Технологія проактивних засобів захисту від мережних атак повинна вирішувати такі завдання [1]:

-розпізнавання відомих атак і попередження про них відповідного персоналу;

-«розуміння» часто незрозумілих джерел інформації про атаки;

-зниження навантаження на персонал, що відповідає за безпеку, від поточних рутинних операцій з контролю за користувачами, системами та мережами;

-можливість управління засобами захисту не експертами в галузі безпеки;

-контроль всіх дій суб'єктів корпоративної мережі.

Одним із засобів захисту комп'ютера при раньому виявленні мережевих атак – це встановлення програмного комплексу, який контролює зміст трафіку. Завдяки своєчасним заходам можна виявляти різні види шкідливих програм. Такі комплекси функціонують на мережевому рівні за моделлю OSI, здійснюючи контроль встановлюваних з'єднань, аналіз структури та вмісту мережевих пакетів [3]. Механізм контролю та аналізу статистики встановлюваних з'єднань дозволяє виявити спробу сканування системи або проведення атаки виду «відмова в обслуговуванні» (одночасно відкривається безліч з'єднань з яких-небудь сервісом).

Часто системи виявлення атак можуть виконувати функції, які істотно розширюють спектр їх застосування, наприклад:

-контроль ефективності міжмережевих екранів;

-контроль вузлів мережі з невстановленими оновленнями або вузлів із застарілим програмним забезпеченням;

-контроль електронної пошти.

Усунувши причини виникнення атак, тобто виявивши і усунувши уразливості, адміністратор тим самим усуває і сам факт потенційної реалізації атак, що дає можливість плідному використанню часу і досвіду фахівців в області інформаційної безпеки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Климков С.М. Методы и модели противостояния компьютерным атакам /С.М. Климков – Люберцы: КАТАЛИТ, 2008. – 316 с.

2. НД ТЗІ 1.1-003-9 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua.

3. Шангин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шангин – М.: ДМК Пресс, 2010. – 544 с.

УДК 004.728.4 (043.2)

Дрововозов В.І., к.т.н., Мартинова О.П., к.т.н.,
Толстікова О.В., к.т.н.
(Національний авіаційний університет, Україна)

ЗАСТОСУВАННЯ РІШЕНЬ ВІРТУАЛІЗАЦІЇ В ЦЕНТРІ ОБРОБКИ ДАНИХ

У структурі центру обробки даних (ЦОД) можна віртуалізувати серверний сегмент вцілому. 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.

Застосування рішень віртуалізації можливо при використанні гіпервізорів (згідно з вимогами до сервісів). Подібні рішення віртуалізації представлені гіпервізором *VMware ESXi*, який має високу швидкодію та широкими можливостями конфігурування. Важливою вимогою до системи віртуалізації є підтримка операційних систем, які будуть використані для виконання необхідних сервісів.

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.

Модель роботи гіпервізора при застосуванні рішень віртуалізації, яка пояснює загальний принцип віртуалізації, надана на рис. 1.

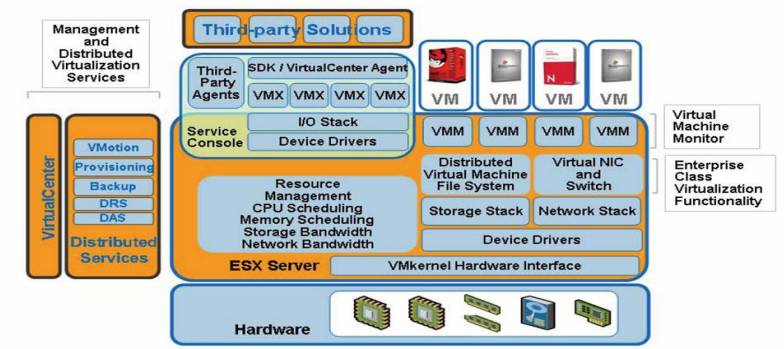


Рис. 1. Модель роботи гіпервізора

Переваги застосування подібних рішень віртуалізації дуже значні:

- підвищення відмовостійкості;
- можливість плавного оновлення та нарощування апаратної платформи;
- збільшення можливостей масштабування інформаційної системи;
- ізоляція служб;
- можливість гнучкого розподілу ресурсів між службами.

Використання системи віртуалізації *VMware vSphere* дозволить ефективно розподілити сервіси центру обробки даних, зменшити кількість простоїв і непродуктивної роботи серверного обладнання. Так само за допомогою цієї

системи буде 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, повинне бути достатньо для виконання всіх сервісів.

Важливо передбачити використання рішень віртуалізації при виборі програмної та апаратній складової, а також при проектуванні мережі ЦОД.

Програмна складова центру обробки даних - комплекс керуючих, обробляючих програм і систем моніторингу та обробки журналів, які розподіляють обчислювальні ресурси між сервісами ЦОД, регулюють і визначають роботу цих сервісів. Вибір програмного середовища можна розбити на складові: система віртуалізації, системи керування, системи моніторингу, система збору та обробки журналів.

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. Ще одна вимога – це можливість установки різних рівнів доступу для індивідуальних користувачів або груп користувачів, що вимагає відповідної підтримки з боку всіх систем.

Програмне середовище для реалізації системи віртуалізації. Кількість систем повної віртуалізації промислового рівня відносно невелике, це *VMware vSphere, Microsoft Hyper-V, Citrix XenServer і RedHat RHEV.*

Причини вибору рішення VMware по віртуалізації. Пропонуємо рішення по віртуалізації засноване на *VMware vSphere* – надійній і перевіреній платформі віртуалізації.

VMware vSphere – це комплексна платформа віртуалізації серверів, що надає широкий вибір можливостей:

- підвищення коефіцієнта використання серверних ресурсів на 80%;
- скорочення капітальних і експлуатаційних витрат на 50%;
- коефіцієнт консолідації серверів 10:1 або вище.

Таким чином, система віртуалізації *VMware* є підходящою для використання в ЦОД. Апаратна підтримка віртуалізації з боку обладнання, на яке буде встановлено гіпервізори, повинна бути передбачена при виборі апаратної складової [1,2].

Для виконання вимог по відмовоспроможності, балансуванню навантаження та максимального ефективного використання ресурсів у системі віртуалізації *VMware vSphere* є ряд систем і механізмів керування, розподілу й балансування.

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

УДК 004.75

Жолдаков О.О., Жолдаков А.О.
(Національний авіаційний університет, Україна).

ОСОБЛИВОСТІ МОДЕЛЮВАННЯ ЗАДАЧІ ОПЕРАТИВНОГО ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ПОВІТРЯНИХ СУДЕН

Комплекс робіт, який виконується після кожної посадки літака і перед його вильотом і включає оцінку технічного стану повітряного судна (ПС) після польоту, виконання робіт по підготовці ПС до стоянки, забезпечення справності і працездатності ПС, усіх його систем на землі і в польоті відноситься до сфери оперативного технічного обслуговування (ТО). Щоб виконати ТОПС необхідно вибрати варіант організації підготовки літака, що забезпечить своєчасне відправлення за розкладом; визначити необхідний термін для заправки літака і розвантаження; визначити необхідний терміну завантаження літака залежно від його маси та розміщення вантажу.

В залежності від типу літака і наявних технічних ресурсів складаються відповідні технологічні графіки, що встановлюють порядок організації робіт для кожного варіанту робіт при мінімально можливій тривалості стоянки. При розв'язанні цих задач для кожного конкретного рейсу, необхідно вибрати варіант організації робіт, що забезпечить своєчасну підготовку літака. Якщо задана розписом польотів тривалість стоянки літака більше мінімально можливої для вибраного варіанту, необхідно виконати перерахунок параметрів окремих операцій і подій процесу.

Особливості технічної підготовки повітряних суден до польоту вимагають насамперед значної динаміки виконання, урахування безперервної зміни інформації щодо виявлених відмов і дефектів, а поряд з цим необхідно дотримуватись строгої детермінованості у виконанні всього комплексу робіт; крім того виникає необхідність в обслуговуванні позачергових рейсів, що вимагає перерозподілу ресурсів.

Керування такою системою можливе лише за умов застосування сучасних обчислювальних засобів для автоматизації збору і обробки інформації та пошуку об'єктивно можливих оперативних рішень.

Якщо в основу вибору оптимальної моделі технічної підготовки повітряних суден до польоту покласти критерій мінімізації відхилень моментів порушення регулярності у часі, то постає необхідність оцінки основних параметрів автоматизованої системи ТО. Підвищення ефективності експертних оцінок цих параметрів надає математичний апарат теорії нечітких множин.

Припускається, що модель оптимального вирішення задачі оперативного технічного обслуговування повітряних суден не може бути детермінованою, чи навіть стохастичною, оскільки вектор змінних стану, що характеризує процес обслуговування не підлягає кількісному прогнозуванню.

Таким чином, формалізація глобальної цілі та дерева цілей, як і системи обмежень, стає нетривіальною задачею, що пов'язано з особливостями об'єкту керування, професійним рівнем самих експертів, методом обробки та корегування їх оцінок.

Найважливішим компонентом прийняття рішення в нечітких умовах є представлення нечітких цілей $G_i\left(i=\overline{1,n}\right)$ і нечітких обмежень $C_j\left(j=\overline{1,m}\right)$, як розплив-

частих множин у просторі альтернатив X з функціями приналежності $\mu_{G_i}(x)$ і $\mu_{C_j}(x)$ відповідно. При цьому підході під рішенням розуміється розпливчаста множина виду

$$D = G_1 \bigcap G_2 \bigcap ... \bigcap G_n \bigcap C_1 \bigcap C_2 \bigcap ... \bigcap C_m,$$

функція приналежності якої визначається співвідношенням

$$\mu_D(x) = \mu_{G_1}(x) \wedge \mu_{G_2}(x) \wedge ... \wedge \mu_{G_n}(x) \wedge \mu_{C_1}(x) \wedge \mu_{C_2}(x) \wedge ... \wedge \mu_{C_m}(x).$$

Оптимальне рішення, якщо воно існує, визначає як субнормальну підмножину $D^m \subset D$, що задана умовою

$$\mu_D(x) = \begin{cases} \max \mu_D(x) & \text{для } x \in K \\ 0 & \text{для } x \notin K \end{cases}$$

де K — множина тих точок у просторі альтернатив X, для яких функція $\mu_D(x)$ має максимальне значення.

Вибір експертом лінгвістичних значень з терм-множин здійснюється відповідно до його уявлень про нечітку мету і нечітке обмеження для відповідної змінної.

Тоді під рішенням розуміється розпливчаста множина, функція приналежності якої визначається співвідношенням

$$\mu_D(x) = \sum_{j=1}^{n} \alpha_{A_{ij}} \mu_{A_{ij}}(u) + \sum_{k=1}^{m} \beta_{C_{ik}} \mu_{C_{ik}}(u),$$

де $\alpha_{A_{ij}}$ і $\beta_{C_{ik}}$ - коефіцієнти узгодження думок експертів.

Результуючі рішення, що відбивають узагальнену думку групи експертів щодо нечітко визначених параметрів задачі, виражаються опуклою комбінацією всіх цілей і обмежень, що прийняті експертами для кожної лінгвістичної змінної.

Викладений підхід прийняття рішень при формуванні параметрів в умовах нечіткої вихідної інформації дозволяє побудувати модель керування технічною підготовкою повітряних суден до вильоту адекватність якої залежить від фаховості експертів та способу обробки їх оцінок. Саме метод обробки результатів експертизи при формуванні результуючих рішень і форма їх представлення суттєво впливатиме на застосовність викладеного підходу до розв'язку задачі керування ТО ПС.

ВИКОРИСТАНІ ДЖЕРЕЛА:

1. Нечеткие множества и теория возможностей. Последние достижения: Пер. с англ./Под ред. Р.Р. Ягера. – М.: Радио и связь, 1986. 408 с.

2. Додонов А.Г. Методы принятия решений в автоматизированной системе управления предполетной подготовкой летательных аппаратов: монография/А.Г. Додонов, А.Е. Литвиненко, М.Г. Луцкий. – К.: НАУ, 2011. – 340 с.

3. "From computing with numbers to computing with words — from manipulation of measurements to manipulation of perceptions" in International Journal of Applied Math and Computer Science, pp. 307–324, vol. 12, no. 3, 2002.

УДК 004.056.53

Жуков І.А., д.т.н., Гузій М.М., к.т.н.
(Національний авіаційний університет, Україна)

МЕРЕЖЕВІ СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ СТРУКТУРОВАНОГО ТРАФІКУ

Виявлення мережевих атак є однією з найбільш актуальних проблем безпеки мережевих інформаційних технологій. В комп'ютерних мережах застосовуються активні засоби попередження атак - антивіруси, міжмережеві екрани, системи попередження вторгнень рівня хоста. Проте лише активних засобів виявлення атак недостатньо, проблема потребує комплексного підходу, зокрема використання адаптивних систем реального часу - мережевих систем запобігання вторгненням в комп'ютерні системи.

Мережеві системи попередження вторгнень *(Network-based Intrusion Prevention, NIPS*) відстежують трафік в комп'ютерній мережі і блокують підозрілі потоки даних. Системи *IPS* можна розглядати як розширення систем виявлення вторгнень *(IDS), IPS* повинна відстежувати активність в реальному часі і реалізовувати дії щодо запобігання атак. Можливі заходи - блокування потоків трафіку в мережі, відключення з'єднання, видача сигналів оператору. Зазвичай виділяють три етапи вторгнення: сканування мережі; вплив на вразливість; повторне отримання управління системою через завантажену програму, яка використовує недокументований вхід в систему. Функціонально *IPS* діляться на мережеві, вузлові та гібридні.

Архітектура типової *IPS* включає в себе наступні підсистеми:

- сенсорну підсистему, що збирає інформацію з захищається системи;
- підсистему виявлення вторгнень на основі аналізу даних сенсорів;
- підсистему зберігання - бази даних та знань;
- підсистему управління і конфігурації *IPS*;
- інтерфейс користувача та мережевий інтерфейс.

На практиці застосовують два підходи до виявлення вторгнень: методи, засновані на сигнатурах і методи, засновані на аномаліях. Сигнатурний метод на основі результатів порівняльного аналізу контрольованих даних з еталонними шаблонами вторгнень дозволяє виявити і класифікувати відомі вторгнення. Метод аномалій створює профілі нормальної поведінки контрольованого процесу і порівнює поточний стан процесу з його нормальним профілем. Метод, заснований на аномаліях, дозволяє виявити нові типи вторгнень, але має порівняно низьку надійність виявлення відомих типів вторгнень. Найбільш перспективним є метод виявлення вторгнень, який використовує методи інтелектуального аналізу числових послідовностей контрольованого процесу - характеристики мережевого трафіку.

Мережеві системи виявлення вторгнень аналізують мережевий трафік і при виявленні відхилень параметрів трафіку від «нормального» сигналізують про аномалію. Формальні *IPS* працюють за сигнатурним методом - параметри трафіку порівнюються з БД сигнатур і, в разі виявлення збігів, виявляється атака. Фізично неможливо оновлювати БД сигнатур формальних *IPS* реальному часі, збільшення обсягу БД сигнатур негативно позначається на продуктивності комп'ютерної си-

стеми. Вирішенням цієї проблеми є застосування систем виявлення вторгнень на основі виявлення аномальної активності або евристичних *IPS.* На даний час існує досить велика кількість евристичних *IPS*, що працюють на прикладному рівні. В області виявлення вторгнень на мережевому / транспортному рівнях досі не запропоновано системи, здатної працювати в реальному часі.

Для виявлення аномалій трафіку комп'ютерної мережі використовуються методи *Data Mining*. методи опорних векторів, штучних імунних систем та нейронних мереж, ймовірнісні моделі, методи мультифрактального та тензорного аналізу трафіку.

Одним з перспективних напрямів є створення *IPS* на основі методу кратномасштабного аналізу (КМА) трафіку, що передбачає подання його параметрів в різних часових масштабах [1]. Теорія вейвлетів є альтернативою класичному аналізу Фур'є і дає більш гнучку технологію обробки сигналів. Теорія вейвлетів дає зручний і ефективний інструмент для вирішення багатьох практичних завдань, зокрема аналізу мережевого трафіка [2].

Одна з головних ідей вейвлетного представлення сигналів полягає в поділі функцій наближення до сигналу на дві групи: апроксимуючу з досить повільною часовою динамікою змін і уточнюючу - з локальною і швидкою динамікою змін на тлі плавної динаміки. В основному вейвлет-перетворення ділять на дві групи: безперервне (CWT) і дискретне (DWT), в кожній з яких існує кілька різновидів. Технологія вейвлет-аналізу використовується в системах виявлення вторгнень, вона дозволяє розкладати сигнал на декілька частотних компонент для їх подальшого аналізу.

У роботі [3] для *NIPS* пропонується імовірнісна модель на основі аналізу послідовності характеристик мережевого трафіку. Серед ймовірнісних моделей найбільш перспективним є застосування динамічних байєсовскіх мереж (ДБС) , які описуються в просторі станів у вигляді орієнтірованних графів. Методи та алгоритми, засновані на використанні ДБС, перевершують інші імовірнісні моделі в точності опису модельованих процесів і гнучкості застосування, однак вимагають застосування більш трудомістких алгоритмів, ніж, наприклад, приховані Марківські моделі або фільтр Калмана.

Проведені експериментальні дослідження підтверджують перспективність запропонованих підходів для виявлення аномалій трафіку комп'ютерних мереж в часі, близькому до реального.

ВИКОРИСТАНІ ДЖЕРЕЛА:

1. Шелухин О.И., Панкрушин А.В. Сравнительный анализ характеристик обнаружения аномалий трафика методами кратномасштабного анализа Телекоммуникации и транспорт М., Том 8 №6, 2014. С. 65-71.

2. Тишина Н.А., Дворовой И.Г., Соловьев Н.А. Обнаружение вторжений на основе вейвлет-анализа сетевого трафика. // Управление, вычислительная техника и информатика. Вестник УГАТУ, Уфа, Т.14, №5(40), 2010. - С.188-194.

3. Арустамов С. А., Дайнеко В. Ю. Применение динамической байесовской сети в системах обнаружения вторжений // Научно-технический вестник информационных технологий, механики и оптики. — СПб.: НИУ ИТМО, № 3(79), 2012. — С. 128-133.

УДК 004.415.2 (043.2)

Журавель Н.В., Журавель С.В.
(Національний авіаційний університет, Україна)

ПРОБЛЕМИ ВЗАЄМОДІЇ СИСТЕМИ БУХГАЛТЕРСЬКОГО ОБЛІКУ 1С: БУХГАЛТЕРІЇ ТА ГЛОБАЛЬНОЇ СИСТЕМИ БРОНЮВАННЯ «GALILEO»

Успіх будь-якого підприємства і можливість його виживання залежать від здатності швидко адаптуватися до зовнішніх змін. У постійному прагненні підтримувати відповідність організації умовам зовнішнього середовища неможливо обійтись без корпоративної мережі та автоматизації процесу виробництва. Це виявляється в динамічному освоєнні нової продукції, сучасної техніки і технологій, застосуванні прогресивних форм організації праці, виробництва і керування, безупинному удосконалюванні кадрового потенціалу.

В умовах динамічності сучасного виробництва і суспільства керування повинне знаходитися в стані безупинного розвитку, що сьогодні неможливо забезпечити без дослідження тенденцій і можливостей, без вибору альтернатив і напрямків розвитку.

Різного роду нововведення виявляють себе на підприємствах у формі організаційного удосконалювання системи автоматизації, що вимагає уточнення окремих зв'язків, параметрів системи, застосування більш ефективних способів їхньої реалізації, підвищення рівня надійності і т.д. Організаційне удосконалення системи (чи підсистем) торкається вже не тільки окремих зв'язків, але й структури мережі в цілому. А це, у свою чергу, вимагає встановлення і забезпечення нових зв’язків, усунення зайвих зв'язків, істотної зміни функцій керування і способів прийняття управлінських рішень.

Розвиток і удосконалювання підприємства базується на ретельному і глибокому знанні діяльності організації, що вимагає проведення дослідження систем керування.

В час сучасних інформаційних технологій та розвитку мережевих засобів автоматизації роботи персоналу керівнику підприємства необхідно максимально використовувати можливості програмного забезпечення.

У бухгалтерській і банківській діяльності це особливо важливо, тому широке застосування бухгалтерських пакетів і програм, завдяки впровадженню яких підвищується оперативність обробки даних і вірогідність ділової інформації, приймаються більш об'єктивні фінансові й управлінські рішення.

Враховуючи широке поле застосування важко підібрати таке програмне забезпечення, яке б повністю задовольняло потреби підприємства, тому що надійність не завжди знаходиться поряд з гнучкістю налаштувань та ефективністю використання. В такій ситуації на допомогу стають системи, які мають власний, ефективний інструмент розробки нових модулів, простий у вивченні та використанні. Яскравим прикладом є продукт «1С:Підприємство».

З іншого боку для замовлень авіаквитків найбільшою популярністю користується глобальна система бронювання Galileo. Оригінальний інтерфейс та режими доступу зробили цей продукт надійним, але зовсім не інтегрованим з різноманітним бухгалтерським програмним забезпеченням.

Метою роботи є розробка інтерфейсу взаємодії цих двох систем для забезпечення найбільш ефективного їх використання (рис.1).

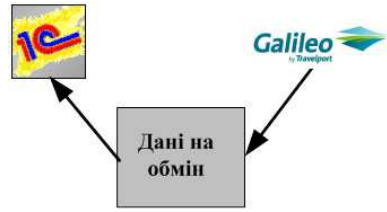


Рис.1. Взаємодія системи Galileo та «1С:Підприємство».

Даний модуль можливо буде використовувати для об'єднання не тільки системи Galileo, але й інших систем бронювання.

Під час робочого дня менеджер бронює велику кількість авіаквитків. Їх потрібно внести в базу та провести по бухгалтерії. Під час формування документів в базі 1С використовується не вся інформація представлена в Galileo, тому для цього потрібно проміжне сховище даних, яке б відповідало наступним вимогам:

- збереження даних в текстовому не запакованому форматі;
- можливість сортування даних за датою бронювання;
- можливість звернення за допомогою автоматизованих інструментів.

Логічним було б вивантаження даних по квитках у файл, який би зберігався у сховищі. Файли можливо відбирати за датою.

Система Galileo дозволяє використовувати віртуальні принтери, які друкують дані по бронюванню в файл. Це будуть текстові файли з усіма необхідними даними по квиткам, що були замовлені.

Для автоматизації відповідності даних з текстового файлу системи Galileo та документу, що заповнює менеджер в системі 1С було розроблено модуль, що пов'язує ці дві системи. Даний модуль є доповненням до конфігурації 1С.

Цей модуль дозволяє зчитувати необхідні дані з текстового файлу Galileo та автоматично формувати документи в системі 1С.

У докладі була розглядається проблема взаємодії двох окремих видів програмного забезпечення. Перший – система бронювання авіаквитків Galileo, другий – система бухгалтерського обліку «1С:Підприємство».

Поставлене завдання було досягнуто шляхом: встановлення віртуального принтера, який друкує білети в файл; за допомогою вбудованої мови програмування розроблено модуль, що зчитує дані з файлу-квитка і заносить їх у відповідні регістри документу 1С. Розроблений інтерфейс дозволяє: значно спростити роботу агентів; автоматизувати процес заносу заявок до систем бухгалтерського обліку для подальшої обробки; зменшити помилки при ручному занесенні заявок; підвищити ефективність роботи відділів замовлення та бронювання авіаквитків

Результати розробки можуть бути використані цілком або частково для розробки інших модулів для взаємодії з іншими системами бронювання. Будь-яка система, що дозволяє вигружати дані у зовнішній текстовий файл може бути пов'язана за допомогою цього модуля з системою «1С:Підприємство» шляхом модернізації інтерфейсу під конкретну структуру зовнішнього файлу.

УДК 004.415(043.2)

Іванілов Д.В.
(Національний авіаційний університет, Україна)

МУЛЬТИАГЕНТНА СИСТЕМА КОНТРОЛЮ МІСЬКОГО ТРАФІКУ

Можливість автоматичного регулювання міського трафіку в наш час перетворюється з абстрактної ідеї в практичні проекти завдяки, по-перше, розвиненим засобам швидкісної обробки великих масивів інформації, по-друге, наявності критичної маси досліджень та методів їх аналізу і організації, як то нейронні мережі, мультиагентні системи, та ін.

Необхідність комп'ютеризованої системи базується на оптимальному показнику користі до затрат порівняно з альтернативами – автопілоти, підземні та надземні шляхи, публічний транспорт, повітряні транспорти та ін. В цьому напрямі активно розвиваються корпорації з розробки пошукових систем, одним з результатів їх діяльності є карти навантаження на міські вулиці в реальному часі. Іншим можуть слугувати системи GPS, що будують маршрут з урахуванням показників вищевказаної системи.

Щоб побудувати «електронного регулювальника», потрібно визначитись з його можливостями, компетенцією та метою. Візьмемо за об'єкт впливу транспортний засіб (агент), що рухається міськими вулицями з пункту А в пункт Б. Мету роботи системи охарактеризуємо набором правил:

1. Агент має дістатись кінцевого пункту
2. Він повинен це зробити за мінімальний час
3. Вулиці міста повинні бути мінімально навантажені

Мети 2 та 3 можуть суперечити одна одній, але цей факт має бути використаний для наладки системи шляхом задання пріоритетів. Що стосується можливостей, чим більше їх в системи, тим легше їй виконувати свої обов'язки. Проте, на практиці можливості будь-якої системи, заснованої на взаємодії з людьми, є обмеженими. Зробимо перелік можливостей системи, які теж можна регулювати:

1. Система бачить конкретного агента в реальному часі
2. Система бачить агентів на певній ділянці в реальному часі
3. Система бачить всіх агентів в місті в реальному часі
5. Система знає одну чи обидві точки А та Б
6. Система знає маршрут агентів

Компетенції системи залежать від того, як користувач має намір змінювати маршрут агентів. Обмеження на використання доступних системі можливостей задано в її правилах, які можна доповнювати та редагувати (вище вказано лише базові). До можливостей системи можна віднести:

1. Попередження водіїв про пробки, рівень навантаження вулиць та їх прогноз
2. Перекриття вулиць
3. Перехід між двостороннім та одностороннім рухом вулиць

В роботі пропонується дослідити концепцію розробки такої системи та проаналізувати її можливості.

УДК 004:618.3.06 (043.2)

Кірхар Н.В., к.т.н., Гайдачук В.В.
(Національний авіаційний університет, Україна)

МЕТОДИ ТА ЗАСОБИ ПРОЕКТУВАННЯ ІНТЕРАКТИВНОЇ ВЕБ–ПЛАТФОРМИ ДЛЯ ВИВЧЕННЯ МОВИ ПРОГРАМУВАННЯ PHP

Процес навчання в сучасному індустріальному суспільстві не може бути реалізований без використання технічних засобів, що дозволяють повніше, глибше та з імітацією реальних умов освоювати як базові, так і професійні знання. Застосування з цією метою автоматизованих навчальних систем (АНС) покликане, зокрема, вирішити протиріччя між зростаючим обсягом навчальної інформації та обмеженими термінами навчання, між масовістю навчання і його індивідуалізацією, а також створити умови для якісної фундаментальної підготовки в поєднанні з одночасним освоєнням сучасних інформаційних технологій.

Почали з'являтись різного роду навчальні програми, викладені на різних сайтах. Вони допомагали навчати інших людей на відстані. Це було досить зручно і практично. І в наш час, на піку розвитку web'у ця тенденція піднялась на небувалі висоти. Завдяки інтеграції Інтернет-технологій та архітектури клієнт-сервер, процес впровадження та супроводу інформаційної системи суттєво спрощується при збереженні досить високої ефективності і простоти спільного використання інформації.

В якості мови програмування обрані: PHP – мова розробки програмного забезпечення для Web, написана розробниками Web і для розробників Web; ECMAScript – об'єктно-орієнтована мова програмування, призначена для проведення обчислень і маніпуляцій з обчислювальними об'єктами в середовищі виконання.

Вся структура сайту буде побудована на стандарті MVC, так як він пропонує найбільш оптимальний варіант побудови структури додатку. В результаті чого, проект можна легко розширювати і вдосконалювати, незалежно від його масштабів.

MVC – це конструкційний шаблон, який описує спосіб побудови структури проектованого додатку, сфери відповідальності та взаємодії кожної з частин в даній структурі. Шалена популярність даної структури в веб додатках склалася завдяки її включенню в два середовища розробки, які стали дуже популярними: Struts і Ruby on Rails. Ці два середовища розробки намітили шляхи розвитку для сотень робочих середовищ, створених пізніше.

Після проектування автоматизованої системи навчання, була отримана така картина файлової структури, яка зображена на рис. 1. Шаблон проектування MVC дозволив розробити власну реалізацію його принципів, що зробило додаток більш гнучким і дало можливість розширювати функціонал. Також стало можливим написання власних окремих модулів, які не будуть залежати від системи і можуть працювати повністю автономно.

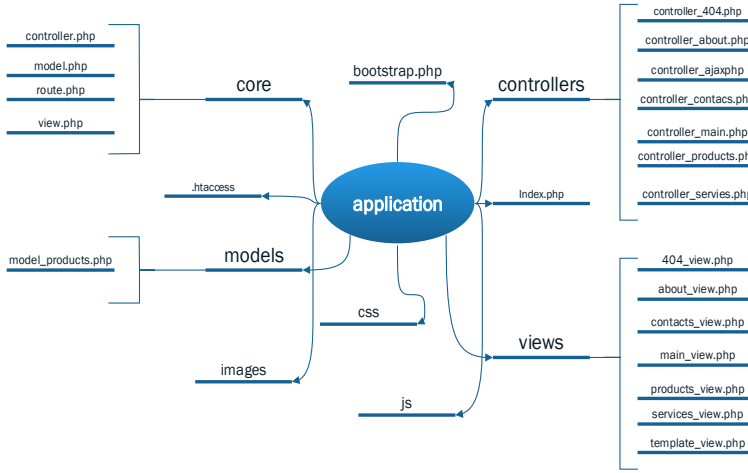


Рис. 1. Файлова структура системи

Призначення файлів системи:

- core – ядро додатка
- models – моделі додатка
- controllers – контролери додатка
- views – види додатка
- index.php – точка входу в додаток
- bootstartp.php – ініціалізує завантаження додатка, підключаючи всі необхідні модулі та ін..
- css – директорія зі стилями додатку
- images - директорія із зображеннями додатку
- js - директорія з файлами JavaScript
- core/roure.php – маршрутизатор
- .htaccess – файл додаткової конфігурація для веб – сервера Apache

В папці core зберігаються базові класи Model, View і Controller. Їхні нащадки зберігаються в директоріях controllers, models та views.

Для більшої безпеки розробленого продукту була створена єдина точка входу в систему, а всі «незадовільні» запити до платформи, перенаправляються на так звану сторінку 404, яка інформує користувача, що даної сторінки на сайті не існує. Всі інші запити, ведуть на методи відповідних класів, які в свою чергу формують сторінку і видають користувачу запрошену інформацію.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Гамма Э. Прийоми об'єктно-орієнтованого проектування. Патерни проектування / Э.Гамма, Р.Хелм, Р.Джонсон, Дж Влиссидес - СПб: Питер, 2001. — 368с.

2. Мазуркевич А. PHP: настольная книга программиста. / А. Мазуркевич, Д. Еловой – Мн.: Новое знание, 2006. — 495 с.

UDC 004.728.4(045)

Komnatna A.M., Kudrenko S.A.
(National Aviation University, Ukraine)

CHARACTERISTICS ANALYSIS OF MODERN WIFI ROUTERS

During the network technologies development the WIFI technologies was highly improved. The latest WIFI standard introduced in 2013 (by IEEE 802.11 group), with the aim to provide full communication with latest standard: 802.11a (introduced in 1999), 802.11b (2000), 802.11g (2003) and 802.11n (2007). That is why the most routers still dual-band.

In general, the work of routers based on previous standards was expensive because of widely used bandwidth (2.4GHz is used for most of devices, from cordless home phones to microwaves), 5GHz bandwidth allows to obtain much cleaner signal.

802.11ac standard provide the idea of "Beamforming". It means, that "smart signal" has been provided, which detects where connected devices are and increases signal strength specifically in their direction. So there is no need to place router in the center of planning area, to provide somewhat equivalent signal.

The newest standard also provide several other dimensions for speed increasing:

- More channel bonding, increased from a maximum of 40 MHz with 802.11n up to 80 or even 160 MHz (for speed increases of 117 or 333 percent, respectively).

- Denser modulation, now using 256 quadrature amplitude modulation (QAM), up from 64QAM in 802.11n (for a 33 percent speed burst at shorter, yet still usable, ranges).

- More multiple input, multiple output (MIMO). Whereas 802.11n stopped at four spatial streams, 802.11ac goes all the way to eight (for another 100 percent speed increase).

The speed of the devices has been increases in three times only during last two years. The theoretical maximum speed is given on figure 1.

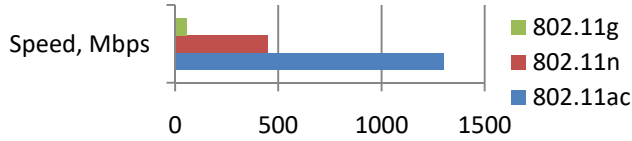


Fig.1 Speed comparison of different WIFI standards

The problem is these speeds are garbage. In the real world no-one ever gets close to theoretical speeds and the fastest 802.11ac real world speeds recorded in testing are around 720Mbps (90MBps). By contrast 802.11n tops out at about 240Mbps (30MBps) so the 3x estimate is still true, just much lower.

Considering of modern routers speed on different distance (5ft and 140ft — 1.524m, 42.672m), shown in fig.2.

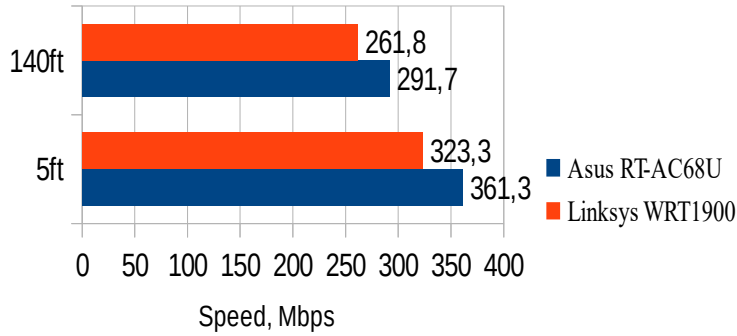


Fig. 2 Comparison of two routers speed on 5ft and 140 ft distance

Both devices has dual-core CPU, has UCB 3.0 ports for fast data transfer.

The RT-AC68U's crowning achievement was its throughput at 140 feet on the AC band. At 291.7 Mbps, the ASUS was 30 Mbps faster than the WRT1900AC and a blazing 80 Mbps faster than the category average of 211.2 Mbps.

Ironically, the only distance at which the RT-AC68U stumbled was 5 feet, where its 74.9 Mbps on the N band was neck and neck with the category average of 73.7Mbps and 10Mbps behind the Linksys WRT1900AC's showing. It's possible that the N-band signal is so strong at 5 feet that it actually crowds the band.

Modern technologies has great responsibilities relatively to distance, loses in speed became less, dependent on technology.

REFERENCES

1. *IEEE Standard for Information technology— Telecommunications and information exchange between systems Local and metropolitan area networks— Specific requirements - IEEE Std 802.11ac™-2013*

2. *802.11ac: The Fifth Generation of Wi-Fi, Technical White Paper, March 2014 — Cisco (http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.pdf)*

УДК 681.3.06

Корочкін О., к.т.н., Репета Я.
(Національний технічний університет України "КПІ", Україна)

АНАЛІЗ ЗАСОБІВ ПРОГРАМУВАННЯ ПОТОКІВ В БАГАТОЯДЕРНИХ КОМП'ЮТЕРНИЇ СИСТЕМАХ

Сучасний етап розвитку обчислювальної техніки пов'язаний з використанням багатоядерних комп'ютерних систем (БКС). Програмування для таких систем ґрунтується на застосуванні механізму процесів (потоків), який можна реалізувати за допомогою мов або бібліотек паралельного програмування. Час виконання паралельної програми в значній мірі залежить від часу обчислень, але також визначається часом, що витрачається на взаємодію процесів.

Метою даної роботи є пошук шляхів скорочення часу взаємодії процесів в БКС на основі аналізу, вибору та ефективного використання оптимальних засобів організації взаємодії процесів.

Існує дві моделі взаємодії процесів. Це модель, що ґрунтується на спільних змінних, та модель, що ґрунтується на посиланні повідомлень. Модель спільних змінних потребує вирішення двох завдань: завдання взаємного виключення та завдання синхронізації процесів. Засоби для вирішення цих завдань можна розподілити на три групи: низько рівневі примітиви (семафори, мютекси, події), механізм критичних секцій (критичні секції, замки, синхронізовані блоки), механізм моніторів (захищені модулі).

Затрати часу, що виникають при взаємодії процесів, пов'язані з наявністю в цих засобах операції блокування процесу в залежності від визначених умов. Оптимізація взаємодії процесів можлива за рахунок застосування атомарних (atomic та volatile) змінних та неблокуючих засобів комунікації. Важлива складова таких операцій – підтримка з боку операційної системи та на апаратному рівні. В бібліотеці POSIX використаються примітиви, що мажуть одночасно бути і блокованими і неблокованими.

Для моделі, що ґрунтується на посилці повідомлень, оптимізація можлива за рахунок застосування умовних (мова Ada) або асинхронних (бібліотеки MPI, PVM) операцій приймання/передавання.

В докладі представлені результати експериментальні дослідження ефективності розглянутих засобів комунікації процесів в реальній шести ядерної БКС при розробці пакету векторно-матричних операцій. Завдання взаємного виключення в таких задача пов'язано з використанням повних векторів або матриць. Значне скорочення часу виконання програми достягалось у випадку, коли виконувалось попереднє копіювання таких змінних в кожному потоці з розміщенням в кеш-пам'яті відповідного ядра. Програмування процесів здійснювалось з використанням мов паралельного програмування Java, C#, Ada та бібліотек WinAPI, OpenMP, MPI. Для реалізації взаємодії процесів були задіяні засоби комунікації всіх трьох груп, що дозволило визначити засоби, оптимальні для кожної задачі.

Висновки: застосування оптимальних засобів комунікації процесів дозволяє скоротити час, необхідний для організації взаємодії процесів (потоків). Для розглянутих задач покращення часу становило 8-9 відсотків.

УДК 004.056.53(044)

Кравченко О.Д.
(Національний авіаційний університет, Україна)

РЕАЛІЗАЦІЯ АЛГОРИТМІВ НА БАЗІ SOC СІМЕЙСТВА ZYNQ-7000

Сучасні системи управління космічними апаратами та іншими комплексними системи потребують впровадження сучасних високопродуктивних і компактних бортових обчислювачів [1], які мають широкий спектр можливостей і, в першу чергу, можливість реконфігурації. Такі технічні рішення можна ефективно реалізувати за допомогою сучасних кристалів Zynq-7000 [2]. Сімейство мікросхем Zynq-7000 засновано на архітектурі SoC й об'єднують процесор ARM Cortex-A9 та програмовану логіку Xilinx в одному кристалі. Реалізована за 28-нм технологією Zynq-7000 містить 2-ядерну процесорну систему ARM Cortex-A9 MPCore. Сімейство ARM Cortex [3] має розширену лінійку процесорів, що складають 3 групи різних за своєю побудовою і функціоналом: A, R та M серії.

Серія ARM Cortex-M відрізняється від інших своєю ергономічністю, малим споживанням енергії, високою енергоефективністю при відносно високих обчислювальних показниках. Серія Cortex-M є ідеальним рішенням для вбудованих пристроїв, таких як мікроконтролери, системи керування авто й т.д., де потрібно враховувати економічність, потужність і продуктивність.

Основною функцією ARM Cortex-R є забезпечення роботи в режимі реального часу. Ці процесори мають високопродуктивні обчислювальні можливості для вбудованих систем, швидку обробку інформації з високою тактовою частотою, де надійність, висока доступність, відмовостійкість, ремонтопридатність і детерміновані реакції в режимі реального часу мають важливе значення. Широке застосування знайшла ця лінійка процесорів в автомобільних блоках управління та інших пересувних засобах (двигуном, системою навігації, пристроях зберігання та обробки інформації,мобільних пристроях).

Процесори ARM Cortex-A є флагманом компанії та відрізняються серед інших високою продуктивністю (до 2,0 MFLOPS/МГц), наявністю технології ARM big.LITTLE, яка дозволяє регулювати енергоспоживання і заощаджувати близько 75% енергії процесора і збільшувати продуктивність на 60% в разі надходження багатьох поточних навантажень, мультимедійною-підсистемою NEON і модулем обробки операцій з плаваючою комою подвійної точності, а також пам'яттю L1– та L2–Cache і широким набором периферії. Саме такі процесори знайшли широке застосування у більшості мобільних телефонів (95% усіх процесорів), ноутбуках, планшетах, в сучасних системах управління та в платформі Zynq-7000.

Платформа Zynq-7000 EPP унікальна тим, що головна в ній – процесорна система ARM, а не програмовна логіка. Це означає, що система забезпечує загрузку процесора за включенням живлення (до старту логіки FPGA) і запускає необхідні операційні системи незалежно від комутованої матриці програмованої логіки. Після загрузки розробники можуть запрограмувати процесорну систему, щоб при необхідності конфігурувати програмовну логіку.

В багатьох електронних системах сьогодні використовується комбінація FPGA або з автономним процесором, або з ASIC із вбудованим процесором на одній

друкованій платі. Нова технологія дозволить створювати системи останнього покоління на базі одного кристалу Zynq-7000.

Кожен пристрій сімейства Zynq-7000 містить одне і теж процесорне ядро, але програмовна логіка і можливості вводу/виводу, залежно від його призначення дещо відрізняються. Тому Zynq-7000 мають широкий спектр застосування, наприклад: системи допомоги водію (driver assistant), медична діагностика та обробка зображень, системи обробки відеосигналів та інші.

Архітектура Zynq-7000 дозволяє реалізувати на замовлення, відповідно до вимог, програмовану логіку та процесорну систему. Це зробило можливим реалізацію унікальних та диференційованих функцій системи. Об'єднання програмовної логіки із процесорною системою дозволяє такий рівень продуктивності в яких 2-чіпове (two-chip) рішення (наприклад, ASSP з FPGA) не може зрівнятися у зв'язку з обмеженням пропускної здатності вводу /виводу, енергетичних ресурсів та затримки.

І найголовніше, можливість реконфігурації Zynq-7000 дозволяє нам самим,в залежності від задач, створювати алгоритми і програмувати ядро для них. Сама програма може бути написана мовою високого рівня програмування (C, C++, Java) і за допомогою ретранслятора переводитися у внутрішню мову ядра, сам програмний код вводиться в блок пам'яті, який пов'язаний з прикладним процесором APU, периферією вводу-виводу даних і програмовною логікою матриць з'єднанням ARM AMBA AXI, що і дозволяє ефективно вирішувати цей алгоритм.

Використання Zynq-7000 дозволяє вивести обчислювальні системи бортового обладнання на новий рівень, завдяки компактним розмірам, високій обчислювальній здатності, низькому енергоспоживанню, надійності та невисокій собівартості у порівняні з іншими. Крім того широкий спектр можливостей дозволяє створювати надскладні алгоритми, а здатність реконфігурації дозволяє змінювати конфігурацію всередині кристала Zynq-7000 як в процесі проектування,так і в процесі експлуатації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Опанасенко В.Н. Бортовые проблемно-ориентированные процессоры для аппаратной реализации алгоритмов управления космическими аппаратами / В.Н. Опанасенко, А.Н. Лисовый // Проблеми інформатизації та управління: Зб. наукових праць НАУ. – Вип. 3 (47). – Київ, 2014. – С. 70–74.

2. Zynq-7000 All Programmable SoC Overview. DS. 190 (v1.7). Xilinx Inc. October 8, 2014. – 21p. / available at http://www.xilinx.com/support/ documentation/data_sheets/ds190-Zynq-7000-Overview.pdf.

3. ARM Cortex processors, ARM Ltd. 2H 2014 Expiration QI 2015.-4p / available at http://arm.com/files/pdf/ARM-Cortex-Portfolio-2014.pdf.

УДК 004.72 (043.2)

Куклінський М.В., к.т.н., доцент
(Національний авіаційний університет, Україна)

ПРОБЛЕМИ УПРАВЛІННЯ ВЕЛИКИМИ МЕРЕЖАМИ З ВИКОРИСТАННЯМ SDN ТЕХНОЛОГІЙ

На сьогодні головною проблемою традиційних мереж є те, що вони занадто статичні. Чим більша мережа тим менш ефективно вирішуються задачі її управління. Стрімке зростання об'ємів трафіку та постійна зміна його структури спонукають розробників до підвищення процесу управління мережі, і як наслідок підвищення її динамічності.

В загальному випадку великі мережі можна розбити на дві підгрупи: масові та виробничі. До першої підгрупи відноситься всесвітня мережа Інтернет, до другої – корпоративні мережі підприємств.

Серед основних проблем управління великими мережами, які сьогодні вирішуються, можна виділити наступні:

– відсутність повної інформації про параметри і стан всієї мережі;

– запізнювання команд управління, і як наслідок затримка роботи всього процесу управління;

– проблеми розмірності мережі;

– проблеми об'єднання розрізнених програм управління мережевих пристроїв єдину систему управління, тощо.

Наряду з цим великі мережі повинні мати можливість до розширення та масштабування, що однозначно залежить від архітектури та функціональних можливостей обраних мережевих апаратно-програмних засобів.

Саме для вирішення проблеми управління великих мереж з урахуванням їх особливостей було запропоновано підхід який дістав назву – програмно-конфігуровані мережі (SDN). В таких мережах функції управління та функції передачі даних розділені. Декілька різнорідних пристроїв які регулюють передачу даних можуть знаходитися під контролем однієї управляючої програми або додатку. Крім того що таке розділення значно розширило можливості управління мережею, воно ще дозволило віртуалізувати фізичні мережеві ресурси.

Проте ефективність та продуктивність роботи мережі крім її оптимального управління, ще залежить від процесу передачі даних. Крім цього оптимальність управління ще дуже сильно залежить від затримок команд управління, які можуть передаватися із деяким запізненням. Тому необхідне дослідження та розробка засобів, які направлені на інтелектуалізацію технологій передачі та доставки даних за рахунок внутрішніх можливостей транспортної системи мережі.

У свою чергу необхідно враховувати, що як правило, інтелектуалізація може проводитися з метою підвищення визначення продуктивності зв'язки комутатор-контролер, а також продуктивності окремо контролера і комутатора. Це викликано особливостями архітектури програмно-конфігурованих комутаторів, в яких швидкість комутації вже відомого потоку близька до швидкості каналу. Тому характеристикою продуктивності в програмно-конфігурованих мережах може бути не тільки кількість пакетів в секунду, як в традиційних Ethernet мережах, а ще й кількість нових з'єднань в секунду.

УДК 004.056.53(044)

Левадний С. М., Петренко А. Б.
(Національний авіаційний університет, Україна)

МОНІТОРИНГ ТА ФОРМУВАННЯ СПИСКУ ВИКОНУВАНИХ ПРОЦЕСІВ В ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID

Актуальність: Виконано багато праць, в яких говориться про можливі вразливості інформаційних систем та відповідні загрози. Враховуючи те, що ОС Android за невеликий проміжок часу стала одною з найбільш популярних систем для різноманітних мобільних пристроїв. Не зважаючи на високу захищенність операційної ситеми жоден користувач не може бути повністю впевненим у цілковитій безпеці програмних додатків, що встановлюються на мобільний пристрій. Більшість різноманітних загроз для інформаційних систем реалізовується шляхом розроблення спеціалізованого програмного забезпечення, яке направлено на виконання дій, які прямо чи опосередковано призводять до витоку конфіденційної інформації. Реалізація контролю виконуваних процесів в операційній системі Android може попередити великий спектр загроз.

Новизна: Існують розроблені додатки, які направлені на часткове блокування процесів, визначених як несанкціоновані та такі, що можуть призвести до втрати інформації. Однак, найчастіше, користувач не впливає на список процесів, на які направлений моніторинг і рішення про безпеку того чи іншого процесу приймається на основі антивірусного аналізу вже після активування деструктивного програмного забезпечення на пристрій. Функціонують зазначені додатки на мобільному пристрої та частково можуть виконувати повний моніторинг процесів, що діють на даному пристрої під управлінням операційної системи Android. Новизна даного підходу полягає в тому, щоб запобігти активуванню програмного забезпечення, що несе загрозу, шляхом аналізу прав доступу додатків, побудови списку гарантовано безпечних додатків да надання можливості користувачу вибіркового керування правами доступу окремих додатків.

Постановка задачі: Постає необхідність у розробці програмного забезпечення, що виконує моніторинг процесів, які виконуються на мобільних пристроях, згідно певного зазначеного списку. Повинна бути передбачена можливість аналізу процесів, що активовні чи можуть бути запущені за так званим білим та чорним списком. У чорному списку зазначено, які процеси повинні бути заблоковані, робота всіх інших дозволяється. При використанні білого списку активними лишаються всі процеси, які визначені, робота всіх інших процесів припиняється. Також повинна бути передбачена можливість перегляду дозволів додатку, що встановлений та можливість вібіркової зупинки та блокування процесів користувачем. Таким чином, досягається порівняно більша безпека та захищеність інформації, що обробляється на мобільному пристрої.

Методика дослідження: На одному з мобільних пристроїв встановлюється декілька додатків. На пристрої формуються чорні та білі списки. Клієнтська програма сканує активні процеси на даному пристрої та виконує звірення з чорними та білими списками. Користувач вибірково блокує процеси та аналізує проведену роботу. Також перевіряє перевіряє дозволи окремих додатків та виконує вибіркове блокування дозволів.

Основні результати: Створене програмне забезпечення має високу швидкодію, яка визначається інтервалом спрацювання системного таймеру. Що в свою чергу

дозволяє оперативно виявляти та зупиняти шкідливі процеси. Інтервал спрацювання таймера можна задавати в налаштуваннях клієнтського програмного забезпечення. Користувач має можливість самостійно керувати чорними та білими списками або користуватися заздалегідь визначеними. При встановленні додатків є можливість звірити його з визначеним списком дозволених.

Використання: Розроблене програмне забезпечення може використовуватися в операційній системі Android 4.0 та вище.

Висновок: Одною з головних проблем безпеки при роботі з ОС Android, насамперед, є людський фактор.Дане рішення дозволяє попередити користувача або самостіно заблокувати шкідливі процеси зазанчені у чорному списку. Оскільки повний моніторинг всіх активних поцесів неможливий та не дозволяє у повній мірі бути впевненим у безпечності всіх процесів, то розроблений продукт вирішує дану проблему шляхом запровадження списку довірених програм. Розроблене програмне забезпечення виконує моніторинг та формує список процесів, які виконуються на мобільному пристрої під управлінням операційної системи Android. Дозволяє запобігти потраплянню деструктивного ПЗ до розпізнання його таким, дозволяє користувачу самостіно формувати списки процесів, керувати критичними дозволами додатків та вибірково блокувати небажані дозволи.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Мещеряков Р.В. Теоретические основы информационной безопасности автоматизированных систем, Мещеряков Р.В., Праскурин Г.А. – Томск: Из-во Томск. межвуз. центр дист. образ., 2005. – 243 с.

2. Android & iOS: концепции распространения приложений и вопросы безопасности [Електронний ресурс] // Режим доступу: http://habrahabr.ru/company/drweb/blog/143971/

3. Защита компьютерной информации от несанкционированного доступа, А.Ю. Щеглов, - Санкт-Петербург : Наука и Техника, 2004 – 385 с.

УДК 004.728.4 (043.2)

Лукашенко В.В., к.т.н., доцент
(Национальный авиационный университет, Украина)
Чхаидзе Д.
(Национальный технический университет Украины «КПИ», Украина)

СПОСОБ ФОРМИРОВАНИЯ ЗАПАСНЫХ ПУТЕЙ ДЛЯ ОРГАНИЗАЦИИ БЕЗОПАСНОЙ МНОГОПУТЕВОЙ МАРШРУТИЗАЦИИ

На сегодняшний день, при быстром темпе развития беспроводной связи, одной из перспективных современных технологий передачи данных являются мобильные сети типа *ad hoc*. Их отличительной особенностью является то, что узлы сети соединяются «на лету» и они независимы друг от друга. Мобильность узлов позволяет им входить и выходить из сети динамично, что предполагает постоянно меняющуюся топологию. В связи с этим, основной задачей является обход скомпрометированных или вышедших из сети узлов.

Для решения этой задачи, предлагается способ обхода скомпрометированных вершин (узлов) с использованием заранее сформированных запасных путей, минимально пересекающихся с основным путем [1]. Суть алгоритма заключается в формировании запасного пути $L_n=\{l_j| j=1,\dots m\}$ на основании выбора очередной смежной вершины B_j, максимально близкой к одной из вершин основного пути $L_0=\{l_i| i=1,\dots n\}$. Каждый путь l_j будем определять множеством $B_j=\{в_i| i=1,2,\dots k\}$ входящих в него вершин. Выбор очередной вершины осуществляется на основании операций над множествами смежных вершин.

В общем случае, для каждого основного пути $l_i \in L_0$ может быть два максимально близких к нему запасных путей l_j и l_m, один из которых располагается слева, а второй - справа от основного пути, и обход может осуществляться по одному из них в зависимости от топологии графа. После обхода скомпрометированной вершины осуществляется переход с запасного на основной путь. Если основной путь содержит хотя бы одну граничную вершину сети, то формируется только один запасной путь, максимально близкий к основному пути.

При организации многопутевой маршрутизации в предельном случае запасные пути могут принадлежать множеству L_0. При этом запасной путь строится как непересекающийся с основным, который может частично или полностью совпадать с каким-то другим путем множества L_0. В этом случае целесообразно выполнять процедуру обхода только «проблемных» узлов с возвращением на основной маршрут. Пути l_j и l_m не пересекаются при условии $B_i \cap B_m = \varnothing$. Пути l_j и l_m частично пересекаются, если $B_j \cap B_m \neq \varnothing$.

Рассмотрим поэтапно алгоритм формирования запасных путей [2]:

1) На первом этапе формируется множество вершин $B_0=\{B_i| i=1,\dots, n\}$ основного пути;

2) Для начальной вершины $B_i \in B_0$ множества вершин основного пути L_0 формируется множество смежных с ней вершин $B_{Si}=\{B_j| j=1,\dots,k\}$;

3) Далее для каждой вершины B_j множества $B_{Si}=\{B_j|j=1,...,m\}$ формируется соответствующее множество смежных с ней вершин $B_{Sk} = \{B_k|k=1,\dots,r\}$;

4) Для j=1,...,m выполняется операция пересечения множеств $B_{Sj}=B_0 \cap B_{Sk}$;

5) Среди полученных множеств выбирается множество B_{Sp} с максимальной степенью, соответственно в качестве очередной вершины запасного пути выбирается вершина B_p;

6) Если вершина B_p является конечной вершиной основного пути, то конец алгоритма;

7) Иначе для вершины B_p формируется множество смежных с ней вершин $B_{Si} = \{B_j | j = 1,\ldots,k\}$ и выполняется переход к пункту 3.

Для нахождения коэффициента задержки перехода воспользуемся формулой:

$$k_з = \frac{N_{пер.} - N_{осн.}}{N_{осн.}} = \frac{N_{пер.}}{N_{осн.}} - 1,$$

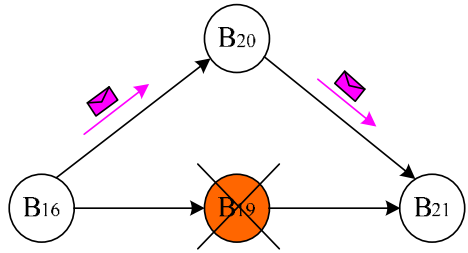
где

$N_{осн}$ – количество каналов основного участка пути, который обходится;

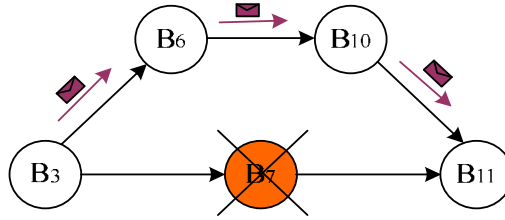
$N_{пер}$ – количество каналов участка запасного пути, по которому осуществляется обход вершины основного пути.

Существует три способа обхода одной скомпрометированной вершины через запасные пути:

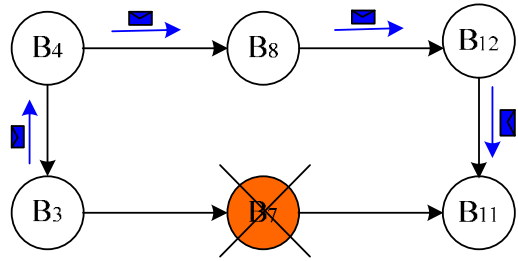
1. Обход по треугольнику, который происходит когда обходим одну скомпрометированную вершину через одну смежную с ней вершину. При этом $N_{пер} = N_{осн}=2$, а $k_з=0$;



2. Обход по трапеции, который осуществляется через две смежные вершины, где $N_{пер} = 3$, $N_{осн}=2$, в этом случае $k_з=0,5$;



3. Обход по прямоугольнику, который осуществляется через три смежные вершины. $N_{пер} = 4$, $N_{осн}=2$, в этом случае $k_з=1$.



При организации многопутевой безопасной маршрутизации, в рамках данной работы, был предложен способ обхода скомпрометированных вершин, которое позволяет с минимальным временем задержки осуществить обход «проблемной зоны» и обеспечить безотказную работу системы.

ИСПОЛЬЗОВАНЫЕ ИСТОЧНИКИ

1. Кулаков Ю.А. Способ и средства конструирования трафика на основе безопасной многопутевой маршрутизации в мобильных сетях. / Ю.А. Кулаков, В.В. Лукашенко, А.В. Коган // Transactions of Azerbaijan national academy of sciences. Informatics and control problems. – 2014. – №3, Vol. XXXIV. – Pp.62-68.

2. Кулаков Ю.О. Спосіб мінімізації часу обходу скомпрометованих вузлів в мобільних мережах / Кулаков Ю.О., Коган А.В. // Electronics and Communications. Електроніка та зв'язок. Електроніка та зв'язок. – 2014. – Том 19. – №2(79), – С.116-122.

УДК 004.728.4 (043.2)

Мартинова О.П., к.т.н., Дрововозов В.І., к.т.н.
(Національний авіаційний університет, Україна)

ЦЕНТР ОБРОБКИ ДАНИХ ВИРОБНИЦТВА

Застосування центру обробки даних (ЦОД) для управлінням виробництвом дозволяє масштабувати інформаційну інфраструктуру у разі зростання і розширення виробництва. Організація мережевого середовища ЦОД дає можливість гнучко, ефективно та централізовано управляти обчислювальною мережею, яка відособлена від локальних і глобальних мереж. Він зазвичай служить для взаємодії між собою облаштувань зберігання даних, підключених до одного або більше серверам. ЦОД характеризується високими швидкостями передачі даних між зовнішніми облаштуваннями зберігання і своєю високо масштабованою архітектурою. Рішення віртуалізації дозволяють зменшити витрати виробництва на апаратне забезпечення та електроенергію, а також підвищать доступність мережевих сервісів, що надаються.

Рішення, що забезпечують відмовостійкість на різних рівнях ЦОД значно збільшують надійність платформи. При цьому надмірність, необхідна для відмовостійкості, використана для збільшення ефективного навантаження на вузли центру обробки даних.

Підсистема доступу до зовнішніх мереж забезпечує широкі можливості управління маршрутизацією трафіку, захищає внутрішні ресурси мережі від мережевих загроз із зовнішніх мереж.

Мета створення ЦОД – впровадження інформаційної системи для здійснення можливості високопродуктивного функціонування необхідних мережних сервісів управління виробництвом, ефективної взаємодії внутрішніх інформаційних ресурсів виробництва.

Центр обробки даних повинен надавати можливості ефективної взаємодії мережних сервісів виробництва, надати можливість гнучкого масштабування інформаційної системи. Повинна бути реалізована відмовостійкість на рівні виходу з ладу будь-якого вузла або каналу зв'язку (згідно з *Tier-II* стандарту *TIA-942*), реалізована відмовостійкість на рівні виходу з ладу одного накопичувача даних у будь-якому вузлі. Має бути надійна дворівнева система резервного копіювання даних виробництва, при цьому ризики фатального результату повинні бути мінімізовані. ЦОД повинен мати систему моніторингу серверного обладнання і основних програмних систем.

Усе обладнання повинне мати можливість віддаленого управління і мати можливість горизонтального та вертикального масштабування.

Вимоги до мережного середовища центру обробки даних. Можливість сегментації та розширення інформаційної системи. Збільшення ступіню ефективного використання мережного обладнання.

У серверному сегменті крім самих серверів допускається знаходження тільки комп'ютерів операторів і обслуговуючого персоналу інформаційної інфраструктури.

Вимоги до організації мережних сервісів ЦОД. Забезпечення можливості роботи наступних мережних сервісів:

- файлові сервіси для зберігання інформаційних баз з можливістю доступу з внутрішньої мережі компанії;

- служба каталогів для зберігання облікових даних користувачів і централізованого керування пов'язаними мережевими ресурсами;

- сервіси, що забезпечують вирішення імен вузлів;

- сервіси, що забезпечують контрольовану ізоляцію внутрішньої мережі виробництва від зовнішньої мережі (Інтернет);

- система планування ресурсів виробництва (*Enterprise Resource Planning System*, *ERP*-система) *SAP*;

- сервіси управління обладнанням;

- можливість розширення мережевих сервісів.

Потрібен розподіл сервісів, що зменшує кількість простоїв і непродуктивної роботи серверного обладнання.

Можливість автоматичного відновлення працездатності сервісів у випадку апаратних або програмних збоїв серверів.

Мінімізація витрат на придбання операційних систем для сервісів.

Згідно цих вимог центр обробки даних повинен надавати можливості роботи наступних сервісів:

- файлові сервіси для зберігання інформаційних баз із можливостями доступу із внутрішньої мережі компанії;

- служба каталогів для зберігання облікових даних користувачів і централізованого керування пов'язаними мережевими ресурсами;

- сервіс для автоматичного присвоєння мережевих адрес робочім станціям;

- сервіси, що забезпечують розв'язання імен вузлів;

- сервіси, що забезпечують контрольовану ізоляцію внутрішньої мережі виробництва від зовнішньої мережі (інтернет);

- інші сервіси.

Вимоги до організації підсистеми ЦОД для доступу до зовнішніх мереж. Підсистема доступу до зовнішнніх мереж має розташовуватися на ізольованому фізичному вузлі. При цьому доступ у мережу Інтернет має надаватися для будь-якого сегмента мережі. Внутрішня структура мережі виробництва має бути схована для зовнішніх мереж. Забезпечення захисту локальної мережі виробництва від зовнішніх мережевих погроз. Шлюз до зовнішніх мереж має бути дубльованим. Канали зв’язку мають бути дубльовані (два провайдери). Високий рівень надійності мережевого обладнання [1-4].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Дроворозов В.І. Розвиток корпоративної мережі центру високопродуктивної обробки даних / В.І. Дроворозов, 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.

УДК 004.77

Марченко В.А., к.т.н.
(Інститут кібернетики ім. В.М. Глушкова НАНУ, Україна)

ОСОБЛИВОСТІ СТВОРЕННЯ СИСТЕМ ЗАХИСТУ VOIP В СУЧАСНИХ МЕРЕЖАХ

Останнім часом набули бурхливого розвитку мобільних технологій та модернізація мереж загального призначення. Це призвело до стандартизації технологій зв'язку. Особливу увагу заслуговує сімейство технологій VOIP, які все ширше застосовуються в існуючих системах зв'язку. Зокрема мережі 3G а особливо 4G повністю переходять на вказаний стек [1]. Тому питання захисту систем зв'язку і особливо захисту сеансів зв'язку від прослуховування є важливою задачею в існуючих системах захисту.

На даний момент значного розповсюдження набули способи організації зв'язку на базі «клієнт-серверної» архітектури, на відміну від систем типу «Peer-to-Peer». Це обумовлено історичними причинами та значно простішою організацією зв'язку. В подібних системах передбачається наявність центрального сервера, який виконує ряд задач таких як організація та контроль сеансів зв'язку.

Базовою задачею підсистеми захисту в подібних системах є захист каналу зв'язку між кінцевим учасниками. Найбільш ефективним способом захисту є шифрування трафіку між користувачами. Для організації захисту за допомогою шифрування необхідно виконати ряд вимог до архітектури системи та алгоритмів організації та проведення сеансів зв'язку.

У випадку використання системи захисту виключно між кінцевими користувачами значно ускладнюється архітектура підсистеми захисту. В даному випадку неможливо використати можливості центрального сервера для різноманітних криптографічних перетворень та узгоджень. Тому запропоновано використання спеціалізованої системи захисту яка працює виключно на стеку протоколів SIP\RTP [2]. Таким чином це дає можливість організувати захищений канал зв'язку між кінцевими користувачами прозоро від застосовуваного телефонного серверу, при цьому не вимагаючи додаткових затрат на підтримку необхідної функціональності на серверній стороні. Слід зазначити, що цей підхід має ряд проблем з точки зору протидіє на рівні власників серверу зв'язку. Зокрема використовуючи технологію транскодування можливо надавати відповідний сервіс при цьому повністю руйнуючи зашифровані пакети та не дозволяючи використання шифрування.

У доповіді описуються особливості побудови систем захисту для VIOP між кінцевими користувачами з використанням проміжного серверу зв'язку.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Martin Sauter. Beyond 3G - Bringing Networks, Terminals and the Web Together: LTE, WiMAX, IMS, 4G Devices and the Mobile Web 2.0. John Wiley & Sons, 2011. 366 pp.*
2. *Wallingford Theodore. Switching to VoIP. – O'Reilly Media, 2009. – 504 p.*

УДК 004.772

Мацуєва К.А.
(Національний авіаційний університет, Україна)

АЛГОРИТМ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В ГІБРИДНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ НА БАЗІ АРХІТЕКТУРИ SOA

На даний момент системи з хмарними обчисленнями є досить актуальним. Такі системи можуть використовуватись в якості додаткової обчислювальної потужності як в учбових закладах так и на підприемствах. Хмарні сервери дозволяють розширити обчислювальний потенціал, однак виконання всіх обчислень на них іноді буває економічно недоцільно. Для автоматизації вибору середовища виконання задачі а отже і балансування обчислювального навантаження пропонується використовувати програмний монітор-розподільник.

Для розподілу обчислювального навантаження між серверами локальної мережі і хмарою необхідно враховувати завантаженість внутрішніх серверів і час, що відводиться на вирішення завдання.

Для вирішення поставленого завдання за основу був взятий алгоритм розподілу навантаження розподіленої обчислювальної системи методом перебору та впорядкування її елементів по круговому циклу (round robin) [1]. Використовуючи алгоритм без зміни, передбачалося, що обробники завдань рівні за своїми обчислювальними потужностями. У випадку з хмарою є різнорангові сервери: це хмарний сервер з потенційно більшою обчислювальною потужністю і різнорангові сервера локальної обчислювальної мережі (ЛОМ). У такому випадку, алгоритм зазнав змін, і при кожній новій ітерації алгоритму обходу обчислювальних вузлів, кожен обчислювальний вузол отримує свій коефіцієнт, який вказує на те, скільки часу буде потрібно на вирішення поставленої обчислювальної задачі [2].

Після перебору всіх серверів вибирається той, який може якнайшвидше обробити обчислювальну задачу. При цьому балансувальник після завершення опитування вузлових серверів зберігає в пам'яті таблицю отриманих значень, і на її підставі може вибирати необхідний сервер через пряме звернення, без потреби в циклічному обході.

Розроблений балансувальник відноситься до класу балансувальників, що працюють на програмному рівні. Це дозволяє використовувати дане ПО незалежно від мережевого обладнання.

Балансувальник може вирішує ряд завдань таких як контроль завантаження кожного вузлового обчислювального сервера ЛОМ, організація вибору оптимального обчислювального ресурсу для кожної конкретної задачі, розподіл трафіку в гібридному середовищі, що включає в себе ЛОМ і хмарний вузол.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Клепиков, А.К. Модель распределения ресурсов при "облачных вычислениях"/А.К. Клепиков, А.Н. Привалов // Известия Тульского государственного университета. Технические науки. 2012. С. 151 - 157.

2. Карпов, В. Е. Основы операционных систем [Текст] / В.Е. Карпов, К. А. Коньков. М.: Интернет-университет информационных технологий, 2005. 536 с.

УДК 004.772

Мацуєва Х.А.
(Національний авіаційний університет, Україна)

ГЕОМЕТРИЧНІ ВЛАСТИВОСТІ ГРАФІВ ОДИНИЧНИХ КІЛ У МОДЕЛЮВАННІ МАРШРУТИЗАЦІЇ ГРАНЯМИ

У теорії графів графом одиничних кіл називається граф перетину сімейства одиничних кіл на евклідовій площині. Тобто, утворюється вершина для кожного кола і дві вершини з'єднується ребром, якщо відповідні кола перетинаються.

Графи одиничних кіл використовуються в інформатиці для моделювання топології бездротових динамічних мереж. У цьому випадку вершини з'єднані прямим бездротовим зв'язком без базової станції. Передбачається, що всі вершини однорідні і забезпечені всеспрямованими антенами. Розташування антени моделюється точками на евклідовій площині, а область, де сигнал може бути отриманий інший вершиною, моделюється колом. Якщо всі вершини мають передавачі однакової потужності, ці кола матимуть один і той же радіус. Випадкові геометричні графи, утворені як графи одиничних кіл з випадковими центрами, можна використовувати для моделювання фільтрації та деяких інших явищ.

З метою визначення інформації, що необхідна на кожному вузлі під час доставки пакету, визначимо властивості графів одиничних кіл. Наступна лема визначає геометричну властивість будь-яких двох ребер, які перетинають одне одного у графах одиничних кіл.

Визначення 1. Для будь-якого ребра *(u,v)*, лінзообразна область з хордою *(u,v)* є перетином двох кіл з одиничним радіусом, які містять *(u,v)* як хорду.

Затемнена область на рис. 1 є прикладом. Якщо вузол знаходиться у даній області з хордою *(u,v), то він є* сусідом як *u ,так v*.

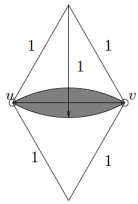


Рис. 1. Лінзообразна область з хордою *(u,v)*.

Лема 1. Якщо у графах одиничних кіл ребро *(x, y)* перетинає ребро *(u,v)*, і ні *x*, ні *y* не знаходяться у лінзообразній області з хордою *(u,v)*, то *x* і *y* є сусідами *u*, або обидва сусіди *v*.

Слідство 1. Якщо у графі одиничних кіл ребро *(x, y)* перетинає ребро *(u, v)*, обидва *x* і *y* знаходяться на відстані не більше двох переходів від *u* і *v*.

Випадок 2: Принаймні один з *x* і *y* знаходиться у лінзообразній області з хордою *(u, v)*. Припустимо, що *x* у даній області. Отже, *x* є сусідом обох *u* і *v*. Таким чином, *y* знаходиться на відстані не більше двох переходів від *u* і *v*.

Слідство 1 означає, що якщо кожен вузол має інформацію про сусідні два переходи, то йому відомі всі ребра, які перетинають кожні його інцидентні ребра.

УДК 621.382:62-1/-9(045)

Мельник О. С., Романюк В.Ю.
(Національний авіаційний університет, Україна)

НАНОЕЛЕКТРОННІ АРИФМЕТИКО-ЛОГІЧНІ ПРИСТРОЇ В СИСТЕМАХ ТЕЛЕКОМУНІКАЦІЙ

Квантові коміркові автомати – технологія, що виникла два десятиліття тому, в якій значенням логічних станів відповідають позиції окремих електронів. Квантові комірки використовуються для конструювання логічних наноелементів та арифметичних нанопристроїв). В роботі виконується моделювання квантових нанопристроїв з використанням системи автоматизованого проектування (САПР) QCADesiner.

За допомогою КА можуть бути сконструйовані різні елементи для виконання логічних і арифметичних операцій. Базовими логічними нанокомпонентами в теорії коміркових автоматів є мажоритарний елемент (МЕ)та інвертор .

Однобітний напівсуматор на КА може бути складений з чотирьох МЕ і двох інверторів. Вирази для суми S і переповнення C цього суматора наступні:

$$S = maj(x\overline{y}, \overline{x}y, 1) = x \oplus y,$$

$$C = maj(x, y, 0) = xy,$$

де x, y – вхідні доданки

Якщо провідник з однаково поляризованих комірок перетинає інвертуючий провідник, провідники не взаємодіють між собою, тому можуть працювати незалежно на одному рівні. Затримка такого суматора – один тактовий цикл, що складається з чотирьох тактових зон, представлених різними ступенями градацій сірого.

Дворозрядний суматор реалізує арифметичне додавання S_2, S_1, S_0 дворозрядних бінарних чисел x_1x_0 та y_1y_0 .

Спроектована таким чином наносхема дворозрядного суматора базується на 98 квантових коміркових автоматах, розмір яких (18х18) нм. Розмір конструкції (360х414) нм. Існує 11 входів і три виходи, а чотири комірки мають фіксовану поляризацію.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Tougaw, P.D., Lent C.S .Logic devices implemented using quantum cellular automata / Tougaw, P.D., Lent C.S //J. Appl. Phys., American Institute of Physics. – 1994.

2. Пакулов Н.Н. Мажоритарный принцип построения надежных узлов и устройств ЦВМ / Пакулов Н.Н. – М.: Сов. радио – 1974.

3. Bhanja, S., Ottavi, M., Lombardi, F., Pontarelli. S. OCA circuit for robust coplanar crossing. / Bhanja, S., Ottavi, M., Lombardi, F., Pontarelli. S. // Journal of Electronic Testing. – 2007, -P. 193-210.

4.Melnyk O.S., Tsapok L.O. Computer simulation of nanoelectronics arithmetic – logic devices // Електроніка та системи управління.- 2012,- N1 (31), - p.5-10.

УДК 621.376

Одарченко Р.С., Даков С.Ю.
(Національний авіаційний університет, Україна)

ОСНОВНІ ТРЕНДИ В РОЗВИТКУ БЕЗПРОВОДОВИХ СТІЛЬНИКОВИХ МЕРЕЖ

У зв'язку з розвитком технологій, а також з появою нових, більш вдосконалених мобільних пристроїв, які надають користувачам більше можливостей, з'являється необхідність у наявності високошвидкісного бездротового інтернет з'єднання. Сучасні смартфони, планшетні ПК, ноутбуки та інші «розумні» пристрої надають користувачам нові можливості. Завдяки цьому з'являється попит на більш швидкісний зв'язок. Так, завдяки цьому, сучасні оператори мобільного зв'язку починають впроваджувати у свої мережі нові технології, які здатні надати абонентам необхідну швидкість з'єднання і якість зв'язку. Однією з таких технологій є LTE (англ. Long Term Evolution – «довготерміновий розвиток»). На даному етапі свого розвитку існує більше трьохсот комерційних мереж LTE. Але, не дивлячись на всі переваги, аналітики розуміють, що на зміну LTE за оцінками експертів після 2020 року мають прийти мережі 5-го покоління – 5G. Вони повинні будуть враховувати всі недоліки мереж попередніх поколінь. Тому метою даною роботи є дослідження недоліків мереж LTE та визначення основних трендів, за якими мають розвиватись перспективні безпроводові технології на шляху до 5G. На рисунку 1 представлені основні напрямки розвитку безпроводових мереж, які відображають як побажання користувачів, так і операторів стільникового зв'язку.

Рис. 1 Шляхи розвитку стільникових мереж зв'язку

Таким чином, в даній роботі були окреслені основні напрямки досліджень на майбутні 5-10 років, які будуть проводитись по всьому світу в області розвитку безпроводових мереж зв'язку.

УДК 519.852.35:004.7

Печурин Н.К., д.т.н.
(Национальный авиационный университет, Украина)
Кондратова Л.П., к.т.н.
(Национальный технический университет Украины "КПИ", Украина)
Печурин С.Н., к.т.н.

РАСПРЕДЕЛЕНИЕ ПОТОКОВ ФИЗИЧЕСКОГО УРОВНЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

Применяемые способы распределения трафика в компьютерных сетях тесно связаны с уровнем представления протокольных единиц данных, образующих потоки данных. В работе рассмотрен низший уровень представления протокольных единиц данных эталонной модели взаимодействия открытых систем - физический. Основной теоремой, использованной для синтеза алгоритмов распределения потоков физического уровня является теорема о максимальном потоке и минимальном разрезе (Форда-Фалкерсона). Решение задач об однополюсном и многополюсном потоке основано на использовании алгоритмов Форда-Фалкерсона и Гомори-Ху соответственно [1]. Предложенные алгоритмы поиска потоков минимальной стоимости и максимальных потоков в своей основе используют математические модели класса целочисленного программирования с системами линейных и/или нелинейных алгебраических уравнений. В данной работе исследуется модель распределения трафика физического уровня в компьютерной сети, где в качестве среды передачи данных используется радиоэфир, а функции распределения трафика выполняют взаимодействующие между собой через распределительную систему базовые станции сети. Рассматривается задача поиска потока минимальной стоимости как обобщение задачи поиска максимального потока, которая заключается в определении минимальной стоимости транспортировки потока заданной величины $f_{st}=v$ между узлами s и t, представляющие источник и сток соответственно. Полагается, что в связном ориентированном графе с множествами V узлов и E дуг каждой дуге $(i,j)\in E$ соответствуют веса f_{ij} потока по дуге, U_{ij} пропускной способности, c_{ij} стоимости транспортировки единицы потока. В качестве альтернативы используемым специальным потоковым алгоритмам распределения предлагается использовать классические декомпозиционные алгоритмы для модели целочисленного линейного программирования. Учитывая особую структуру матриц коэффициентов математической модели, можно рекомендовать для решения рассматриваемой задачи декомпозиционные подходы Данцига – Вулфа или Корнаи – Липтака [2].

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Алгоритмы и программы решения задач на графах и сетях / М.И.Нечипуренко, В.К.Попков, С.М.Майнагашев и др.–Новосибирск: Наука. Сиб. отд-ние, 1990. – 515 с.

2. Жариков А.В. Исследование скорости сходимости некоторых алгоритмов блочного линейного программирования // Управление, вычислительная техника и информатика. – 2011. – С.100-105.

УДК 004.56.5(043.2)

Работнік А.О., Черниш Л.Г., к.т.н.
(Національний авіаційний університет, Україна)

МАТЕМАТИЧНА ПОСТАНОВКА ЗАДАЧІ ОЦІНКИ РИЗИКІВ РЕАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Мета роботи – аналіз рівня захисту інформації, що циркулює в інформаційній системі підприємства шляхом розрахунку ризиків реалізації загроз інформаційної безпеці.

Актуальність – визначається тим, що дана методика дає можливість визначити рівень збитків, які несе будь-яке підприємство або установа через реалізацію загроз інформаційним ресурсам, а також дозволяє обґрунтувати впровадження контрзаходів заходів безпеки та оцінити їх ефективність.

Розглянемо послідовність розрахунку ризиків реалізації загроз інформаційній безпеці та ефективності впровадження заходів безпеки.

1) На першому етапі розраховуємо рівень загрози по кожній уразливості на основі критичності та ймовірності реалізації загрози через дану уразливість. Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації.

$$\mathbf{У_З = КР_З \times I_З} \qquad (1)$$

де $\mathbf{У_з}$ – рівень загрози по вразливості;

$\mathbf{КР_з}$ – критичність загрози;

$\mathbf{I_з}$ – ймовірність реалізації загрози.

На другому етапі розраховуємо рівень загрози також по кожній по уразливості з урахуванням контрзаходів на основі критичності та ймовірності реалізації загрози через дану уразливість. Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації після прийняття контрзаходів.

3) На третьому етапі розраховується первісний ризик по кожному інформаційному ресурсу в процентній та грошовій формах за формулами:

4) На четвертому етапі розраховується ризик від кожної загрози по кожному інформаційному ресурсу з урахуванням контрзаходів.

5) На п’ятому етапі розраховується первісний загальний ризик по кожному ресурсу за усіма загрозами та загальний ризик по кожному ресурсу.

6) На шостому етапі розраховується первісний ризик по інформаційній системі ($\mathbf{P_{ic}}$) та ризик по інформаційній системі з урахуванням контрзаходів ($\mathbf{P_{ic\_контр}}$)

Ефективність впровадження контрзаходів $\mathbf{E_{контр}}$ визначається співвідношенням вартості впровадження контрзаходів $\mathbf{B_{контр}}$ та різниці між первісним ризиком та його значенням після здійснення контрзаходів:

$$\mathbf{E_{контр} = \frac{B_{контр}}{P_{ic} - P_{ic\_контр}}} \qquad (2)$$

Сформульована математична постановка задачі оцінки ризиків реалізації загроз інформаційної безпеці та визначення ефективності впровадження контрзаходів проти існуючих загроз.

УДК 004.7:004.738.5 (043.2)

Рибасова Н.О., Тімченко Д.О.
(Національний авіаційний університет, Україна)

ВЕБ-ДОДАТОК ПОШТОВОГО СЕРВІСУ З МОДЕРНІЗАЦІЄЮ ГРАФІЧНОГО ІНТЕРФЕЙСУ ТА ВНУТРІШНЬОЇ ЛОГІКИ

Запропонований веб-додаток поштового сервісу розроблений засобами Java EE технології. Додаток побудований на основі Servlets Api, EJB, JavaScript, HTML, CSS, AJAX. Усі ці технології тісно взаємодіють між собою, щоб забезпечити правильну роботу сервісу. Технології JavaScript, HTML, CSS, AJAX забезпечують чітку роботу клієнтської частини сервісу, забезпечують побудову графічного інтерфейсу користувача, відправку та отримання запитів. Servlets Api забезпечує чіткий розподіл запитів до відповідних ресурсів, а також виконує автентифікацію користувачів на сервісі. EJB відповідає за взаємодіє з базою даних, а саме: вибірка даних, додавання нових даних, видалення та оновлення даних.

Архітектура додатку побудована на основі патерну MVC (Model View Controller). Модель (M - Model): зберігає в собі бізнес-логіку програми, регулює доступ до даних і їх зміну. Вигляд (V - View): view відображає вміст моделі, визначає як необхідно представити дані, отримані від моделі. View бере на себе збір даних користувача і передачу їх контролеру. Контролер (C - Controller): контролер визначає поведінку всього додатку, отримує від view дані користувача, інтерпретує їх в дії, що виконуються за допомогою моделі. Контролер передає view вказівку, яке уявлення необхідно застосувати, на основі результатів роботи моделі та взаємодії з користувачем.

Архітектура веб-сервісу представляє собою клієнт-сервер, а точніше - Thick Web Client, адже значна частина логіки знаходиться на стороні клієнта. Така архітектура має багато переваг над класичними додатками, які необхідно інсталювати на ПК. До основних переваг можна віднести: низькі вимоги до комп'ютера користувача, відсутність необхідності встановлення додатку, незалежність від операційної системи і т.д.

При використанні Thick Web Client клієнтських сценаріїв, керуючих елементів і аплетів дуже важливо, щоб групою тестування був виконаний повний набір тестів для всіх підтримуваних клієнтських конфігурацій. Якщо на клієнті розміщена важлива частина бізнес-логіки, то необхідно упевнитися в її коректному виконанні на всіх типах використовуваних браузерів. Не можна сподіватися, що всі броузери працюють однаково. Різні браузери будуть по-різному обробляти один і той же вихідний код, і, більше того, один і той же броузер буде по-різному працювати в різних операційних системах.

Для роботи даного типу додатків необхідний цілий комплекс програмних засобів. Ці засоби включають: операційну систему, систему управління базами даних, мову програмування, веб-сервер. При виборі комплексу засобів розробки зважені всі переваги та недоліки існуючих засобів.

Використання складних інструментів при розробці простого сервісу може призвести до збільшення часу розробки та ускладнення самого процесу розробки, при цьому переваг сервісу це не надасть.

Сервіс є невимогливим до апаратної частини комп'ютера користувача, але при цьому забезпечується його швидка робота, інтерфейс додатку – простий і для повноцінної роботи з ним користувач не потребує спеціальних знань.

Сервіс має такі переваги:

− доступність – локальному сервісу необхідна лише робоча внутрішня мережа;

− безпека – локальний сервіс безпечніший, адже ви повністю знаєте як працює ваш сервіс;

− керованість – все що відбувається на сервісі керується виключно його власником;

− гнучкість – вносити зміни в його структуру досить просто та швидко.

Сервіс працює швидше ніж додаток gmail від Google за рахунок:

− використання технології AJAX, яка значно зменшує навантаження на сервер, відсилає до серверу менше інформації та зменшує кількість елементів сторінки необхідних "перемалювати" браузеру;

− розташування сервісу на внутрішньому сервері, як результат менший шлях, який необхідно подолати сигналу щоб дійти до адресата і назад;

− меншій кількості користувачів. Сервіс від Google налічує мільйони користувачів, цей аспект збільшує кількість часу необхідного на автентифікацію користувача та пошук його повідомлень.

Проведено порівняння швидкості роботи запропонованого сервісу в порівнянні з сервісом Google gmail (для перевірки швидкості роботи використано вбудований додаток розробника програми Google chrome версії 40.0.2214.93 та наявності Internet підключення на швидкості 100 Мбіт/с). Отримані дані свідчать про перевагу сервісу. Виконано порівняння швидкості автентифікації користувача та порівняння швидкості завантаження повідомлень [1-7].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Морган М. Java2. Руководство разработчика.: Пер. с англ.:Уч. Пособие – М.: "Вильямс", 2000. – 720 с.:ил..

2. Ноутон П., Шилдт Г. Java 2 в подлиннике.: Пер. с англ. – СПб.:БХВ-Петербург, 2000. – 1072 с.: ил.

3. Смирнов Н. И. JAVA 2 Enterprise. Основы практической разработки распределенных корпоративных приложений. – М.: КУДИЦ-ОБРАЗ, 2002. – 240 с.

4. Кей С. Хорстманн Java SE 8. Вводный курс. — М.: «Вильямс», 2014. — 208 с.

5. Соколов Е. Технологии Java для разработки веб-приложений :[Електронний ресурс]. - Режим доступа: http://www.techinfo.net.ru/docs/web/javawebdev.html.

6. HTML - Wikipedia, the free encyclopedia site [електронний ресурс]. Адреса: http://uk.wikipedia.org/wiki/HTML

7. Джуниперо Т. Создание простого веб-приложения с использованием базы данных MySQL: [Електронний ресурс]. - Режим доступа: https://netbeans.org/kb/docs/web/mysql-webapp_ru.html.

УДК 004.72

Ролик А.И., д.т.н., Кравченко Т.В., Кравчун Н.В.
(Национальный технический университет Украины «КПИ», Украина)

УПРАВЛЕНИЕ РАСПРЕДЕЛЕНИЕМ РЕСУРСОВ В ПРОГРАММНО КОНФИГУРИРУЕМЫХ СЕТЯХ

В настоящее время сфера предоставления ИТ-услуг способствует повышению эффективности выполнения бизнес-процессов. ИТ-компании, предоставляющие такие услуги, для обеспечения своей конкурентоспособности стремятся минимизировать затраты на ИТ-инфраструктуру без ухудшения качества ИТ-услуг. Поэтому задача поддержания высокого уровня ИТ-услуг путем управления распределением ИТ-ресурсов, обеспечивающих работоспособность этих услуг, является актуальной.

Для сокращения затрат в современных ИТ-инфраструктурах повсеместно используется технология виртуализации. Виртуализируются серверное и сетевое оборудование, а также предоставляемые заказчику сервисы и ИТ-инфраструктура.

Поддержание качества услуг на согласованном уровне осуществляется путем управления объемами ресурсов, выделяемых ИТ-услугам. Увеличение количества пользователей ИТ-услуги, приводящее к снижению качества, компенсируется выделением услуге дополнительных ресурсов. Ресурсами, выделяемыми ИТ-услугам, являются процессорное время, объем оперативной памяти и дисковое пространство, а также полоса пропускания канала связи. Распределение и перераспределение процессорного времени, оперативной памяти и дискового пространства осуществляется посредством гипервизора с использованием методов и моделей, предложенных в [1].

В работе особое внимание уделено аспектам управления полосой пропускания, выделяемой отдельным ИТ-услугам.

Рассмотрены методы управления полосой пропускания в программно конфигурируемых сетях (SDN). Предложен метод динамического изменения пропускной способности виртуального канала в зависимости от текущего качества ИТ-услуги. Метод основан на анализе динамики размера очереди в SDN-коммутаторах инфраструктурного уровня и последующего перераспределения полосы пропускания. В случае невозможности перераспределения ресурсов между услугами осуществляется миграция виртуальных машин, предоставляющих ИТ-услуги, на другие физические сервера.

Предложен алгоритм динамического перераспределения полосы пропускания между виртуальными машинами так, что бы было задействовано минимальное количество ресурсов без ухудшения качества предоставляемых ИТ-услуг.

Предложенный метод позволяет поддерживать согласованный уровень ИТ-услуг с рациональным использованием ресурсов ИТ-инфраструктуры при существенной динамике запросов пользователей.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Теленик С.Ф. Адаптивный генетический алгоритм для решения класса задач распределения ресурсов ЦОД / С.Ф. Теленик, А.И. Ролик, П.С. Савченко // Вісник НТУУ «КПІ»: Інформатика, управління та обчислювальна техніка. – К.: «ВЕК+», 2011. – № 54. – С. 164–174.

УДК 004.7

Ролик А.И., д.т.н., проф., Барна В.В.,
Бабичук Ю.И., Боровик Р.О.
(Национальный технический университет Украины «КПИ», Украина)

ОЦЕНКА КАЧЕСТВА УСЛУГИ VOIP В ВЫСОКОНАГРУЖЕННЫХ IP СЕТЯХ С ПРОТОКОЛОМ SIP

В настоящее время одной из самых широко распространенных мультимедийных услуг является технология обмена голосовыми сообщениями VoIP. Операторам, предоставляющим услугу VoIP, для поддержания своей конкурентоспособности необходимо обеспечивать текущий контроль качества услуги и оперативное управление телекоммуникационной сетью для поддержания качества на высоком уровне. Поэтому тема работы, посвященной оценке качества услуги VoIP, является актуальной.

В работе предложен подход к оценке качества VoIP, основанный на анализе пакетов голосового трафика в узлах сети оператора. Подход предполагает предварительную классификацию трафика, проходящего через узлы сети с целью выделения отдельных SIP-сессий и связанных с ними голосовых пакетов протокола RTP, с использованием протокола SDP, и пакетов управления протокола RTCP. После выделения пакетов осуществляется определение значений вероятности потери пакетов, величин задержки и флуктуации задержки передачи пакетов (джиттера) для каждой сессии. Исходя из значений этих величин, вычисляется R-фактор, в соответствии с которым оценивается качество услуги VoIP для каждой сессии.

Разработаны методы определения величины задержки передачи пакетов, джиттера и количества потерянных пакетов. Разработана структура системы оценки качества услуги VoIP, обладающая свойствами масштабируемости, возможности захвата и анализа пакетов высокоскоростных потоков голосового трафика. Захват трафика осуществляется с буферов сетевой карты посредством netmap [1], а в качестве базы для анализа пакетов использовано решение BlockMon [2], применяемо для DPI.

Разработаны блоки для захвата трафика с помощью выбранного инструментария, а также для фильтрации пакетов голосового трафика, дефрагментации пакетов с изначально большим значением MTU, сортировки пакетов по принадлежности к отдельной сессии, определения значений параметров для последующего вычисления R-фактора. Создан блок формирования отчетов в формате JSON о полученных системой данных и их отправки в систему управления телекоммуникационной сетью оператора услуги VoIP.

Произведены реализация и тестирование системы анализа голосового трафика по оценке производительности и использования ресурсов сервера. Эмпирическим путем определены оптимальные параметры настройки критических компонентов системы. Доказана работоспособность и высокая производительность системы.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Rizzo L. netmap: A Novel Framework for Fast Packet I/O // USENIX Annual Technical Conference ATC'12, Boston, MA. USENIX Association, 2012. – 12 p.

2. Simoncelli D., Dusi M., Gringoli F., Niccolini S. Stream-monitoring with blockmon: convergence of network measurements and data analytics platforms// SIGCOMM Comput. Commun. Rev., 2013 — 6 p.

УДК 621.3

Rusanova O.V.
(National Technical Univerity of Ukraine "KPI", Ukraine)

SCHEDULING ALGORITHM FOR MULTI-CORE CLUSTERS

Analysis of 44-th edition TOP500, that includes computer systems with highest performance, shows that: most of them have clustering architecture; all systems use multi-core technology. 85% use eight or more cores; some systems, including Tianhe-2, which ranks first in the TOP-500 list, belong to heterogeneous type; middle core number in clusters equal to 46288, but we are observed a slowdown in systems performance increasing. This paper is dedicated to increasing the real performance of modern clusters by improving static scheduling algorithms.

The effective scheduling algorithms for modern clusters must support multi-core architecture, topology and heterogeneity of nodes. Different list, cluster, genetic and duplication scheduling heuristics for heterogeneous clusters are discussed and analyzed. We defined the most effective scheduling algorithms such as *HEFT, CPOP, LDBS, LMT* [1] and *HETS* [2]. Most of them belong to list scheduling methods, support topology and heterogeneity of nodes, but don't support multi-core architecture. The algorithm proposed in paper [3] takes into account multi-core architecture of clusters but doesn't consider system topology.

We propose scheduling approach based on combination of list and cluster heuristics that takes into account all demands of modern heterogeneous or homogeneous multi-core clusters with any nodes topologies. We use the following initial data for our approach, such as application model (DAG task graph), heterogeneous or homogeneous multi-core cluster computing model (two levels system graph) and optimization criteria [2]. Proposed heuristic includes two main stages, such as: definition of initial priorities for graph task nodes (subtasks) and order formation; dynamical correction of subtasks priorities and their allocation to nodes cores.

Developed a software model for the implementation of our approach and well known heuristics. We performed a comparative analysis of our algorithm with these well known heuristics. The comparision are based on the following metrics: *SL* (scheduling length); *SLR* (scheduling length ratio); *SU* (speedup); *RT* (running time); *E* (efficiency) [2]. For testing such approaches we consider random task graphs with different connectivities. Proposed algorithm during testing showed the best scheduling characteristics compared with other approaches by an average of 10-20%.

Advanced scheduling approach can significantly improve the real performance of any multi-core cluster systems.

REFERENCES

1. H. Topcuoglu, S. Hariri and M. Wu, «Performance-Effective and Low-Complexity Task Scheduling for Heterogeneous Computing», IEEE Trans. Paralleland Distributed Systems, vol. 13, no. 3, pp. 260–274, March 2002.

2. Русанова О.В., Ярох Ю.А. Планирование вычислений в гетерогенных кластерных системах. Вісник НТУУ"КПИ".Сер. Інформатика, управління та обчислювальна техніка. - 2012. Випуск 49. - С.155 –163.

3. Gaochao Xu, Xiaodong Fu, Yuan Zhang, «A Task Scheduling Algorithm For Multi-Core-Cluster Systems», Journal of Computers, vol.7,no11, pp.2797-2804, November 2012.

УДК 004.056

Сінько Ю.І., к.п.н.
(Національний авіаційний університет, Україна)

УПРАВЛІННЯ РІШЕННЯМИ І ПРОЕКТАМИ В VISUAL STUDIO 2013

Середовище Visual Studio 2013 пропонує різноманітні мови розробки та види проектів. Для розробки використовуються концепції *проект* (project) (програма, що розробляється) і *рішення* (solution) (група взаємопов'язаних проектів). Рішення – це більш велика одиниця: рішення може складатися з одного або декількох проектів. Можливо також створення порожнього рішення, до якого поступово додаються все нові проекти. Для кожного виду проектів передбачені шаблони коду, що значно полегшують розробку. При введенні програмного коду середовище забезпечує підказки, контроль правильності введеного коду і т.д.

Код програмного проекту може мати складну структуру і складатися з декількох файлів вихідного коду і конфігураційних файлів. Крім того, сам код може бути доволі специфічним: наприклад, код Web-сервісу може мати Web-методи, анотовані спеціальними атрибутами, і т.д. У зв'язку з цим, середовище Visual Studio полегшує створення проектів за допомогою *шаблонів* (templates). Шаблон задає типову структуру коду проекту та його конфігураційних файлів, і розробнику залишається "тільки" додати в шаблон конкретний код.

За замовчуванням розробник, як правило, створює в середовищі один проект. При цьому за замовчуванням середовище створює і рішення, частиною якого стає проект, що створюється. Ім'я рішення збігається з ім'ям проекту.

Найбільш поширений спосіб створення нового проекту в середовищі Visual Studio – вибір пунктів головного меню: File / New / Project. Відкривається вікно New Project.

Основна змістовна частина вікна (крім, зрозуміло, імені нового проекту і директорії для його розміщення) – вибір *шаблону* (template) нового проекту. Зміст шаблону визначається, по-перше, мовою розробки (C#, Visual Basic, Managed C++, F# і т.д.), по-друге, видом проекту: консольний додаток, хмарний сервіс і т.п.

Слід зазначити, що набір видів проектів можна доповнювати. Таке розширення середовища (add-ins) визначає нові різновиди проектів, що специфічні для даного розширення. Крім того, не всі види проектів доступні в початковій конфігурації Visual Studio 2013, в тому вигляді, в якому вона інстальована на Ваш комп'ютер. Для використання (фактично – доповнення) деяких видів проектів можуть знадобитися додаткові інсталяції. Перш за все, це стосується хмарних проектів для платформи Microsoft Azure. При спробі вибрати і використати один з видів проектів, що відноситься до категорії Cloud, середовище виведе повідомлення, що для їх використання необхідно інсталювати Microsoft Azure SDK відповідної версії – комплекс інструментів, який необхідно додатково завантажити та інсталювати.

У версії Visual Studio 2013 Ultimate доступні наступні види проектів (для кожної мови розробки):

- *Windows* – проекти, специфічні для Windows: *Windows Forms Application* (проекти, що використовують GUI в стилі Windows – вікна, меню і т.д.); *Windows Presentation Foundation Application* (проекти в стилі WPF); *Console Application*

(проекти, з інтерфейсом користувача у вигляді командного рядка); *Class Library* (бібліотеки класів); *Portable Class Library* (переносні бібліотеки класів); *WPF Browser Application* (Web-додатки для браузера з інтерфейсом в стилі WPF); *Empty Project* (пустий проект); *Windows Service* (сервісний процес для Windows); *WPF Custom Control Library* (бібліотека елементів управління); *WPF User Control Library* (бібліотека елементів управління користувачів); *Windows Forms Control Library* (бібліотека елементів управління з інтерфейсом в стилі Windows Forms);

- *Web* – веб-сервіси, засновані на ASP.NET;
- *Office / SharePoint* – додатки, що використовують офісні продукти Microsoft: Microsoft Office і SharePoint;
- *Cloud* – хмарні сервіси для платформи Microsoft Azure;
- *LightSwitch* – проекти на основі Microsoft Silverlight;
- *Reporting* – проекти для генерації та обробки звітів на основі баз даних;
- *Silverlight* – проекти з розробки різних видів Web-додатків на основі Silverlight;
- *Test* – різні види проектів з розробки та прогонки тестів, у тому числі – unit-тестів, які згенеровані інструментом JUnit;
- *WCF* – проекти для реалізації різного роду додатків і сервісів на основі Windows Communication Foundation (WCF);
- *Workflow* – проекти з планування діяльності (activity) групи розробників.

Для мови Visual Basic набір проектів такий самий.

Для мови Visual C++ передбачені лише деякі види проектів "в старому стилі", що відображають специфіку даної мови: наприклад, Win32 Application – додаток, що використовує Win32 API; MFC Application – додаток, що використовує бібліотеку Microsoft Foundation Classes і т.д.

Передбачені також і другі мови і види проектів: *Visual F#* – функціональна мова зі своїм набором проектів, у тому числі – консольний додаток, tutorial і Silverlight-додаток; *SQL Server* – проект з розробки додатку, що взаємодіє з базою даних; T*ypeScript* – проекти на мові TypeScript (вимагають окремої інсталяції TypeScript в середовищі Visual Studio); *Python* – проекти на мові Python, яка широко використовується сьогодні для Web-програмування (вимагають окремої інсталяції Python); *Modeling Projects* – проекти з розробки UML-моделей.

Різноманітність мов і видів проектів просто вражає. За своєю суттю і призначенням, середовище Visual Studio відкрите для розширення новими мовами і видами проектів. Так що справа за Вами, шановні розробники!

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Web-сторінки корпорації Microsoft, присвячені Visual Studio 2013. Режим доступу: https://msdn.microsoft.com/ru-ru/library/dd831853.aspx.

UDC 629.7.01+65.011.3

Soroka M.V.
(Central research institute of armament and military equipment of Armed Forces of Ukraine)

ABOUT DEVELOPMENT OF DECISION SUPPORT SYSTEM OF AVIATION PROJECTS ON BASIS OF THE USE OF INTELLECTUAL INFORMATION TECHNOLOGIES

Foreign commercial companies devote considerable attention to the risks assessments (financial, innovative, currency and other) long enough. The policy of companies is implemented through the creation and improvement of complex risk management system that allow to detect risks to assess their significance and limit the influence of risks on the company.

As a result, these companies become more efficient and competitive in the market of sales of goods and services. Recently, this approach is becoming urgent to address the problems of risk management and assessment in the design of complex aviation technique patterns.

It is related to the fact that, according to experts, creation of aviation projects with novelty more than 25% is characterized by a high degree of technical risk [1].

Under the technical risk we understand the risk that's associated with a probability of losses due to the negative results of research work, achieving the planned technical parameters during design and technological developments, low technology manufacturing capabilities to improve further developments, the probability of losses due to problems in the use of new technologies [2].

In full, this problem also concerns Ukraine, taking into account certain specifics, that in addition to traditional areas of development of aircrafts for military cargo aviation tasks of implementing of new ambitious projects in development of aviation technique is posed by military command. Among them should be noted the development of training and combat aircraft, multipurpose light helicopter, unmanned aerial systems, patrol aircraft, airborne early warning and control aircraft.

Today, one of the effective tools for minimizing risks of project is the use of decision support system which allows performing the necessary calculations and providing informed advice on choosing the best option that is based on a set of methods and algorithms that are implemented in modern software.

It includes such software as COBRA, CRAMM (Central Computer and Telecommunications Agency, Great Britain), SAP ERP (company SAP AG, Germany), Callio Secura 17799 (Callio Technologies, Canada), Microsoft Office Project (USA), OCTAVE (Software Engineering Institute Carnegie Mellon University), Proteus Enterprise, RiskWatch, vsRisk, RA2 art of risk, RiskManager (Avangard) (Russian Federation) and others.

It should be noted that during the development of aviation project based on intelligent information technology should be taken into account as much as possible the subject area of realization. The definition of set of criteria that is which allow to assess the quality and feasibility of the project, its coast, scientific and technical level is needed.

An important issue in this case there is a justification of sufficient set of criteria. It is planned that the criteria will be selected from three sources. These include standards

in the field of arms and military equipment, legal documents (laws, regulations, etc.), card survey of experts.

Mathematical processing of criteria will be conducted using advanced intelligent informational technologies based on the theory of fuzzy sets. This theory has shown good results when operating fuzzy concepts to which the technical risk of aviation project are belong.

REFERENCES

1. Ливанов В. Что происходит с авиационной отраслью? [Електронний ресурс]. – Режим доступу: http://www.aex.ru/fdocs/2/2013/3/7/22656/.

2. Олійник І.І., Жданов С.В., Сорока М.В. Актуальні питання оцінки ризиків при реалізації нових проектів створення авіаційної техніки // Зб. Наук. Праць ЦНДІ ОВТ Збройних Сил України, 2014. Вип.3(50). - С.122-140.

3. Power D.J. A Brief History of Decision Support Systems. DSSResources. COM, World Wide Web, http://DSSResources.COM/history/dsshistory.html, version 2.8, May 31, 2003.

УДК 004.738.5(043.2)

Ткаченко Р.В., Ткаченко Б.В.
(Национальный авиационный университет, Украина)

ОБЛАЧНЫЕ ТЕХНОЛОГИИ И ИХ ПРИМЕНЕНИЯ В НОВЕЙШИХ РАЗРАБОТКАХ

Облачные вычисления — это технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис.

Значительную роль в развитии облачных технологий сыграли технологии виртуализации, в частности программное обеспечение позволяющее создавать виртуальную инфраструктуру.

Преимущества облачных технологий:

- **Доступность** – облака доступны всем, из любой точки, где есть Интернет.
- **Низкая стоимость -** позволяет пользователям экономить на покупке лицензий к ПО.
- **Гибкость** — распределение и подача можностей между пользователями происходит по мере необходимости.
- **Надежность** – обеспечение отказоустойчивости.

Одним из ярких представителей использующих облако есть такой гигант как Microsoft и его продукт Office 365.

Office 365 **–** современный и удобный способ решения определенных задач в облаке.

Облачные службы Майкрософт позволят сократить расходы и получить адекватный набор рабочих средств для пользователей, обеспечиваемый необходимыми средствами обеспечения безопасности и соответствия требованиям.

Преимущества данного продукта:

Мобильность – возможность работы на разных устройствах имея доступ к нужным файлам: документам, электронной почте, и т.д.

- **Привычные инструменты** – сохранение документа непосредственно в облако и совмесно работать над ним в знакомых программах.
- **Безупречная безопасность** – встроенная система безопасности, единый канал администрирования.

Так же одним из новейших представителей использующих облако является база данных SAP HANA.

УДК 004.738.5:061(043.2)

Толстікова О.В., к.т.н., Кіпіч В.В.
(Національний авіаційний університет, Україна)

ВЕБ-ДОДАТОК ПОШТОВОГО СЕРВІСУ ДЛЯ КОРИСТУВАЧІВ МЕРЕЖІ МАЛОГО ПІДПРИЄМСТВА

Обмін текстовими повідомленнями з необхідною швидкістю в мережі для працівників малих, середніх, великих підприємств з використанням єдиної централізованої системи забезпечує необхідний сервіс для працівників та клієнтів підприємств. Використання веб – додатку поштового сервісу з метою заощадження комп'ютерних ресурсів та забезпечення найліпшою швидкодією сприяє вирішенню даної задачі.

Пропонується програмний веб – додаток для користувачів мережі малого підприємства, які обмежені в комп'ютерних ресурсах. Сервіс додатку є не ресурсоємним, відзивчивим до користувача, захищеним, має можливість легко розширятися до нового функціоналу в разі необхідності та достатньо швидко доставляти повідомлення адресатам.

В якості мови програмування обрана Java, тому що стек технологій Java EE забезпечує побудову масштабованої, надійної і гнучкої серверної архітектури.

Для проектування веб – додатку використовується шаблон проектування: Модель – Представлення – Контроллер (Model – View – Controller). Шаблон забезпечує чіткий поділ проблем, надаючи артефакти, які використовуються виключно в якості даних (моделі), в той час як інші артефакти відповідають (використовуються) виключно за відображення (подання даних), а інші несуть відповідальність за управління даними (контролер) і передають управління необхідному поданню.

Обрана архітектура MVC дозволила чітко розмежувати область дій кожної складової частини проекту:

- модель відповідає за звертання до БД з метою отримання або запису інформації в базу. Звертається із запитом до обраної БД MySQL;
- представлення відповідає за відображення інтерфейсу користувачу. Воно нічого не знає ні про модель ні про контролер. Використано технології HTML, CSS, AJAX, JavaScript;
- контролер відповідає за логіку програми, тобто саме він вирішує який метод в моделі та представлені викликати. Реалізовано за допомогою Servlets, EJB (component, session, entity) складових.

Рівень управління. В якості контролера може служити сама реалізація шаблону MVC, яка повинна забезпечувати надійну структуру. З цим завданням повністю справляється модуль Spring MVC на базі фреймворка MVC. Розгорнута підтримка даного шаблону, а також інших засобів (наприклад, оформлення темами, інтернаціоналізацію, перевірку достовірності, перетворення типів, форматування і т.п.). Головною і найважливішою особливістю його є Inversion of control контейнер, який представляє засоби конфігурування та управління об'єктами Java за допомогою відображення. Контейнер відповідає за управління життєвим циклом об'єкту: створення об'єктів, виклик методів ініціалізації, конфігурування об'єктів шляхом зв'язування їх між собою.

Фреймворк Vaadin, який на відміну від бібліотек на JavaScript і специфічних плагінів для браузерів пропонує сервер-орієнтовану архітектуру, базовану на

JavaEnterpriseEdition. Використання JEE дозволяє виконувати основну частину логіки програми настороні сервера, тоді як технологія AJAX, використовувана на стороні браузера, дозволяє інтерактивно взаємодіяти з користувачем. Для відображення елементів інтерфейсу користувача та взаємодії з сервером на стороні клієнта Vaadin використовує Google Web Toolkit [1-8].

На базі інтеграції фреймворків Spring MVC і Vaadin пропонується структура web-додатку, яка надана на рис. 1.

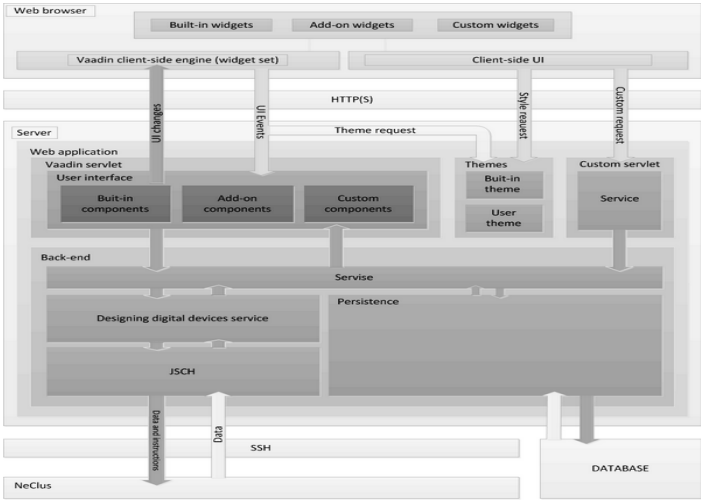


Рис. 1. Структура web-додатку

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Гамма Э. Прийоми об'єктно-орієнтованого проектування. Патерни проектування / Э.Гамма, Р.Хелм, Р.Джонсон, Дж Влиссидес - СПб: Питер, 2001. — 368с.*
2. *Дейтел Х. М. Програмування на Java / Х. М. Дейтел, П. Дж. Дейтел, С. І. Сантрі – М.: ДиаСофтЮП, 2003. – 863 с.*
3. *Дронов В. JavaScript в Web-дизайне / В. Дронов - СПб.: БХВ, 2001. – 880 с.*
4. *Голицына О.Л. Базы данных: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - 2-е изд. М.: Форум:ИНФРА-М, 2009. – 400 с.*
5. *Коржинский С. Настольная книга Web-мастера: эффективное применение HTML, JavaScript / С. Коржинский. - Кнорус, 2000. – 320 с.*
6. *Хеффельфингер Д. Java EE 6 та сервер додатків GlassFish 3 / Д.Хеффельфингер- М.: ДМК Пресс, 2013.-416 с.*
7. *Харроп Р. Spring 3 для професіоналів / Роб Харроп, КларенсХо. – М.: Вильямс, 2012. – 880с.*
8. *Хеффельфингер Д. Розробка додатків Java EE 6 в NetBeans 7 / Д.Хеффельфингер-М.: ДМК Пресс, 2013.-330 с.*

УДК 629.735.33(043.2)

Харченко В.С., д.т.н.
(Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Україна)

НЕЙМАНІВСЬКА ПАРАДИГМА, БЕЗПЕЧНИЙ І ЗЕЛЕНИЙ КОМП'ЮТИНГ ТА IT-КООПЕРАЦІЯ: ЩО СПІЛЬНОГО?

Еволюція парадигми фон Неймана: надійнісний і зелений виміри. 63 роки тому Джон фон Нейман прочитав цикл лекцій «Lectures on probabilistic logics and the synthesis of reliable organisms from unreliable components». Однією з фундаментальних ідей лекцій була парадигма побудови надійних систем з ненадійних компонентів. Фактично, це дозволило сформувати ключові принципи теорії резервування, зокрема, мажоритування, цифрових (і не тільки) систем. Нейманівська парадигма (НП) еволюціонувала відповідно до розвитку технологій, компонент і систем, їх властивостей (від безвідмовності до гарантоздатності).

В доповіді аналізуються 6 стадій її еволюції, завершуючи парадигмою «гарантоздатних/безпечних IT-інфраструктур з недостатньо безпечних систем із змінними параметрами в умовах невизначеності середовища». Схема аналізу має такі складові (рис.1): елемент/властивості елементу-система/властивості системи-принципи, методи, засоби.

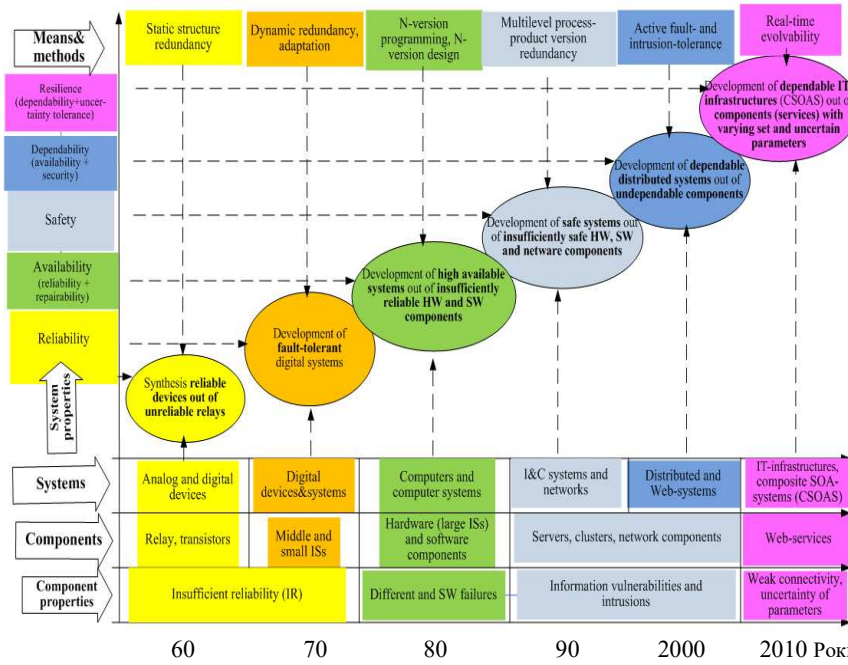


Рис.1. Еволіціонування парадигми фон Неймана

Кожен з етапів приблизно має десятирічній термін, починаючи з 60-х років і завершуючи 2010-ми роками. Іншою лінією розвитку НП є її модифікація для ненадійнісних властивостей (характеристик) систем, зокрема, енергоефективності та енергозберігання. Системи, для яких вони є пріоритетними, називають зеленими (green systems). Поставимо запитання: чи можливий такий варіант НП: зелена система з незелених (недостатньо зелених) компонент (?). Прикладом можливості і доцільності такого формулювання є система на кристалі, яка має кілька незалежних каналів вимірювання, контролю або керування, показники енергоспоживання яких можуть бути покращено шляхом взаємного припустимого зсуву у часі їх функціонування і відповідної керованої синхронізації, що забезпечує зменшення кількості одночасних спрацювань елементів. Якщо маємо кілька паралельно працюючих резервних каналів, тоді такий підхід, за умов можливості їх несинхронного функціонування, ілюструє реалізацію НП у андійнісному і зеленому вимірах.

Зелений комп'ютинг: таксономія. Зелений комп'ютинг – особливий вид комп'ютингу. У вузькому смислі комп'ютинг – це методи і засоби обчислень на комп'ютері або комп'ютерній системі, у широкому – сукупність наукових знань,

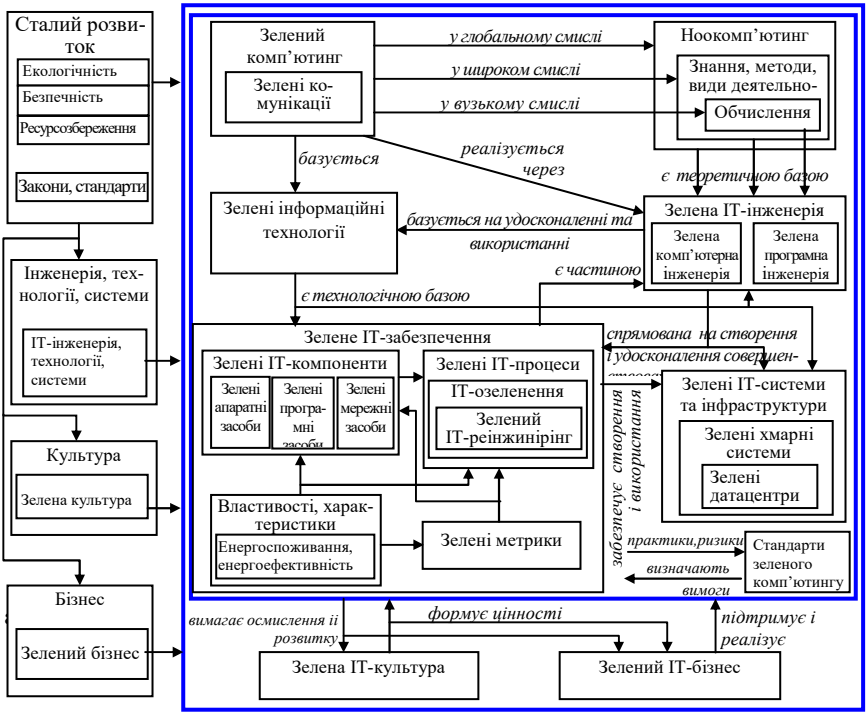


Рис.2. Таксономічна схема зеленого комп'ютингу

інженерних методів і видів діяльності з розробки та застосування комп'ютерних технологій, у глобальному – це частина ноосфери і може бути визначений як ноокомп'ютинг, важлива складова світової інфраструктури. Відповідно зелений комп'ютинг визначається як енергоефективні (енерго-

зберігаючі) обчислення і обчислення на комп'ютерах, керуючих зеленими технічними системами (у вузькому смислі), або як сукупність знань, методів і видів діяльності, пов'язаних підвищенням енергоефективності, екологічності та безпеки комп'ютерних технологій (у широкому смислі). З урахуванням цих складових зелений комп'ютинг природнім чином монтується у поняття ноокомп'ютингу. Таксономічна схема (рис.2) поєднує основні поняття зеленого комп'ютингу.

ІТ-кооперація у галузі зелених і безпечних технологій. Розвиток ІТ-індустрії як ключової галузі економіки України, галузі, яка може у стислі терміни зробити її провідною у світовому розподілі праці потребує спільних зусиль університетів, ІТ-компаній, урядових і комунальних органів влади. Технології зеленого і безпечного комп'ютингу, спрямовані на вирішення двох найгостріших проблем (безпеки середовища і енергозабезпечення), можуть і мають бути рушійними силами такого розвитку. Їх створення національними розробниками дає змогу перейти від виключно аутсорсингової моделі розвитку до інноваційної моделі, спрямованої на створення нових технологій об'єднаними індустріальними і університетськими командами, а також бізнесової моделі, яка базуються на русі старт-апів і спін-оффів. Україна може за об'ємом створеного ІТ-продукту порівнятися з Індією за умов пріоритетного розвитку саме двох останніх моделей.

Обовязковою складовою має бути соціальна складова. Спеціалісти з інформаційних технологій і зеленого комп'ютингу повинні бути провідниками цінностей зеленої ІТ-культури, зеленої культури і культури безпеки взагалі. Взагалі зелені ІТ повинні гармонійно розвиватися як об'єкт і засіб озеленення (забезпечення безпеки) та інструмент просування зелених цінностей. Така концепція сформована і реалізується кафедрою комп'ютерних систем і мереж ХАІ на протязі останніх десяти років. Основний принци – системна участь у розробленні та виконанні міжнародних проектів за програмами FP7, Horozon2020, TEMPUS, двосторонніх проектів з університетськими центрами країн Євросоюзу, США, проектів за національними програмами і замовленням ІТ-компаній, а також у розвитку спін-офф, старт-апів, які виконуються викладачами, аспірантами і студентами у галузі безпекових і зелених технологій.

Висновки. Нейманівська парадигма еволюціонує, наповнюється новим змістом і дає змогу генерувати принципові ідеї та рішення для створення безпечних і зелених ІТ-систем. Зелений комп'ютинг стає самостійною і важливою складовою комп'ютерних наук і технологій. Розроблення і впровадження безпекових і зелених технологій є інноваційним напрямом розвитку ІТ-галузі.

Матеріали доповіді базуються на огляді результатів проектів TEMPUS (MASTAC, SAFEGUARD, GREENCO, CABRIOLET, SEREIN), KhAI-ERA (FP7) та інш. а також видання: *Харченко В.С. (ред.) Зеленая ИТ-инженерия. В 2х томах. Том.1. Принципы, компоненты, модели; Том.2. Системы, индустрия, социум, ХАИ, 2014, 594с., 688с.*

УДК 004.056.53(044)

Юдін О.К., д.т.н., Корнієнко Б.Я., Мариняк М.С.
(Національний авіаційний університет, Україна)

ЗАХИСТ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ МІЖНАРОДНОГО СТАНДАРТУ ISO 27001

Сьогодні важко уявити бізнес і процес управління організацією, чи підприємством без підтримки інформаційних технологій, які необхідні для роботи організації. Підтримка та забезпечення безпеки інформаційних об'єктів – дуже важливе завдання для будь-якого бізнесу. Кожен власник бізнесу, а також призначене ним керівництво не повинні закривати очі на поточний стан інформаційних систем, вони повинні аналізувати та оцінювати існуючі проблеми і вирішувати їх.

Кожне підприємство активно працює над забезпеченням інформаційної безпеки, але цього недостатньо. В загальному розумінні, інформаційна безпека пов'язана з обмеженням доступу третіх осіб до інформації. Передові світові корпорації вирішують надзвичайно великий комплекс проблем, пов'язаних з інформаційною безпекою. Їх дії над забезпеченням безпеки економлять кошти підприємства як у процесі роботи, так і за рахунок нейтралізації неприємних наслідків.

Кращі світові практики в галузі управління інформаційною безпекою описані в міжнародному стандарті на системи менеджменту інформаційної безпеки ISO / IEC 27001 (ISO 27001). ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси.

Стандарт встановлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки у контексті існуючих бізнес-ризиків організації.

Вимоги даного стандарту мають загальний характер і можуть бути застосовані до всіх організацій незалежно від їх типу, розміру, форми власності.

Сертифікована система менеджменту інформаційної безпеки - гарантія того, що система управління інформаційною безпекою правильно й ефективно впроваджена в сфери діяльності організації. А ефективна система менеджменту інформаційної безпеки, у свою чергу, забезпечує необхідний рівень захисту активів організації, тобто істотно знижує ризик нанесення організації збитку внаслідок порушення інформаційної безпеки і гарантує, що заходи та засоби захисту інформації є адекватними і пропорційними можливому збитку організації.

Отже, кращі світові практики в галузі управління інформаційною безпекою описані в міжнародному стандарті на системи менеджменту інформаційної безпеки ISO / IEC 27001 (ISO 27001). Стандарт встановлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки у контексті існуючих бізнес-ризиків організації.

Хоча, єдиного алгоритму стосовно впровадження політики безпеки не існує, так як технології на місці не стоять, вони прогресують, і прогресують достатньо швидко. Тому необхідно розробляти достатньо ефективну політику безпеки комп'ютерної мережі об'єкту інформаційної діяльності і тоді можна буде досягти найвищого рівня ефективності її захищеності.

Наукове видання

ЗБІРНИК ТЕЗ
VIII МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2015)

16–18 квітня 2015 року

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

Підп. до друку 14.04.15. Формат 60x84/16. Папір офс.
Офс. друк. Ум. друк. арк. 7,90. Обл.-вид. арк. 8,5
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