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

ЗБІРНИК ТЕЗ

VI МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2013)

11–13 червня 2013 року

Київ 2013

УДК 004.7(043.2)

Збірник тез VI Міжнародної науково-технічної конференції «Комп'ютерні системи та мережні технології» (CSNT-2013), м. Київ, 11–13 червня 2013 р. Національний авіаційний університет. – К.: НАУ, 2013. – 136 с.

Збірник містить тези доповідей, які були представлені на конференції «Комп'ютерні системи та мережні технології» (CSNT-2013). В доповідях розглянуті наукові, технічні та технологічні проблеми будови, проектування сучасних комп'ютерних систем, засоби і методи моделювання комп'ютерних мереж, проблеми захисту ресурсів в інформаційних системах, проблеми і технології підготовки авіаційних фахівців.

Затверджено вченою радою Інституту комп'ютерних інформаційних технологій Національного авіаційного університету (протокол № 5 від 10 червня 2013 р.).

ЗМІСТ

УДК 004.77

Н.І. Алішов, д.т.н; В.А. Марченко, к.т.н.
(Інститут кібернетики ім. В.М. Глушкова НАНУ, Україна)

ЗАСТОСУВАНЯ МЕТОДУ ОПТИМІЗАЦІЇ ДОСТАВКИ ІНФОРМАЦІЙНИХ ПАКЕТІВ У SDN МЕРЕЖАХ

Прогрес сучасних інформаційних технологій в частині створення нових підходів до побудови комп'ютерних мереж призвів до появи нового класу мереж що називаюся "програмно визначені мережі"(*Software Defined Networking*)[1].

Вказана парадигма створення сучасних комп'ютерних мереж визначає нову базову архітектуру мережі. В ній визначається два умовних рівні:

- рівень комутації пакетів;
- рівень прийняття рішень про комутацію.

Рівень комутації представлений спрощеними активними мережевими пристроями, основна задача яких полягає у отриманні пакету та передача його адресату при умові знаходження відповідного правила у таблиці потоків. У разі коли вказаного правила немає, то необхідні ідентифікаційні дані пакету пересилаються на центральний комутатор (рівень прийняття рішень про комутацію) за допомогу спеціального протоколу управління OpenFlow[2], який приймає рішення про подальшу комутацію пакету. Таким чином центральний комутатор знає про архітектуру всієї мережі та про всі особливості її функціювання. Така особливість нової мережної архітектури дозволяє власнику мережі програмувати поведінку комп'ютерної мережі у відповідності до його потреб без необхідності зміни використовуваного мережного обладнання.

Авторами запропоновано впровадження методу оптимізації часу доставки інформаційних масивів даних[3] у програмно визначені мережі. Це дозволить реалізувати можливість доставки будь-яких масивів даних в заданий вузол у заданий час, або організуавти паралельну передачу різнорідних даних з різними вимогами до часових затримок. Вирішення вказаних задач у сучасних комп'ютерних мережах є неможливим без значних накладних витрат.

Таким чином використання запропонованого авторами методу оптимізації часу доставки інформаційних пакетів у програмно реконфігуруємих мережах є перспективним напрямом подальшого розвитку сучасних комп'ютерних мереж.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Farias, F. N. N., Salvatti, J. J., Cerqueira, E. C., Abelem, A. J. G.* A Proposal Management of The Legacy Network Environment using OpenFlow Control Plane // Network Operations and Management Symposium (NOMS). – 2012 , Maui, HI, USA. – p. 1143-1150.
2. OpenFlow Specification. — Режим доступу.– http://www.openflow.org.
3. *Алишов Н.И., Оруджева С.Г.* Оптимизация времени доставки информационных масивов данных // Актуальні проблеми економіки. – 2009. – №12(102). – С. 194–199.

УДК 004.45(043.2)

В.І. Андрєєв, к.т.н; О.В. Андреєв
(Національний авіаційний університет, Україна)

МЕТОД ЕКСПЕРИМЕНТАЛЬНОГО ДОСЛІДЖЕННЯ ТА ЕКСТРАПОЛЯЦІЇ ХАРАКТЕРИСТИК ТРАФІКУ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Розвиток комп'ютерної техніки в наш час набув великого розмаху. З розвитком комп'ютерних мереж з'явилась необхідність моніторингу трафіку з метою його оптимізації та управління. На базі локальної мережі ІКІТ було розглянуто деякі програмні та апаратні засоби моніторингу трафіку локальної комп'ютерної мережі з метою його управління.

Для досягнення цієї мети на базі методики статистичної обробки експериментів, методу статистичного імітаційного моделювання (СІМ) та методу двопараметричної оптимальної екстраполяції розроблено метод дослідження та оптимальної екстраполяції характеристик нестаціонарного трафіку комп'ютерних мереж. За допомогою експерименту показана ефективність розробленого методу дослідження характеристик нестаціонарного трафіку на фоні завад.

Моніторинг трафіку проводиться за допомогою сніфферу, наприклад *PRTG Network Monitor*, який дозволяє вимірювати значення трафіку з інтервалом в одну хвилину. На трафіку обрано інтервал за три хвилини, для якого виконано три експерименти з різними значеннями інтервалу спостереження ΔT, інтервалу екстраполяції τ та величини потужності завади σ^2_ξ . Запропонована методика статистичної обробки результатів експериментів з даними трафіку, на базі якої розроблена програма статистичного імітаційного моделювання ПСІМ - *traffic* у системі *MathCAD*. За допомогою програми виконана екстраполяція для десяти триад трафіку (де n – номер триади) та обчислені значення відносних похибок екстрапольованих величин $Y_3(n)^*$ до відповідних значень трафіку без завади $X_3(n)$ і з завадою $Y_3(n) - (\delta_{X(n)}, \delta_{Y(n)})$.

Експерименти показали, що алгоритм оптимальної двопараметричної екстраполяції при роботі з реальним трафіком КМ дає прийнятні для практики результати, які залежать від параметрів – інтервалу спостереження ΔT, екстраполяції τ і потужності завади σ^2_ξ .

Обосновано набір апріорної ймовірностної інформації, яку необхідно знати про трафік, для виконання оптимальної екстраполяції в оптимальному режимі. Це наступний набір: m_{Y1}, m_{Y2}, D_{Y1}, D_{Y2}, σ^2_{Y1}, σ^2_{Y2}, $K_Y(t_1, t_2)$. Запропоновано алгоритм довизначення відсутніх параметрів для точки трафіку, яку збираємось екстраполювати: m_{Y3}, D_{Y3}, σ^2_{Y3}, $K_Y(t_1, t_3)$, $K_Y(t_2, t_3)$. На базі апріорної та ймовірностної інформації, що була довизначена, запропоновано алгоритм екстраполяції трафіку в реальному часі на основі оптимального способу двопараметричної екстраполяції.

Запропоновано алгоритм на основі методу двопараметричної екстраполяції, за допомогою якого можна організовувати перерозподіл трафіку між робочими станціями чи інтерфейсами мережі при його перенавантаженні. Для цього необхідно мати набір спеціального електронного обладнання та спеціальне програмне забезпечення для сервера.

УДК 004.78 (043.2)

Є.Б. Артамонов
(Национальный авиационный университет, Украина)

СЕТЕВАЯ ИНФОРМАЦИОННАЯ СИСТЕМА СОДЕРЖАНИЯ МОДУЛЕЙ ДИСЦИПЛИН, КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ КАЧЕСТВА ОБУЧЕНИЯ

В последнее время всё чаще поднимается вопрос о соответствии уровня образования, которое получают студенты в высших учебных заведениях, требованиям рынка.

По законам рынка формируется принцип «кто оплачивает счета, тот и заказывает «профиль» выпускников, а основным заказчиком уже давно является государство. Именно оно, по большей части, финансирует образование. Также к процессу «заказа» специалистов начали подключаться государственные и коммерческие организации.

Но и тут не обходится без неприятных сюрпризов - договора с ВУЗами заключаются на подготовку специалистов по определённым направлениям и специальностям, но единственная информация, которой располагает непосредственный заказчик – это рабочий учебный план, в котором указан перечень дисциплин, но содержание этих дисциплин является недоступной.

Но и предприятия готовы идти на риск, вкладывая деньги в украинскую систему образования, однако для этого требуются инструменты, которые позволят не только выбрать ВУЗ и направление обучения по потребностям предприятия, но и задать требования на изучаемые курсы дисциплин, а также их наполнение.

На сегодня подобного инструмента не существует не только в Украине, но и в мире. Реализация такого инструмента должна проводиться в несколько этапов, среди которых есть, как организационные, так и чисто программные. Необходимо четко осознавать, что на выходе должен появиться не просто программный продукт или база данных, а полноценная сетевая система со всеми возможностями по управлению сетевыми базами данных и гибким интерфейсом.

Данная система может позволить не только предприятиям упростить поиск будущих сотрудников, но и абитуриентам делать осознанный выбор при поступлении в ВУЗ, что повысит качество основного продукта ВУЗов – образовательной услуги.

УДК 621.3 (043.2)

О.К. Басараб
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький
І.А. Кисельов
Національний авіаційний університет, Київ

МЕТОДИКИ ВИЗНАЧЕННЯ РАЦІОНАЛЬНОЇ СТРУКТУРИ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Вступ. Аналіз оперативно-службової діяльності (ОСД) Державної прикордонної служби України (ДПСУ) показав, що ефективність охорони кордону залежить від ефективності функціонування інформаційно-телекомунікаційних систем (ІТС). Складність будови сучасних інформаційно-телекомунікаційних систем дозволяє зробити висновок про те, що важливим елементом, від якого залежить працездатність цих систем, є мережева складова. В більшості телекомунікаційних систем спеціального призначення, в тому числі і в ДПСУ, використовуються стандартні мережеві технології. На сьогодні доступність телекомунікаційної системи (ТКС) ДПСУ не відповідає світовим вимогам до сучасних комп'ютерних мереж що знижує ефективність оперативно-службової діяльності до неприпустимих значень.Існуючі підходи до побудови телекомунікаційних систем спеціального призначення не враховують особливості зумовлені використанням ТКС в складі ІТС ДПСУ. Так система показників яка запропонована в не містить показники ефективності ОСД ДПСУ. У зв'язку з цим, необхідність підвищення ефективності функціонування ІТС ДПСУ і зокрема їх мережевої складової вимагає вирішення питань розробки наукового апарату визначення раціональної будови мережі з використанням резервуванням каналів і особливостей ОСД ДПСУ.

Метою даної роботи є розробка методики визначення раціональної структури ТКС ДПСУ на основі використання резервних каналівз урахуванням особливостей функціонування ТКС у складі інтегрованої інформаційно-телекомунікаційної системи ДПСУ «Гарт».

Першим елементом методики визначенняраціональної структури ТКС ДПСУ є побудова множини $\mathbf{M}(M_1,M_2,\dots M_n)$ можливих варіантів будови мережі з використанням різних способів резервування каналів та обраних протоколів динамічної маршрутизації. Важливим елементом методики є проведення експертизи для кожного можливого варіанту побудови мережі M_i. При проведенні експертизи важливим є коректний вибір системи показників та визначення критеріїв оцінки.

Висновок. В результаті проведених досліджень сформована методика вибору раціональної будови PartialMesh мережі ДПСУ. Її важливим елементом є методика отримання шляхом моделювання функції належності для нечіткого комплексного імовірнісного показника ефективності ОСД в залежності від архітектури мережі.Запропонованийпідхід дозволяє здійснити раціональнийвибір побудови мережевої складової ІТС ДПСУ з резервуванням каналів і використанням протоколу динамічної маршрутизації.

УДК 004.912(043.2)

О.О. Бєляков
(Національний авіаційний університет, Україна)

АНАЛІЗ МОДЕЛЕЙ ПРЕДСТАВЛЕННЯ ЗМІСТУ ТЕКСТОВОЇ ІНФОРМАЦІЇ

Глобальна автоматизація суспільства вимагає впровадження систем інтелектуальної обробки інформації в усі сфери життя та виробництва. Основна частина інформації, яку обробляють такі системи, представлена у вигляді тексту. Архітектура систем інтелектуальної обробки текстової інформації базується на використанні моделей представлення змісту тексту. В даній роботі проаналізовані чотири моделі представлення змісту текстів з точки зору сфер їх застосування.

Логічні моделі подання знань реалізуються засобами логіки предикатів. Предикатом називається функція, що приймає два значення і призначена для вираження властивостей об'єктів або зв'язків між ними.

В основі мережевих моделей лежить конструкція, названа семантичною мережею. Термін «семантична» означає «смислова». У самому загальному випадку семантична мережа являє собою інформаційну модель предметної області і має вигляд графа, вершини якого відповідають об'єктам предметної області, а дуги – відносинам між ними .

Іншою моделлю представлення змісту тексту є фреймова модель. Фреймом називається також і формалізована модель для відображення образу. Фрейм має певну внутрішню структуру, що складається з множини елементів, які мають назву «слоти», яким також присвоюються імена.

Продукції, так само, як і фрейми, є найбільш популярними засобами подання змісту тексту в штучному інтелекті. Продукції, з одного боку, близькі до логічних моделей, що дозволяє організовувати на них ефективні процедури виведення, а з іншого боку, більш наочно відображають знання, ніж класичні логічні моделі. У загальному вигляді під продукцією розуміється вираз такого вигляду:

(i); Q; P; ; N.

Тут і – ім'я продукції, за допомогою якого дана продукція виділяється із усієї безлічі продукцій. В якості імені може виступати деяка лексема, що відображає суть даної продукції (наприклад, "купівля книги"), або порядковий номер продукцій в їх безлічі, що зберігається в пам'яті системи.

УДК 621.376

А.С. Бойко
(Дата Арт, Украина)

HDINSIGHT – РЕШЕНИЕ ОТ КОМПАНИИ MICROSOFT ДЛЯ АСИНХРОННОГО АНАЛИЗА БОЛЬШИХ МАССИВОВ ДАННЫХ

По результатам исследований компании Gartner, количество данных в современном мире будет увеличиваться в 10 раз каждый год. Это связано с тем, что сейчас на каждого человека имеющего выход в интернет приходится порядка 4.3 устройств которые могут генерировать новые данные (домашний и рабочий ПК, планшетный ПК, смартфон и т.д.). Также важным аспектом есть то, что порядка 85% данных, которые появляются в интернете, являются новыми данными. Сами по себе «сырые» данные обычно не несут много полезной информации, но, проанализировав эти данные, можно получить много ценной информации. Основная задача направления BigData – разработка новых подходов и инструментов, которые смогут позволить собрать и обработать большой объем данных за меньшее время, чем мы потратили бы используя традиционные способы анализа данных.

В докладе представлено сравнение традиционных подходов к анализу данных со специализированными. Указаны положительные и отрицательные особенности каждого из подходов. Основными преимуществами специализированных подходов есть практически линейный прирост производительности при увеличение количества вычислительных мощностей в кластере и ориентация на работу с хранилищами данных которые исчисляются петабайтами.

В данном докладе будет описано использование решения HDInsight, построенного на базе платформы Hadoop и размещаемого в облаке WindowsAzure. Основными преимуществами решения HDInsight есть ориентация на размещение в облаке, что позволило упростить процесс наращивания мощностей при необходимости, а также отказаться от использования невостребованных ресурсов сохранив при этом как исходные данные, так и результаты анализа. Еще одним преимуществом решения HDInsight есть возможность его установки на операционную систему WindowsServer, что позволяет строить приватные и гибридные кластеры для анализа данных.

В данном докладе будет рассмотрен пример использования решения HDInsight в реальном коммерческом проекте. Техническая задача, которую необходимо было решить, состояла из сбора показателей датчиков с мобильного устройства и сравнения этих показателей с огромным словарем предварительно определенных эталонных значений. Размещать копию словаря на мобильном устройстве не представлялось возможным из-за его размера, также было невозможно проводить вычисления на устройстве из-за ограниченности центрального процессора мобильного устройства. Будет подробно описан процесс создания специализированных клиентов на мобильные устройства и полный перенос всех вычислений в публичное облако.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Tom White "Hadoop: The Definitive Guide, 3rd Edition", O'Reilly Media, Print ISBN:978-1-4493-1152-0 | ISBN 10:1-4493-1152-0Ebook ISBN:978-1-4493-1151-3 | ISBN 10:1-4493-1151-2
2. Webinar "Hadoop: A Deep Dive" by WANdisco (http://go.wandisco.com/hadoop-deep-dive.html)
3. Webinar "Hadoop: HBase In-Depth" (http://go.wandisco.com/hadoop-hbase.html)
4. Webinar "Big Data - Enterprise-Enabling Hadoop for the Data Center" by WANdisco (http://go.wandisco.com/enterprise-hadoop.html)
5. http://gettingstarted.hadooponazure.com/
6. http://www.windowsazure.com/en-us/manage/services/hdinsight/

УДК 004.942

Ю.Е. Бояринова, к.т.н.
(НТУУ «КПИ», Украина);
Н.А. Городько
(ИПРИ НАНУ, Украина)

ГИПЕРКОМПЛЕКСНЫЙ ПОДХОД К МОДЕЛИРОВАНИЮ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ

Распределенная система обработки информации (РСОИ) относится к классу сложных и многофункциональных, анализ и оптимизация функционирования которых нуждаются в применении средств математического и компьютерного моделирования[1].

В процессе функционирования модулей РСОИ возникают задачи, целенаправленное решение которых должно обеспечивать быстродействие, надежность и живучесть системы. Сложность рассматриваемой системы, ее масштабность, большое число рассматриваемых условий и ограничений различного уровня детализации требует достаточно полного описания и исследования их в рамках математического моделирования.

На первом этапе моделирования на всем множестве модулей n определяется множество функциональных параметров модуля e_i и их количественные значения x_i. Затем, в виде гиперкомплексных числовых систем (ГЧС) вводится формализованное описание характеристик процессов функционирования модулей РСОИ $X = \sum_{i=1}^{n} x_i e_i$ и устанавливаются законы их взаимодействия $e_i e_j = \sum_{k=1}^{n} \gamma_{ij}^{k} e_k$.

Область допустимых значений решения задачи моделирования является множество возможных параметров функционирования моделей системы, которые удовлетворяют ограничениям, налагаемым на требуемые ресурсы $g_i(X) \le b_i$.

Оптимальным решением X^* можно считать такое допустимое решение, при котором критерии оценки результата F^* достигают своего экстремального значения, т. е. решение, удовлетворяющее условию: $extr F_i(X) = F_i(X^*)$.

Для нахождения оптимального решения поставленной задачи в зависимости от вида и структуры гиперкомплексных функций и уравнений от гиперкомплексной переменной и с гиперкомплексными коэффициентами, которые описывают ограничения и критерии оценки результата, используются методы предложенные в [2,3].

Переход к гиперкомплексному представлению данных обеспечивает быстродействие, надежность и живучесть РСОИ, что обусловлено структурой и свойствами ГЧС.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Э. Таненбаум, М. Стеен.* Распределенные системы. Принципы и парадигмы — Санкт-Петербург: Питер, 2003. — 877 с. — ISBN 5-272-00053-6
2. *М.В.Синьков, Ю.Е.Бояринова, Я.А.Калиновский.* Конечномерные гиперкомплексные числовые системы. Основы теории. Применения. – К.: ИПРИ НАН Украины, 2010. – 389 с. ISBN 978-966-02-5677-4
3. *Я.А.Калиновский, Ю.Е.Бояринова.* Высокоразмерные изоморфные гиперкомплексные системы и их применение. – К: ИПРИ НАН Украины, 2012. – 183с. ISBN 978-966-02-6360-4

УДК 004.738:004.056.53(043.2)

Д. Б. Бур'янцев; С. Б. Литовка; А. І. Гуля
(Національний авіаційний університет, Україна)

БЕЗПЕКА ХМАРНИХ СЕРВІСІВ

На даний момент хмарні сервіси дуже стрімко розвиваються, і питання про безпеку їх використання стоїть дуже гостро. Як прості так і корпоративні користувачі хочуть бути впевненими, що їх інформація буде в повній безпеці, як на віртуальному так і на фізичному рівнях.

Зараз багато великих компаній мають свої хмарні сервіси, серед них можна назвати такі: iCloud від компанії Apple, Google Drive, Dropbox, нещодавно з'явився copy.com який робить акцент на високу безпеку і чималий обсяг безкоштовного сховища.

Хмарні сервіси дають можливість користувачам ПК, що не мають достатнього обсягу фізичної пам'яті, розширювати її за допомогою віртуальної, яку надають сервіси такого роду. Також з допомогою "хмари" можна створювати різного роду обчислювальні процеси не маючи при цьому потужних апаратних ресурсів, і при всьому цьому мати доступ до всього в будь-якій точці світу, при наявності Інтернету.

Звичайно при виборі сховища своїх даних варто відштовхуватися і від того, чим компанія, що надає послуги займалася або займається ще. Наприклад, copy.com, творці якого, як вже було вище сказанно, акцентують увагу на безпеці свого дітища, тому що цей ресурс створено компанією Barracuda Networks, основна діяльність якої – захист даних.

Існують серйозніші сервіси – у них захист і надійність в рази вище, але звичайні користувачі швидше за все не будуть використовувати їх з причини високої вартості і спрямованості цих компаній на корпоративних клієнтів.

Серйозні постачальники хмарних послуг, такі як Amazon, CSC, HP, IBM, Salesforce.com і Verizon Business, мають дуже потужні механізми безпеки. Вони працюють на різних рівнях, як на прикладному, так і на інфраструктурному і включають в свій склад такі інфраструктурні засоби, як системи шифрування і міжмережеві екрани. Ці постачальники зберігають у хмарі петабайт конфіденційних даних і поки що не відчувають серйозних проблем у сфері безпеки [1].

Компанії, що пропонують різне програмне забезпечення для інформаційної безпеки, створили багато систем шифрування і міжмережевих екранів для захисту хмарних послуг. Наприклад CloudProtect CloudSpan від компанії Layer 7 та JaxView for Cloud Management від компанії Managed Methods. Такі компанії, як Catbird Networks, Altor Networks і Reflex Systems, також адаптували свої продукти для безпеки центрів обробки даних до роботи в хмарному середовищі [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Безопасность в облаке. [Electronic resource] / Інтернет-ресурс. — Режим доступу: http://www.cisco.com/web/UA/about/news/2011/11152011b.html — Загол. з екрану.

УДК 658.52 ; 681.3

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

ВИКОРИСТАННЯ ЕЛІПТИЧНИХ КРИВИХ В ЗАХИСТІ ІНФОРМАЦІЇ

Актуальним є вирішення задач: адаптація сучасних методів криптографічного захисту інформації до методів стиску та компактного представлення інформаційних потоків зображень.

Зрозуміло, що новим та актуальним підходом для вирішення зазначених завдань є використання інформації, яка міститься в графічному зображенні при шифруванні інформаційного потоку даних

У додатку до ДСТУ 4145-2002 еліптична крива над кінцевим простим полем $GF(p)$ визначається як безліч пар (x,y), таких що $x,y \equiv GF(p)$, що задовольняють рівнянню: $y^2 = x^3 + ax + b \ mod \ p$, $a,b \equiv GF(p)$ (1).

Необхідно визначити основні параметри та структуру інформації до якої буде адаптований алгоритм еліптичних кривих. В сучасній роботі з графічною інформацією, частіше за все розглядають зображення в кольорових моделях RGB та YUV. Для формування ключа на базі еліптичної кривої візьмемо деяку точку $G(x,y)$ яка належить еліптичній групі $B(a,b)$. Далі використовуючи відому обом учасникам передачі точку $G(x,y)$ вони генерують відкриті ключі: $P_a = n_a G$; $P_b = n_b G$. Де n_a та n_b випадкові множники.

Метод генерації випадкових чисел не гарантує повного забезпечення надійності і крім того використовує додаткові ресурси апаратури. Для уникнення цієї проблеми можна використовувати елементи переданої інформації.

Перевагами такого методо розрахунку випадкових значень є те, що непотрібно використовувати додаткрві ресурси для проведення підрахунків випадкових значень, тому, що розрахунки елептичної кривої проводяться заздалегідь для генерація ключа. Також плюсом є той факт, що інформація яка знаходиться на зображенні є унікальною та неповторною.

Слід зазначити що подібні алгоритми працюватимуть лише зі сторони відправника, але також можливе застосування і зі сторони отримувача при наявності у останнього зображення які не є відкритими та доступними для громадськості.

Підводячи підсумки з усього вище сказаного, можна зробити наступні висновки, що системи криптографічного захисту з адаптованим до графічного зображення алгоритмом еліптичних кривих – можуть формувати доволі криптостійкий шифротекст.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. ISBN 5-89176-233-1.
2. Юдін О.К. Кодування в інформаційно-комунікаційних мережах:- Монографія. - К.: НАУ, 2007.-308с

УДК 004.73(042.4)

В.А. Василенко, к.т.н.
(Національний авіаційний університет, Україна)

ЗАДАЧА ВЫБОРА ПАРАМЕТРОВ ОБРАТНОЙ СВЯЗИ В СИСТЕМЕ УПРАВЛЕНИЯ КОМПЬЮТЕРНОЙ СЕТЬЮ

В работе [1] рассмотрена задача управления сетью передачи данных (СПД) как сложной распределенной системой с задержками доставки пользовательской, сигнальной и управляющей информации. Любая информационно-коммуникационная сеть – это многосвязная система с большим количеством сетевых и терминальных узлов, которые следует рассматривать как элементарные объекты управления, и со случайными задержками в каналах обратной связи.

Разница между борьбой с перегрузкой и управлением потоком состоит в следующем [2]. Предотвращение перегрузки направлено на то, чтобы сети справлялись с проходящим трафиком. При этом нужно учитывать множество факторов, снижающих пропускную способность сети.

Задача управления потоком состоит в согласовании скорости передачи отправителя со скоростью, с которой получатель способен принимать поток пакетов. Однако, чтобы данная схема работала, необходимо тщательно настроить временные параметры. И в том, и в другом случае правильный выбор значения постоянной времени является далеко не тривиальной задачей.

Если маршрутизатор как управляемый объект будет мгновенно реагировать на самое начало перегрузки, система будет находиться в состоянии постоянных незатухающих колебаний. С другой стороны, если маршрутизатор для большей надежности будет давать информацию о возникающей перегрузке с большой задержкой, то механизм борьбы с перегрузкой будет реагировать слишком медленно, чтобы приносить вообще какую-либо пользу.

Поэтому каждый сетевой узел (в том числе и маршрутизатор) должен следить за состоянием своих выходных линий и других ресурсов. Например, с каждой линией можно связать вещественная переменная u, значение которой в пределах от 0,0 до 1,0 отражало бы использование линии за последнее время. Такую усредненную оценку загруженности линии можно получить, периодически замеряя мгновенную загруженность линии (0 либо 1) и рассчитывая новое значение переменной u по формуле

$$u_{new} = au_{old} + (1-a)f),$$

где константа a определяет, насколько быстро маршрутизатор забывает свое прошлое.

Таким образом, даже без учета задержек система управления сетью представляет собой параметрическую систему первого порядка.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Виноградов Н.А.* Сеть передачи данных как объект управления // Комп'ютерні системи та мережні технології (CSNT-2012): Збірник тез IV Міжнародної науково-технічної конференції, м. Київ, 13-15 червня 2012 р. Національний авіаційний університет. – К.: НАУ, 2012. – 136 с. (с. 34).
2. *Tanenbaum, A.S.* Computer Networks, 5th Ed. / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 pp.

УДК 004.048

Г.М. Велиджанова, к.т.н.
(*Институт Кибернетики, Азербайджан*)

МЕТОД РАСЧЕТА МОДЕЛИ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ С ДВУМЯ ТИПАМИ ЗАЯВОК

В последние годы интенсивно исследуются модели систем массового обслуживания (СМО) с разнотипными заявками, которые являются математическими моделями многих процессов в различных отраслях науки и техники [1]. В них изучены модели СМО, где обслуживание заявки не приводит к уменьшению ее ресурсов. Вместе с тем, во многих СМО обслуживания заявки связано с расходованием ресурсов системы.

В настоящей работе изучается модель СМО с двумя типами заявок – расходующие заявки (*p*-заявки) и снабжающие заявки (*c*-заявки). В ней после обслуживание одной *p*-заявки ресурсы СМО уменьшаются, а обслуживание одной *c*-заявки приводит к увеличению ресурсов. Обслуживание разнотипных заявок осуществляются на различных каналах, при этом их параллельное обслуживание невозможно. Предполагается, что имеются ограничения на максимальный и минимальный уровень ресурсов СМО, а также на максимальная длина очереди *c*-заявок ограничена некоторой величиной.

Подобная модель СМО ранее было изучена в работе [2], где предложен подход к расчету ее характеристик. В ней при снижении уровня ресурсов до определенной величины осуществляется заказ для их поставки. Этот заказ выполняется с некоторой задержкой и не в полном объеме. Основными характеристиками данной модели являются средняя длина очереди *p*-заявок, вероятности (интенсивности) их потери, а также средний уровень ресурсов системы. Расчет этих характеристик позволяют определить оптимальные значения объемов поставок ресурсов, а также моменты таких поставок.

В настоящей работе предлагается новый подход к решению указанной выше проблемы. Основным отличительным моментом этой работы от работы [2] состоит в том, что здесь для анализа системы используется подход, основанный на теории фазового укрупнения состояний двумерных цепей Маркова [1]. С использованием этого подхода разработаны простые вычислительные процедуры для нахождения всех характеристик изучаемой системы. Важным достоинством предложенного подхода состоит в том, что он может быть использован для моделей любой размерности, так как искомые характеристики вычисляются с помощью явных формул.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Ponomarenko L., Kim C.S., Melikov A.* Performance analysis and optimization of multi-traffic on communication networks. Springer, 2010. 208 p.
2. *Меликов А.З., Фаталиева М.Р.* Управление запасами систем обслуживания разнотипных встречных потоков с учетом текущей ситуации // Электронное моделирование. 1997. Т.14. №6.

УДК 004.056.5(083.73)(043.2)

В.В. Вербіцька;
В.М. Боровик, к.т.н.
(Національний авіаційний університет, Україна)

ПЕРЕВАГИ ТА НЕДОЛІКИ КРИПТОГРАФІЧНОГО МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

На сьогодні комп'ютерні системи активно впроваджуються у фінансові, промислові, торгові та соціальні сфери. Внаслідок цього різко зріс інтерес широкого кола користувачів до проблем захисту інформації. В останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації.

Метою даної роботи є знаходження переваг та недоліківкриптографічних засобів захисту інформації. Для цього розглянуто два алгоритми шифрування: DES та RSA.

Алгоритм DES (DataEncryption Standard) має наступні переваги: високий рівень захисту даних проти дешифрування і можливої модифікації даних, простота і розуміння, високий ступінь складності, засіб захисту грунтується на ключі і не залежить ні від якої "таємності" алгоритму, економічний у реалізації та ефективний у швидкодії.

Найістотнішим недоліком DES фахівці визнають розмір ключа, що вважається занадто малим.

Для дешифрування інформації засобом підбору ключів достатньо виконати 2^{56} операцій розшифрування, та в наш час немає апаратури, що могла б виконати цю операцію.

Ще один недолік DES полягає в тому, що окремі блоки, що містять однакові дані (наприклад, пропуски), матимуть однаковий вигляд у зашифрованому тексті, що з погляду криптоаналізу є невірним.

Залежно від швидкодії та типу процесора персонального комп'ютера програмна система, що шифрує дані з використанням засобу DES, може обробляти від декількох кілобайт до десятків кілобайт даних у секунду.

Алгоритм RSA є дуже перспективним, оскільки для зашифровування інформації не вимагається передачі ключа іншим користувачам, але очікуєтьсяі більш ефективний алгоритм визначення дільників цілих чисел, в результаті чого засіб шифрування стане абсолютно незахищеним.

До числа переваг RSAслід такожвіднести дуже високу криптостійкість, досить просту програмну і апаратну реалізації. Щоправда, слід відзначити, що використання цього засобу для криптографічного захисту даних нерозривно пов'язане з дуже високим рівнем розвитку техніки.

Отже, криптографічний метод захисту інформації на підприємстві є досить надійним і ефективним на сьогоднішній день. Криптографія забезпечує підзвітність, прозорість, точність і конфіденційність, запобігає спробам шахрайства в електронній комерції.

УДК 351.814.331:519.711.3

С.В. Водопьянов
(Національний авіаційний університет, Україна)

СТАБИЛИЗАЦИЯ ПРОЦЕССА ВЫБОРА ОПТИМАЛЬНОЙ ТОПОЛОГИИ СЕТИ МЕТОДОМ АНАЛИЗА ИЕРАРХИЙ

В перспективных корпоративных сетях систем УВД должна обеспечиваться поддержка всего спектра услуг, как на уровне транспортных сетей, так и на уровне сетей доступа для терминалов, находящихся в распоряжении оператора в настоящее время – обычных, мобильных или IP-телефонов, внутренних сетей громкоговорящей связи, персональных компьютеров. Кроме того, по заявкам клиентов необходимо быстро и без остановки работы системы заказчика (в нашем случае – системы УВД) организовывать и/или модифицировать индивидуальные наборы услуг, в том числе и дополнительные виды обслуживания.

Вследствие многофункциональности систем ОВД возникает проблема многокритериальности оценки её эффективности. Для систематизации критериев, выбора иерархии приоритетов целесообразно применять методы скаляризации вектора показателей, в частности, метод анализ иерархий Саати [1], как наиболее простой и универсальный. При этом устойчивость решения оптимизационной задачи обеспечивается наличием случайных составляющих в матрице приоритетов. Эти составляющие имеют самую различную природу (ошибки экспертов и произвол в выборе относительной важности показателей, ошибки формирования матрицы приоритетов и пр.). Они играют роль стабилизаторов решения задачи выбора иерархий, которая относится к задачам на собственные значения матрицы. В табл. 1 приведены для примера элементы матрицы парных сравнений для критериев, по которым определяется наиболее важный критерий.

Таблица 1

Номер параметра a_i	I	II	III	IV	Wi	Xi
I	1	3	5	1/3	1,495	0,306
II	1/3	1	1/3	1/3	0,439	0,090
III	1/5	3	1	1/3	0,669	0,137
IV	3	3	3	1	2,280	0,467
сумма (Yj)	4,533	10,000	9,333	2,000	4,882	1
$(L_{max})_i$	1,388	0,899	1,278	0,934		

Здесь $W_i=a_i/(a_1+ a_2+...+ a_n)$ – веса, которыми определяется относительная важность параметра, а $X_i=(i*a_{i2}*...*a_{in})*(1/n)$ – оценки компонентов вектора собственных значений.

Для обеспечения устойчивости решений предлагается вводить в значения величин парных сравнений малые возмущения случайного характера. При этом матрица парных сравнений перестает быть строго обратно-симметричной и, соответственно, ее определитель становится не равным нулю.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Саати Т.* Принятие решений. Метод анализа иерархий: Пер. с англ. – М.: Радио и связь, 1993. – 320 с.

УДК 621.396

С.В. Волошко, Ю.О. Омельченко, А.В. Петренко, О.І. Шевельова
(ПолтНТУ ім. Ю. Кондратюка, Україна)

РЕАЛІЗАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ ЦИФРОВОЇ ОБРОБКИ СИГНАЛІВ У ЗАСОБАХ РАДІОЗВ'ЯЗКУ

Бездротові системи зв'язку знаходять сьогодні все більше застосування в різних галузях діяльності людини. Успіхи сучасної радіоелектроніки, стрімкий розвиток мікропроцесорної техніки та нові алгоритми цифрової обробки сигналів разом з використанням перспективних телекомунікаційних технологій відкривають нові можливості щодо створення бездротових систем зв'язку з виконанням жорстких вимог щодо високої пропускної спроможності і завадозахищеності.

Серед перспективних телекомунікаційних технологій слід відзначити методи модуляції цифрових сигналів OFDM (N-OFDM) (ортогональна і неортогональна частотні дискретні модуляції), технології просторово-часової і просторово-поляризаційної обробки сигналів, а також MIMO (множинний вхід - множинний вихід) на базі цифрових антенних решіток. Переваги і недоліки застосування зазначених технологій, а також можливості їх спільного використання достатньо відомі.

Розвиток елементної бази робить можливим використання цих технологій як у малопотужних переносних пристроях, так і в станціях радіо, радіорелейного і тропосферного зв'язку. Крім того, сучасні досягнення процесорної техніки дозволяють створювати уніфіковані комплекси засобів зв'язку з можливістю програмної реконфігурації обладнання, тому питання реалізації в цьому аспекті заслуговують уваги.

У доповіді розглядаються особливості практичної реалізації зазначених вище технологій в засобах радіозв'язку. Для вибору основи необхідних схемотехнічних рішень авторами сформульовано вимоги до створюваної апаратури, а також враховані такі фактори, як: наявність готового системного і прикладного програмного забезпечення; можливість швидкої підготовки до серійного виробництва; наявність кваліфікованих розробників; відкритість архітектури.

Широке застосування в системах цифрової обробки сигналів отримав новий модульний стандарт VITA 46 з базовою специфікацією VPX. Для створення систем з середнім рівнем фінансування розробок доцільно використовувати процесорні модулі VPX6-185 американської компанії Кетіс-Райт. Слід звернути увагу на процесорні модулі PX6030, а також PX3010 канадської компанії Дженерал Динамікс. Запропонований схемотехнічний підхід дозволяє створити базовий модуль цифрової обробки сигналів, на основі якого можна здійснити як модернізацію існуючих засобів радіозв'язку, так і створення нових. Структура такого модуля не залежить від діапазону робочих частот і є економічно ефективною для різних технічних рішень та методів цифрової обробки сигналів.

УДК 004.056.5 (043.2)

Л. П. Галата, Б.Я. Корнієнко
(Національний авіаційний університет, Україна)

БЕЗПЕКА ФАЙЛОВОЇ СИСТЕМИ WINDOWS SERVER 2012

Восени 2012 року вийшла публічна бета-версія Microsoft Windows Server 2012 з підтримкою анонсованої файлової системи ReFS (*Resilient File System - відмовостійка файлова система*), раніше відомої під кодовою назвою «Protogon».

Архітектура файлової системи. Основними структурними елементами нової файлової системи є «B+-дерева». Файл в ReFS не є окремим ключовим елементом «каталогу», а лише існує у вигляді запису. Для папки існують три основних типи записів: дескриптор каталогу, індексний запис і дескриптор вкладеного об'єкта. Розмір метаданих порожньої файлової системи становить близько 0.1% від розміру самої файлової системи. Деякі основні метадані дублюються для кращої стійкості від збоїв.

Захищеність від збоїв. Частина структур метаданих містить власні ідентифікатори, що дозволяє перевірити приналежність структури; посилання на метадані містять 64-біт контрольні суми блоків, що дозволяє оцінити цілісність прочитаного по посиланню блоку. Зміна структури метаданих здійснюється на основі стратегії «Copy-on-Write (копіювання-при-записі)» та дозволяє обійтися без аудиту, зберігаючи автоматично цілісність даних.

Відмовостійкість диска. Всі метадані ReFS перевіряються по контрольних сумах на рівні сторінки дерева «B+», а самі контрольні суми зберігаються окремо від сторінки. Це дозволяє виявити всі форми ушкоджень диска, включаючи втрачені або збережені не в тому місці записи та бітовий розпад (погіршення стану даних на носії). Оновлення контрольних сум відбувається автоматично при записі даних, тому якщо під час запису відбувається збій даних, завжди буде системно-доступна версія файлу.

Стратегія надійного оновлення диска. Для забезпечення узгодженості на диску, NTFS спирається на журнал транзакцій. Цей підхід оновлює метадані на диску та використовує журнал на стороні, щоб враховувати зміни, які можна відкотити в разі помилок або збою. Транзакції будуються на основі підходу «розміщення при записі». Так як верхній рівень ReFS успадкований від NTFS, нова модель транзакцій використовує вже існуючу логічну схему відновлення після помилок, яка була перевірена та стабілізована у багатьох випусках.

Цілісні потоки захищають вміст файлу від усіх видів пошкоджень даних. Система може легко використовувати шифрування BitLocker, списки контролю доступу для безпеки, журнал USN, повідомлення про зміни, символьні посилання, точки з'єднання, точки підключення, точки повторної обробки, знімки томів, файлові ідентифікатори та нежорсткі блоки.

Отже, з розгляду нової файлової системи ОС Windows Server 2012, можна спостерігати початок орієнтованості на серверний сегмент, на системи віртуалізації, взаємодії із СУБД, сервера архівації, у яких швидкість та надійність роботи є головними.

УДК 004.78 (043.2)

А.А. Говтвяниця
(Національний авіаційний університет, Україна)

АНАЛІЗ ПЛАТФОРМИ VUFORIA ДЛЯ СТВОРЕННЯ ЕЛЕМЕНТІВ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Технологія доповненої реальності дозволяє додати до бачення наступний рівень, шар, на якому буде знаходитися інша, додаткова інформація. Завдяки цій технології у людей є можливість оцінити об'єкти більш детально, побачити потрібні функції і якість, побачити більш наочно представлену їм інформацію. Технологія додаткової реальності заснована на алгоритмі розпізнавання зображення та системі спеціальних маркерів-датчиків, аналізуючи вид яких, програма демонструє ту або іншу інформацію.

Сьогодні вона особливо користується попитом в туристичному та рекламному бізнесі. Доповнена реальність швидкими темпами наздоганяє технологію віртуальних середовищ.

Однією з більш відомою компанією з розробки інструментів побудови додатків додаткової реальності є компанія Qualcomm, їх технологія має назву Vuforia.

Vuforia отримує відео-потік з камери пристрою, після цього система аналізує кадр на присутність маркеру і забезпечує відображення просторової інформації за допомогою спеціалізованого API. В результаті, віртуальні об’єкти зливаються в реальні кадри в режимі реального часу. Система має зручний сервіс управління сховищем маркерів, має змогу загружати їх у режимі он-лайн.

Основною задачею роботи було дослідження даної системи, її функцій та методів, ознайомлення з системою розпізнавання міток та їх зберігання.

На основі розглянутого було створено інтерактивний мобільний додаток інформаційної системи Національного авіаційного університету та власний генератор унікальних міток-маркерів. Додаток встановлюється на мобільний пристрій користувача, а точкою доступу до інформації являються мітки, що створюються генератором. Направляючи камеру мобільного пристрою на мітку, користувач отримує призначену для перегляду інформацію. Використання такого додатку ефективно впливає на економію ресурсів як і людських так і матеріальних - замість використання великої кількості паперу для представлення деякої інформації або оголошень використовується лише пристрій користувача.

УДК 004.65+004.7(043.2)

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

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ СИСТЕМИ УПРАВЛІНСЬКОГО ОБЛІКУ

Велика частина інформації, на підставі якої щодня приймаються рішення, з'являється неформальним шляхом.

Кількість інформації, що з'являється в результаті діяльності організації і має вплив на успіх ведення справ, а також швидкість, з якої ця інформація змінюється, робить необхідним для керівництва застосування формальних методів збору і обробки інформації.

Корпоративна система управлінського обліку визначається як формальна система для видачі адміністрації інформації, необхідної для прийняття управлінських рішень.

Загальною метою корпоративної системи управлінського обліку є полегшення ефективного виконання функцій планування, контролю діяльності з надання послуг та процесу управління в цілому. Найважливішим її завданням є видача потрібної інформації потрібним людям в потрібний час, а також розрахунок показників ефективності роботи компанії.

Запровадження корпоративної системи управлінського обліку підприємства варто здійснювати поступово, починаючи з найбільш важливої ланки: побудови сховища даних, що дозволить швидко одержати позитивний ефект у вигляді більшої керованості компанією. У процесі впровадження системи управлінського обліку необхідно забезпечити можливість роботи як за новою, так і за старою технологією, щоб не заважати повсякденній діяльності підприємства. Цьому сприяє підтримка сучасним мережевим обладнанням попередніх технологій.

Для підвищення ефективності функціонування важливим етапом розвитку системи управлінського обліку є підключення до корпоративної мережі віддалених філій компанії. Це дозволить обмін інформацією в режимі реального часу, а також потрапляння інформації від філій в сховище даних без викривлень та втрат, що можливі при пересиланні даних електронною поштою.

Впровадження в корпоративну мережу мультимедійних технологій *Unified Communications* можна здійснювати поступово. Для цього потрібно підготувати мережу та приймально-передавальне обладнання, що забезпечить швидку передачу даних великого обсягу. До того ж, дане обладнання має досить високу вартість, і впровадження доцільно розпочати з одного підрозділу, оцінити ефективність, та з відповідними коригуваннями розповсюдити на всю компанію. У ході впровадження обов'язково потрібно організувати тренінги та консультації для співробітників підприємства з організації переходу на більш сучасні форми обміну інформацією [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принипы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010.- 944 с.

УДК 004.7.052

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

ТЕХНОЛОГІЇ ОПТИМАЛЬНОГО УПРАВЛІННЯ ГАРАНТОЗДАТНОЮ КОМП'ЮТЕРНОЮ МЕРЕЖЕЮ

Проблема оптимального управління гарантоздатними комп'ютерними мережами домінує в сучасній теорії і практиці розробки та експлуатації комп'ютерних систем. Управління комп'ютерною мережею передбачає виконання функцій контролю, планування та моніторингу ресурсів комп'ютерної мережі, управління маршрутизацією, продуктивністю та балансуванням навантаження, відмовостійкістю, безпекою інформаційних ресурсів, розподілом криптографічних ключів. Задачі управління особливо актуальні для великомасштабних комп'ютерних мереж та телекомунікаційних систем.

Важливим напрямом досліджень є створення гарантоздатних комп'ютерних мереж (ГКМ) для систем критичного призначення (системи управління АЕС, аерокосмічні системи та ін.), зокрема забезпечення основних показників гарантоздатності – надійності та захищеності мереж. Для забезпечення надійності ГКМ одним з ефективних є підхід, заснований на введенні фрактальної надлишковості. Захищеність ГКМ потребує розробки систем виявлення аномалій трафіку та виявлення вторгнень в мережу. Сучасні системи виявлення атак засновані переважно на пошуку відповідних сигнатур атак. В дослідженні аналізуються нові підходи до ідентифікації аномалій трафіку в системах попередження вторгнень на базі інтелектуальних технологій. Запропонована структурна схема IDS та алгоритми виявлення вторгнень. Забезпечення заданої якості обслуговування трафіку в рамках класичної парадигми вимагає розробки математичних моделей, що враховують зміну активності мережних користувачів, динамічну маршрутизацію та зміну параметрів мережного керування трафіком і розроблення на їх основі системи керування комп'ютерною мережею в умовах зовнішніх збурень та невизначеності параметрів мережі. В роботі запропоновані рандомізовані моделі оптимального управління трафіком ГКМ та забезпечення QoS. Запропоновані підходи в значній мірі вирішують поставлені задачі. Результати досліджень можуть бути використані в суміжних галузях – мережних інформаційних технологіях, телекомунікаційних системах, системах захисту інформації в комп'ютерних мережах, високопродуктивних розподілених обчислювальних середовищах.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Ігнатов В.О., Гузій М.М. Динаміка інформаційних конфліктів в інтелектуальних системах Проблеми інформатизації та управління: Збірник наукових праць. Випуск 4(15).-К.: НАУ, 2005. С.88-92

2. Гузій М. М., Даниліна Г. В., Ігнатов В. О., Милокум Я. В. Методи і алгоритми оптимального управління трафіком в обчислювальних мережах Проблеми інформатизації та управління. –К.: НАУ, 2006. - Вип. 17 - с. 32-37

УДК 004.048

Х.Н. Гулиева
(НАА, Азербайджан)

СОВРЕМЕННЫЙ ПОДХОД К РАЗРАБОТКЕ ОБУЧАЮЩИХ СИСТЕМ АВИАТРЕНАЖОРОВ

На современном этапе подготовка специалистов в области авиации неизбежно сталкивается с использованием авиатренажеров. Именно поэтому в настоящем докладе исходя из анализа литературных источников определены направления и проблемы в области подготовки авиаспециалистов с учетом новых информационных технологий.

В докладе освящены вопросы использования авиатренажеров и их возможности в свете современных информационных технологий.

Бурный рост вычислительных мощностей компьютеров позволил довести современные авиационные тренажеры до такого уровня развития, что подготовка пилотов на тренажерах стала более эффективной, чем подготовка на реальном воздушном судне.

Такая эффективность авиационных тренажеров обусловлена их возможностями к обеспечению высокой интенсивности подготовки. Так, если в реальном полете экипаж вынужден уделять значительное время выполнению рутинных операций, не связанных с выполнением конкретных задач обучения,то на тренажере специальное программное обеспечение позволяет мгновенно менять условия полета, погоду, географическое положение, останавливать выполнение задания для разбора и повтора и т. д.

Анализ литературных источников показывает, что возможен агентно-ориентированный подход к разработке обучающих систем авиатренажеров.

Агентно-ориентированный подход (АОП) является частным случаем объектно-ориентированного программирования (ООП). В ООП вычислительный процесс понимается достаточно широко как система, собранная из объектов, которые взаимодействуют друг с другом через сообщения. АОП специализирует эти понятия, устанавливая состояние объектов, состоящих из компонентов, таких как верование (убеждения), способности, и решения, каждое из которых обладает определенный синтаксисом. Кроме того различные ограничения помещены в психическое состояние агента. Вычисление состоит из информирования агентов, выполнения их требований, выполняя их предложения, принимая, отклоняя, конкурируя, и помогая друг другу.

В докладе указаны подлежащие исследованию вопросы и указаны пути решения поставленных задач. Отметим, что в разрабатываемой обучающей системе вопрос планирования движения интеллектуальных агентов является одним из ключевых. Здесь также с помощью мультиагентных систем проводится анализ процесса коллективного обучения.

Мультиагентные системы созданы для решения различных задач искусственного интеллекта, в которых присутствует несколько участников. Основным понятием является агент.

Кроме этого рассмотрены требования к планирующимся движущимся интеллектуальным агентам обучающих систем и решен вопрос построения обучающей системы для моделирования движения интеллектуальных агентов.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Серёгин Г. Н.* Авиационные тренажеры — реальный путь к повышению безопасности полётов // "Право и безопасность" : Журнал. - 2006. — № 3-4 (20-21).
2. *Shoham Yoav*. Agent-oriented programming (англ.) // Artificial Intelligence. — 1993. — № 60(1). — С. 51-92.

УДК 004.738

А.И. Гуля; С.Б. Литовка; Д.Б. Бурьянцев
(Национальный авиационный университет, Украина)

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ – БУДУЩЕЕ РАСПРЕДЕЛЛЕННОЙ ОБРАБОТКИ ДАННЫХ

Впервые идея того, что мы сегодня называем облачными вычислениями (ОВ) была озвучена J.C.R. Licklider, в 1970 году. Его идея заключалась в том, что каждый человек в мире будет подключен к компьютерной сети, из которой он будет получать не только данные, но и программы. Другой ученый John McCarthy высказал идею о том, что вычислительные мощности будут предоставляться пользователям как услуга. Развитию облачных технологий способствовал ряд факторов:

1. Расширение пропускной способности Интернетав 90-е годы не позволило получить значительного скачка в развитии в облачной технологии, так как практически ни компании, ни технологии того времени не были готовы к этому. Однако сам факт ускорения Интернета придал ускорение развитию ОВ.

2. Одним из наиболее значимых событий в данной области было появление Salesforce.com в 1999 году. Данная компания стала первой которая предоставила сетевой доступ к своему приложению. По сути, стала первой компанией предоставившей свое программное обеспечение по принципу – программное обеспечение как сервис (SaaS).

3. Следующим шагом стала разработка облачного веб-сервиса компанией Amazon в 2002 году. Данный сервис позволял хранить, информацию и производить вычисления.

4. Другая веха в развитие облачных вычислений произошла после создания компанией Google платформы GoogleApps для веб-приложений в бизнес секторе.

По оценкам экспертов потенциал ОВ очень высок.Соответственно, можно достичь успехов на рынке средств облачных вычислений, работая в следующих направлениях:

1. Предоставление услуг ОВ – данная возможность доступна не многим компаниям, поскольку нужны значительные вложения в построение и разработку центра обработки данных(ЦОД).

2. Разработка ПО для построения виртуальной инфраструктуры - не следует забывать и про тех кто будет внедрять и настраивать это ПО, т. е. потребуются специалисты в этой области.

3. Аутсорсинг, администрирование облаков – потребуются специалисты по администрированию и консультированию в сфере облачных вычислений.

4. Аппаратное обеспечение – появятся компании занимающиеся разработкой и проектированием аппаратного обеспечения для создания «облаков».

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Романченко В.* Облачные вычисления на каждый день – 3DNews2009
2. *Крупин А.* Cloud Computing: высокая облачность – Компьютерра 2009

УДК 621.396.2: 621.396.931

А.Е. Деревянных
(Национальный авиационный университет, Украина)

МЕТОД МНОГОУРОВНЕВОГО РАДИОПЛАНИРОВАНИЯ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ НОВЫХ ПОКОЛЕНИЙ

Задачи радиопланирования сетей связи с подвижными объектами (транкинговых, сотовых) являются весьма сложными и неоднозначными. Для них невозможно разработать некий универсальный метод расчета, поскольку существует слишком много внешних и внутренних факторов влияния, которые приводят к значительным отклонениям решения. В работе [1] отмечается, что одним из основных факторов является невозможность построения регулярных моделей распространения электромагнитных волн в широком диапазоне частот, на которых работают сети мобильной связи разных поколений.

В пределах большого города сеть имеет иерархическую структуру, когда соты небольшого размера (микро- или пикосоты) дополнительно развертываются внутри сот большего размера.

Задача оптимального размещения базовых станций (БС) на территории покрытия относится к классу задач комбинаторной оптимизации, в частности, к так называемым задачам размещения. Задачи комбинаторной оптимизации как задачи перебора вариантов являются крайне ресурсоемкими.

Для снижения размерности задачи предлагается использовать метод многоуровневой (иерархической) оптимизации размещения БС. На высшем уровне – уровне развертывания сети – решаются следующие задачи.

1. Проводится анализ всей зоны покрытия с использованием цифровых карт местности. Оценивается вид рельефа и тип ландшафта – природный, сельский, городской малоэтажный, городской многоэтажный.

2. Выполняются расчеты корреляционных функций высот поверхности и предварительные оценки вклада дифракционных составляющих.

3. Проводятся тест-драйвы и точечные замеры. Сравниваются результаты расчетов и измерений.

4. В первом приближении решается задача размещения БС в зоне покрытия.

Средний уровень – уровень макросоты. Решается задача оптимизации размещения БС в предварительно выбранных ячейках с учетом ограничений технического и организационного характера.

Нижний уровень – микросоты радиусом от 100 до 500 м, организуемые, как правило, в местах с интенсивным телефонным обменом; пикосоты размером от 10 до 100 м для связи в помещениях. Решаются задачи статистической электродинамики: оцениваются затухания при проникновении электромагнитных волн через капитальные стены, внутренние перекрытия, потолки и пр., рассчитываются плотности потока мощности при волноводном распространении вдоль длинных коридоров, в том числе с угловыми ответвлениями и т.д.

Благодаря такому разделению общей задачи радиопланирования размерностью $N_{\text{общ}}$ на частные задачи с размерностями n_1, n_2, n_3, где $n_1 + n_2 + n_3 = N_{\text{общ}}$, следует ожидать асимптотического уменьшения общей размерности в соотношении $\left(\ln n_1 \cdot \ln n_2 \cdot \ln n_3\right) \big/ N_{\text{общ}}$.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Деревянных А.Е. Комбинированный метод радиопланирования сетей 3G // Наукові записки УНДІЗ, №3(19), 2011. – С. 19–27.

УДК 004.048

Т.И. Джафар-заде, к.т.н.
(НАА, Азербайджан)

АНАЛИЗ СИСТЕМЫ ОБСЛУЖИВАНИЯ С ЗАВИСЯЩИМИ ОТ ВРЕМЕНИ ОЖИДАНИЯ СКАЧКООБРАЗНЫМИ ПРИОРИТЕТАМИ

В последнее годы интенсивно исследуются модели систем обслуживания со скачкообразными приоритетами [1], [2]. В работе [3] рассмотрен класс скачкообразных приоритетов в системе с непрерывным временем и общей ограниченной очередью для разнотипных вызовов. Согласно исследованной схемы приоритетов, при освобождении канала, независимо от числа низкоприоритетных пакетов, всегда для обслуживания из очереди выбираются высокоприоритетные пакеты. Ясно, что в этом случае время ожидания низкоприоритетных пакетов на буфере может расти бесконечно. Для того, чтобы устранить отмеченное нежелательное явление целесообразно использовать правило обслуживания, основанного на схеме случайного выбора пакетов из буфера. Исходя из сказанного, в настоящей работе исследована модель одноканальной системы с ограниченными буферами, обслуживающая запросы двух типов. Здесь скачок из одной очереди в другую реализуется в зависимости от времени ожидания низкоприоритетного запроса в очереди. Отличительной особенностью выполненной нами работы является то, что если в момент освобождения канала в очереди имеются разнотипные пакеты (альтернативная ситуация), то для обслуживания с вероятностью α принимается высокоприоритетный пакет, а с вероятностью $1-\alpha$, $0 \le \alpha \le 1$ – низкоприоритетный пакет. При этом при различных значениях параметра α получаются некоторые известные ранее правилы обслуживания. Преимущество анализируемой нами модели заключается в уменьшении “старения” пакетов второго типа в буфере, что, в свою очередь, влияет на показатели качество обслуживания разнотипных вызовов. Основными показателями качество обслуживания являются время ожидания в очереди и вероятности потери разнотипных вызовов.

В работе разработаны точный и приближенный методы решения поставленной задачи и предложены соответствующие алгоритмы. Приводятся результаты численных экспериментов и дан их анализ.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Maertens T., Walraevens J., Bruneel H. A modified HOL priority scheduling discipline: performance analysis // European Journal of Operational Research. 2007. Vol.180, no.3. P. 1168–1185.
2. Меликов А.З., Нагиев Ф.Н., Фейзиев В.Ш. Алгоритмический подход к анализу модели обслуживания со скачкообразными приоритетами // Электронное моделирование. 2012. Том 34, № 3. С. 69-79.
3. Меликов А.З., Джафар-заде Т.И. Анализ модели двух потоковой системы с общей очередью и скачкообразными приоритетами // Проблеми інформатизації та управління. 2012. Том 3, № 39. С. 89-94.

УДК 004.896 (043.2)

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

ОБЧИСЛЮВАЛЬНА ПЛАТФОРМА ARDUINO — ШЛЯХИ ПРОГРАМНОЇ ОПТИМІЗАЦІЇ

Мета моєї роботи полягає в дослідженні шляхів підвищення продуктивності роботи платформи Arduino для подальшого використання на практиці.

Будь-який готовий варіант є своєрідною основою, базою для створення власного продукту. В більшості випадків обчислювальних потужностей платформи вистачає для потреб проекту, проте досить часто виникає необхідність підвищити потужності для задоволення потреб цього проекту або поліпшення робочих характеристик кінцевого продукту.

Напрям автоматизації підтримується відомими компаніями, які пропонують готові платформи як для невеликих аматорських так і для серйозних комерційних проектів. В цій статті якраз мовиться про одну з таких платформ, а саме — Arduino.

Для дослідження швидкості роботи та створення порівняльних таблиць, був проведений ряд експериментів, суть яких полягає в виконанні елементарних дій мікроконтролером, а саме в подачі високого та низького логічного рівня на один з його портів за допомогою стандартних бібліотек і за допомогою прямого звернення до регістрів портів вводу виводу, а також проведенні заміру часу операції. В першому експерименті ми отримали трапецевидний сигнал з періодом в 7.6 мікросекунди, при прямому звертанні до регістрів вводу виводу вдалося отримати сигнал з періодом в 0.82 мікросекунди, а використання компілятору середовища “AVR Studio” зменшило період вихідного сигналу до 0.23, що рівне сигналам з частотою близько 131.58 КГц, 1.2 МГц та 4.35МГц відповідно. Розмір скомпільованого коду також помітно відрізняється: 680 байт (експеримент №1), 342 байт (експеримент №2) та 222 байти (експеримент №3).

Оптимізація роботи апаратної обчислювальної платформи Arduino можлива завдяки більш раціональному використанню процесорного часу мікроконтролера, що досягається шляхом прямого звернення до регістрів, як портів вводу виводу так і регістрів загального призначення. Таким самим чином можна переписати і інші функції стандартних бібліотек Arduino (наприклад функції цифрового та аналогового зчитування сигналів, Широтно-імпульсної модуляції тощо).

УДК 004.7

А.Г. Додонов, д.т.н.; Д.В. Ландэ, д.т.н.
(Институт проблем регистрации информации НАН Украины)

АНАЛИЗ ТРЕНДОВ ИНФОРМАЦИОННЫХ ПОТОКОВ ПРИ ВЫЯВЛЕНИИ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ

Веб-пространство представляет собой динамическую систему из связанных по смыслу элементов (документов), образующих в динамике своей эволюции информационные потоки [1, 2]. Динамика подобных систем описывается временными рядами. Как известно «тренд» (от англ. Trend) – это общая тенденция изменений исследуемого временного ряда.

Целью настоящей работы является определение типичных трендов динамики публикаций в информационном пространстве, соответствующих информационным операциям, определяемым как «акции, направленные на воздействие на информацию и информационные системы противника и защиту собственной информации и информационных систем» [3, 4].

Основным объектом моделирования информационных потоков [5] являются тематические потоки новостей, последовательности документов, соответствующих определенной тематике. Этим потокам ставятся в соответствие временные ряды, для решения задач анализа которых все чаще применяются дисперсионный, фрактальный и вейвлет-анализ [6, 7].

Получить данные динамики тематических информационных потоков можно, например, ежедневно посещая сайты интеграторов новостей (news.yandex.ru, webground.su, uaport.net).

В настоящее время существует несколько открытых информационных сервисов, в рамках которых можно наблюдать временную динамику объемов публикаций по тематикам, определяемым запросами. Так Google Books Ngram Viewer (http://ngrams.googlelabs.com/), предоставляет визуализацию динамики количества книг, в которых упоминаются слова из запроса.

Сервис «Яндекс пульс блогосферы» (http://blogs.yandex.ru/pulse/) также позволяет отображать динамику публикаций в блогах, содержащих заданные пользователем ключевые слова.

На сайте Национального корпуса русского языка (НКРЯ) в бета-режиме запущен сервис *N*-грамм (http://www.ruscorpora.ru/ngram.html), близкий по функциональности сервису Google Books Ngram Viewer.

Многие современные информационно-аналитические системы содержат в своем составе средства отображения статистики вхождения в базы данных понятий, соответствующих пользовательским запросам. В частности, авторами использовалась подсистема статистики в рамках системы контент-мониторинга веб-пространства InfoStream [8], реализующая данную функциональность.

Приведенные в [4] тренды сообщений, соответствующих этапам информационной операции приведены на рис. 1. При этом аналитикам можно следует ориентироваться на такие модели, например, если мониторинг позволяет определить фазы: «фон» – «затишье» – «артподготовка» – «затишье» – «атака», то уже по первым трем компонентам можно с большой вероятностью предсказать будущие события.

Следует отметить, что подобная динамика количества тематических сообщений при проведении информационных операций хорошо описывается известным уравнением:

$$y = A + Bx\sin(x),$$

где x – время, A и B – константы, определяемые эмпирически.

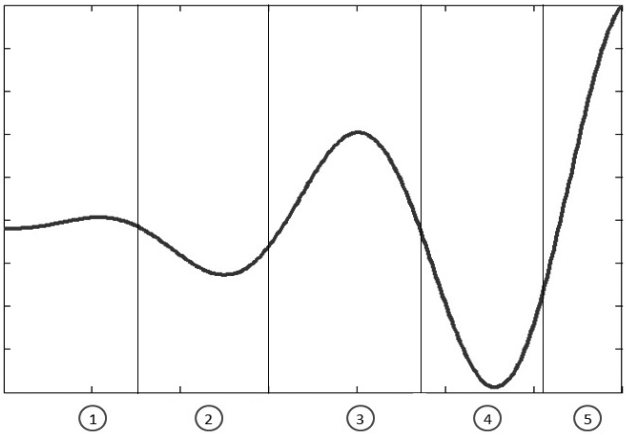


Рис. 1. Динамика количества тематических сообщений во время проведения информационной операции: 1 – фон; 2 – затишье; 3 – «артподготовка»; 4 – затишье; 5 – атака/триггер роста

Как известно, в настоящее время инновационная деятельность также косвенно измеряется количеством публикаций, относящимся к инновациям, существует несколько моделей инновационных процессов, среди которых можно выделить модель диффузии инноваций. Вместе с тем, внедрение инноваций также можно считать информационными операциями. Поэтому обратимся к результатам соответствующих исследований. На рис. 2 приведена обоснованная в [9] диаграмма количества публикаций, соответствующая тренду инновационной деятельности.

Объединяя графики, соответствующие началу информационной операции и тренду инновационной деятельности, можно получить полный график, соответствующий отображению информационных операций в информационном пространстве (рис. 3).

Предложенные модели полностью соответствуют реальным данным, которые экстрагируются системами контент-мониторинга [10]. Поэтому приведенные зависимости могут быть использованы как шаблоны для выявления информационных операций, как путем анализа ретроспективного фонда сетевых публикаций, так и для оперативного мониторинга появления некоторых их признаков в реальном времени.

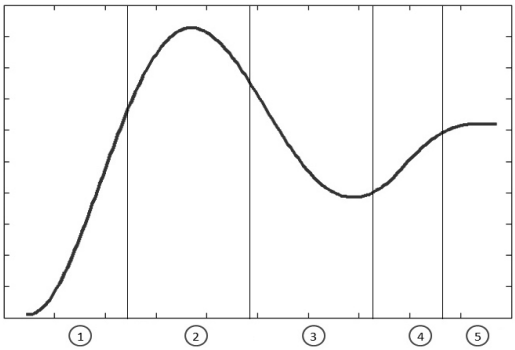


Рис. 2. Диаграмма количества публикаций, соответствующих тренду инновационной деятельности: 1 – атака/триггер роста; 2 – пик завышенных ожиданий; 3 – утрата иллюзий; 4 – общественное осознание; 5 – продуктивность/фон

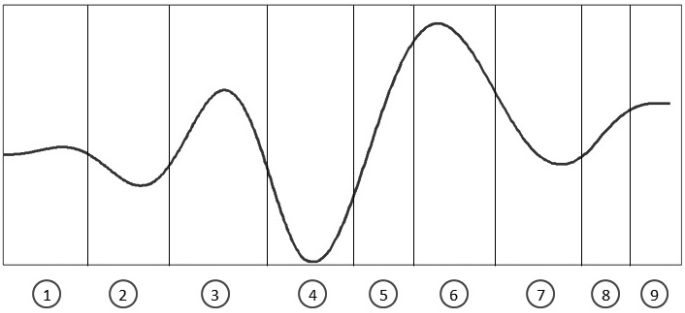


Рис. 3. Обобщенная диаграмма количества публикаций, соответствующая всем этапам жизненного цикла информационных операций: 1 – фон; 2 – затишье; 3 – «артподготовка»; 4 – затишье; 5 – атака/триггер роста; 6 – пик завышенных ожиданий; 7 – утрата иллюзий; 8 – общественное осознание; 9 – продуктивность/фон

Как известно, для выявления информационных операций следует внимательно следить за динамикой публикаций по целевой теме и, если есть возможность, пользоваться доступными аналитическими средствами, средствами цифровой обработки данных и распознавания образов, например, вейвлет-анализом или полиномами Кунченко [11].

Приведенные модели и методы пригодны для описания общих тенденций динамики информационных процессов, однако, проблема прогнозирования остается открытой. По-видимому, реалистичные модели могут быть получены с учетом дополнительного набора факторов, большинство которых не воспроизводятся во времени. Вместе с тем, структура правил, лежащих в основе функционирования большинства из доступных моделей, позволяет вносить соответствующие коррективы, например, искусственно моделировать случайные

отклонения. Отметим, что воспроизведение результатов во времени является серьезной проблемой при моделировании информационных процессов, составляет основу научной методологии. В настоящее время только ретроспективный анализ уже реализованных информационных операций остается относительно надежным способом их верификации.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Kleinberg J. Temporal dynamics of on-line information streams // Data Stream Management: Processing High-Speed Data Streams. – Springer, 2006.
2. Lande D., Braichevski S, Busch D. Informationsfluesse im Internet // IWP - Information Wissenschaft & Praxis, 59(2007), Heft 5. – S. 277-284.
3. Information operations roadmap. – DoD US. – Washington, D.C.: GPO, 2003. – 78 p.
4. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. - К.: Інтертехнологія, 2009. - 164 с.
5. Ландэ Д.В., Снарский А.А., Брайчевский С.М., Дармохвал А.Т. Моделирование динамики новостных текстовых потоков // Интернет-математика 2007: Сборник работ участников конкурса. – Екатеринбург: Изд-во Урал. ун-та, 2007. – С. 98-107.
6. Астафьева Н.М. Вейвлет-анализ: основы теории и примеры применения // Успехи физических наук, 1996. – 166. – № 11. – P. 1145-1170 (http://www.isuct.ru/~artcol/ articles/ Uspekhi_Fiz_Nauk/wavelet-analys.pdf).
7. Lande D.V., Snarskii A.A. Diagram of measurement series elements deviation from local linear approximations // Preprint Arxiv: 0903.3328, 2009.
8. Григорьев А.Н., Ландэ Д.В. и др. Мониторинг новостей из Интернет: технология, система, сервис: научно-методическое пособие. – К.: ООО «Старт-98», 2007. – 40 с.
9. Хорошевский В.Ф. Семантические технологии: ожидания и тренды // Открытые семантические технологии проектирования интеллектуальных систем – Open Semantic Technologies for Intelligent Systems (OSTIS-2012): материалы II Междунар. научн.-техн. конф. (Минск, 16-18 февраля 2012 г.). – Минск : БГУИР, 2012. – С. 143-158.
10. Додонов О.Г., Ланде Д.В., Путятін В.Г. Інформаційні потоки в глобальних комп'ютерних мережах. – К: Наукова думка, 2009. – 295 с.
11. Чертов О.Р. Поліноми Кунченка для розпізнавання образів // Вісник НТУУ «КПІ» Інформатика, управління та обчислювальна техніка, 2009. – № 50. – С. 105-110.

УДК 004.738.5(043.2)

О.В. Дубчак; В.В. Крамарчук
(Національний авіаційний університет, Україна)

ЗАСОБИ ЗАХИСТУ WEB-СЕРВЕРА

Вступ Сучасне розповсюдження з'єднань з мережею Internet, крім забезпечення інформаційними та комунікаційними ресурсами, приховує загрозу несанкціонованого доступу до конфіденційної інформації. Кожна установа, яка веде обмін даними у всесвітній мережі, має співставляти можливі втрати з перевагами, що надає можливість виходу в Internet, та забезпечувати відповідний захист власних ресурсів.

Актуальність Серед варіантів убезпечення web-серверів останнім часом використовується протокол SSH - засіб організації безпечного доступу до комп'ютерів під час роботи небезпечними каналами зв'язку.

Мета Визначити переваги і недоліки протоколу SSH.

SSH (Secure Shell) є мережевим протоколом, який використовується для віддаленого керування комп'ютером і передавання інформаційних пакетів.

За функціональністю SSH схожий на протоколи telnet і rlogin, але шифрує увесь трафік разом із паролями, що передаються.

Для організації безпечного доступу застосовується процедура аутентифікації з використанням асиметричного шифрування з відкритим ключем, що забезпечує вищий рівень безпеки ніж при симетричному шифруванні, яке дозволяє заощаджувати процесорний час і використовується під час подальшого обміну даними.

Протокол надає можливість підтвердження оригінальності хосту, з яким відбувається з'єднання.

SSH підтримує два основних протоколи: SSHv1 і SSHv2. Перший заснований на алгоритмі асиметричного шифрування RSA, а другий – підтримує RSA та алгоритм асиметричного шифрування DSA.

SSH сервером може використовуватися один з трьох типів ключів: SSHv1 RSA, SSHv2 RSA, SSHv2 DSA.

Серед характеристик протоколу SSHv2 слід виділити стійкість до атак прослуховування, «man-in-middle»; атак, що здійснюються шляхом приєднання посередині, «session hijacking»; атак «DNS spoffing».

З метою підвищення безпеки здійснюється подвійна аутентифікація «клієнт – сервер», «сервер – клієнт».

Висновки Протокол SSH забезпечує високий рівень безпеки, хоч і потребує додаткового обчислювального навантаження. Для безпеки використання SSH пропонуються наступні рекомендації: заборонити доступ з потенційно небезпечних адрес; заборонити віддалений root – доступ, підключення з порожнім паролем або відключення входу за паролем; обирати нестандартний порт для SSH-сервера; використовувати довгі SSH2 RSA-ключі; обмежити список IP-адрес, з яких доступ дозволено; регулярно здійснювати перегляд повідомлень про помилки аутентифікації; увести наявність детекторів атак, таких як IDS (Intrusion Detection System); використовувати пастки (honeypots), що підроблюють SSH-сервіс.

УДК 004.738.5(043.2)

О.В. Дубчак; Р.О. Хілик
(Національний авіаційний університет, Україна)

ХАРАКТЕРИСТИКА СПЕЦИФІКАЦІЙ IEEE802.11ac ТА IEEE802.11 ad

Вступ Характерним процесом у розвитку інформаційних технологій є тотальна інтеграція, якою охоплені мікроелектроніка й техніка зв'язку, сигнали й канали, системи й мережі, поряд із чим останнім часом дістала активного розвитку і інтеграція інформаційної безпеки.

Актуальність Найсучаснішою технологією для організації безпровідних локальних обчислювальних мереж всередині приміщень є технологія, що базується на специфікації стандарту IEEE 802.11ac. Одночасно розробляється і новітня специфікація 802.11ad, яка, ймовірно, стане альтернативою Bluetooth.

Мета Визначити переваги і недоліки новітніх специфікацій стандарту бездротового зв'язку серії IEEE 802.11.

У специфікації IEEE 802.11ac передбачено підключення до мережі великої кількості бездротових пристроїв, а енергоспоживання знижено в у 6 разів, що дозволить збільшити час роботи пристроїв; підвищення швидкості передачі даних в декілька разів гарантовано використанням каналу завширшки 80 Mhz та 160 Mhz; зменшення шкідливого впливу вхідних сигналів користувачів, що знаходяться поруч, забезпечується використанням діапазону 5 Ghz; вирішено проблему падіння потужності сигналу через його віддзеркалення від різноманітних поверхонь завдяки зсуву фаз вхідних сигналів, що зменшує сумарну амплітуду; Beamforming (формування спрямованого сигналу) покращує розповсюдженню сигналів, підвищуючи якість приймання.

У поточній версії специфікації 802.11ad визначено максимальну швидкість передачі до 7Гб/с; робоча частота як одна з основних характеристик специфікації складатиме 60 ГГц замість 5 ГГц; робочий діапазон відповідно зменшиться. Визначено, що специфікації 802.11ac і 802.11ad не конфліктуватимуть між собою через невеликий радіус передачі.

Слід зазначити, що необхідною умовою для успішного функціонування обох специфікацій є зменшення значних перешкод на шляху сигналу. Щодо засобів безпеки інформаційних потоків, що циркулюють мережею, то бездротову мережу вважають захищеною, якщо в ній функціонують три основних складових системи безпеки: аутентифікація користувача, конфіденційність і цілісність передачі даних, які необхідно ураховувати при організації і налаштуванні приватної Wi-Fi-мережі.

Висновок Кожна удосконалена специфікація стандарту має такі переваги, як підвищення швидкості передачі та стабільності сигналу, зниження енергоспоживання. Використання специфікації IEEE 802.11ac підвищить пропускну спроможність каналу, що вплине на швидкість обміну даними та їх доступність, дозволить одночасне використання Інтернету в корпоративних мережах, забезпечить багаторазове збільшення швидкості в домашніх мережах. Щодо специфікації 802.11ad, то прогнозується її застосування як безпровідного USB для підключення периферійних пристроїв комп'ютерних систем.

УДК 004.75

О.О. Жолдаков, к.т.н.;
А.О. Жолдаков
(Національний авіаційний університет, Україна)

МЕРЕЖЕВА МОДЕЛЬ У НЕЧІТКОМУ СЕРЕДОВИЩІ ПРОЕКТУВАННЯ ОРГАНІЗАЦІЙНО-ВИРОБНИЧИХ СИСТЕМ

Ефективність процесу проектування нових або модифікованих організаційно-виробничих систем може бути вирішальним фактором її успішного впровадження і подальшої конкурентоспроможної експлуатації. У зв'язку з цим процес проектування потребує дослідження з урахуванням нечіткості його ключових факторів, як то часові параметри його фаз і процесів.

Основною дилемою видається наявність стандартизованих моделей процесу проектування із постійними (детермінованими) етапами і операціями з однієї сторони, а з другої – невизначеність (нечіткість) дійсних часових та інших ресурсних характеристик операцій процесу проектування.

Відомо, що розробка проектної документацій завершується на стадії робочого проектування. Але після кожної фази проектних робіт проектант отримує нові данні (знання) щодо об'єкту проектування, а, отже, повинен провести аналіз цих даних. Це стосується, щоправда в різній степені, технології "водоспад" та "спіральної" технології. Результатом аналізу може бути внесення змін до наступної стадії проектування.

Очевидно, що існує тісний зв'язок між тим, які властивості має об'єкт проектування і управлінням процесом проектування з позицій ефективності його реалізації. Але нечіткість в оцінці умов і ресурсів проектування зумовлює неадекватність детермінованих і статистичних моделей процесу проектування. Ймовірно, експертне оцінювання параметрів проектування в термінах нечітких множин і логіки може дати прийнятну альтернативу.

Якщо кожну фазу проектування представляти як послідовність робіт (операцій), що переводять процес у наступний стан, то весь процес проектування представляється як мережа із вершинами-станами і дугами-операціями. що зв'язують вершини; тоді розрахунок такої мережі (процесу проектування) потребує виявлення резервів часу у виконанні кожної роботи, щоб забезпечити можливість управління процесом проектування.

Алгоритм розрахунку мережі проекту складається із трьох основних етапів: обчислення найбільш ранніх можливих строків кожної події; обчислення найбільш пізніх допустимих строків завершення події; обчислення резерву кожної події та роботи.

За умови розробки мережевого алгоритму для нечіткого середовища проектування, який би мав достатній ступінь універсальності, можна здійснювати навчання експертів із настроюванням моделі на конкретний об'єкт проектування.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Кофман А.* Введение в теорию нечетких множеств: Пер. с франц. М.: Радио и связь, 1982. - 432 с.

УДК 004.2 (043.2)

И.А. Жуков, д.т.н; Н.А. Ковалев
(Національний авіаційний університет, Україна)

СНИЖЕНИЕ АППАРАТНОЙ СЛОЖНОСТИ ЦИФРОВЫХ ИНТЕГРИРУЮЩИХ СТРУКТУР

Для реализации вычислений в реальном времени с высокими точностью, быстродействием при оптимальных затратах оборудования эффективно используются цифровые интегрирующие структуры (ЦИС), в которых реализуется численное интегрирование по Стилтьесу систем уравнений Шеннона (СУШ). При этом используются только аддитивные и мультипликативные операции. ПЛИС типа FPGA являются оптимальной базой для реализации ЦИС [1].

В случаях, когда математическая функция является сложной, использование известного метода получения эквивалентной для нее СУШ в симметричной форме приводит к необходимости включения в состав ЦИС большого количества цифровых интеграторов (ЦИ). Учитывая, что при высоких порядках $(N = 4,...,7)$ точности интегральных вычислений каждый из ЦИ предполагает реализацию от 4 до 14 операций умножений соответственно, интегральная реализация ЦИС потребует значительных расходов ресурсов, особенно блоков умножения (DSP-секций), кристалла FPGA.

Особенность предложенного метода перехода к эквивалентной СУШ заключается в том, что декомпозиция исходной функции и последовательное дифференцирование выделенных функций (при одновременном введении новых переменных) проводится до момента, когда подынтегральные и введенные функции примут вид целых рациональных выражений. В полученную СУШ входят как дифференциальные уравнения, так и целые рациональные функции, выражающие зависимые переменные. ЦИС будет включать ЦИ и операционные блоки (ОБ), реализующие вычисления в соответствии с введенными функциями. Экстраполяцию приращений зависимых переменных, необходимую для согласования ЦИ и ОБ внутри ЦИС, можно проводить также на основе алгоритма с использованием разностей первого порядка.

Исследования показали [2], что при построении ЦИС по сравнению с известным предложенный метод перехода от сложных функций к эквивалентным СУШ позволяет в 1,5-2 раза уменьшить число ЦИ в их составе. Это позволяет практически также снижать ресурсоемкость и повышать другие технико-экономические параметры интегральных реализаций ЦИС, а также использовать при этом более бюджетные микросхемы FPGA. Метод позволяет также упростить процесс перехода к эквивалентным СУШ и повысить точность интегральных вычислений, так как зависимые переменные вычисляются не через системы эквивалентных функций, а непосредственно.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Опанасенко В.М., Лісовий О.М.* Реалізація проблемно-орієнтованих цифрових пристроїв на кристалах FPGA // Радіоелектронні і комп'ютерні системи. – 2009. – № 5(39). – С. 176-183.
2. *Ковалев Н.А., Кравченко Н.И., Стефанович В.Т.* Исследование метода реализации баллистического вычислителя на базе FPGA // Артиллерийское и стрелковое вооружение. – 2007. – № 3 (24). – С. 42-47.

УДК 004.312.2:621.391.25:621.394.14(045)

И.А. Жуков, д.т.н.
(Национальный авиационный університет, Украина);
В.И. Кубицкий, к.т.н.
(Всероссийский научно-исследовательский институт радиоаппаратуры, Россия)

СЛОЖНОСТЬ РЕАЛИЗАЦИИ ВЫЧИСЛЕНИЙ В КОНЕЧНЫХ ПОЛЯХ

Вычисления в конечных полях находят применение во многих областях науки и техники: в теории кодирования, в криптографии, при цифровой обработке сигналов и др. Для операций в конечных полях необходимо создавать дополнительные подпрограммы или специальные вычислительные устройства.

Для большинства информационно-вычислительных систем и систем связи значительную роль играют такие параметры как аппаратурная сложность составляющих их элементов и время обработки/передачи информации. С точки зрения улучшения этих параметров необходимо рассматривать реализацию операций в конечных полях.

В докладе рассмотрены схемы, реализующие некоторые методы выполнения операций над элементами конечных полей $GF(2^m)$, приведены аппаратурные и временные сложности и дана сравнительная оценка сложностей этих схем.

Под *аппаратурной сложностью* (N) схемы будем понимать количество функциональных элементов базисного набора (*И*, *ИЛИ*, *НЕ*) в схеме, реализующей заданную функцию.

Под *временной сложностью* (T) схемы будем понимать время, необходимое для реализации схемой заданной функции; при этом за единицу времени принимается время срабатывания элемента базисного набора (t).

Сложность схем приводится для любого образующего конечное поле неприводимого многочлена $p(x)$ заданной степени m.

Сложность схемы умножения элементов конечного поля на сдвиговых регистрах (ССУЭ) равна:

$$N^{И}_{ССУЭ} = 77m - 2\,, \qquad T^{И}_{ССУЭ} = (22m + 15)t\,.$$

Схема, реализующая умножение по методу Барти–Шнайдера (схема БШУЭ), имеет сложность (без учёта сложности схемы вычисления величин $\alpha^{(i)}_{kl}$, которая в публикациях не приводятся):

$$N^{И}_{БШУЭ} = (m+1)(5m-4)m\,, \qquad T^{И}_{БШУЭ} = (6m-4)t\,.$$

Для разработанного нового метода умножения элементов конечного поля $GF(2^m)$ с использованием умножения и деления многочленов над полем $GF(2)$ сложность комбинационной схемы умножения (КСУЭ) равна:

$$N_{КСУЭ} = m(10m-13)+4\,, \qquad T_{КСУЭ} = (6m-5)t\,.$$

Комбинационные схемы (КСИЭ-М), реализующие новый метод инвертирования элементов конечного поля $GF(2^m)$ с вычислением миноров, имеют сложность:

$$N_{КСИЭ-М} = (5m^2-4m)(m-1)/2 + \sum_{r=2}^{m-1}(5r-4)[m!/r!(m-r)!]\,,$$

$$T_{КСИЭ-М} = (m-1)(3m+4)t/2\,,$$

Инвертирование элементов конечного поля можно выполнять по методу Барти–Шнайдера. Однако схемы инвертирования, реализующих этот метод (схемы БШИЭ), и их сложность в публикациях не приводится.

Сравнивая КСУЭ с ССУЭ, имеем:

$$\Delta N = N^{II}_{ССУЭ} - N_{КСУЭ} = 2(45m - 5m^2 - 3), \qquad \Delta T = T^{II}_{ССУЭ} - T_{КСУЭ} = (16m + 20)t .$$

Видно, что временная сложность КСУЭ всегда меньше временной сложности ССУЭ, а аппаратурная сложность КСУЭ меньше сложности ССУЭ для $m \le 8$.

Сравнивая КСУЭ с БШУЭ, получаем минимальные (т.к. не известна сложность схемы вычисления величин $\alpha^{(i)}_{kl}$) значения величин:

$$\Delta N^{\min} = N^{II}_{БШУЭ} - N_{КСУЭ} = m[m(5m - 9) + 9] - 4 ,$$

$$\Delta T^{\min} = T^{II}_{БШУЭ} - T_{КСУЭ} = t .$$

Таким образом, сложность КСУЭ всегда меньше сложности БШУЭ.

Точное сравнение КСИЭ-М и схем БШИЭ выполнить невозможно, так как не известны сложности схем вычисления элементов $\alpha^{(i)}_{kl}$ матрицы M_i и схем вычисления минора $\hat{M}_{i+1,1}$ элемента $\hat{A}_{i+1,1}$ матрицы $\hat{A}$ в схемах БШИЭ. Однако можно определить величины сложностей этих схем, при которых КСИЭ-М будут лучше схем БШИЭ. Если принять во внимание, что аппаратурные сложности схем вычисления минора $\hat{M}_{i+1,1}$ элемента $\hat{A}_{i+1,1}$ матрицы $\hat{A}$ в схемах БШИЭ и минора M_{1j} элемента A_{1j} матрицы A в КСИЭ-М одинаковы, то в результате сравнения КСИЭ-М и схем БШИЭ получим:

$$\Delta N^{\min} = N^{\min}_{БШИЭ} - N_{КСИЭ-М} = m(5m^2 + m - 4)/2 .$$

Т. е. аппаратурная сложность КСИЭ-М всегда меньше аппаратурной сложности схем БШИЭ. Это при том, что не учтена сложность схемы для вычисления элементов $\alpha^{(i)}_{kl}$ матрицы M_i в схемах БШИЭ (такая схема и её сложность в публикациях отсутствуют). При этом временная сложность $T_{КСИЭ-М} \le T_{БШИЭ}$, если временная сложность схем вычисления элементов $\alpha^{(i)}_{kl}$ матрицы M_i в схемах БШИЭ будет не менее величины $(m-2)t$.

Полученные в результате сравнения соотношения сложностей схем, реализующих разработанные и известные методы вычислений в конечных полях, позволяют выбирать лучшие из этих методов и схем по необходимым параметрам (аппаратурным затратам, времени вычисления).

Комбинационные схемы, реализующие новые методы вычислений в конечных полях, значительно сокращают время вычислений по сравнению с реализацией в линейных последовательностных машинах: для операций умножения элементов конечного поля – в 4 раза.

Для некоторых степеней образующего поле $GF(2^m)$ неприводимого примитивного многочлена $p(x)$ разработанные схемы также лучше с т. з. аппаратурной сложности. Эти схемы имеют также преимущество по сложности перед другими известными комбинационными схемами, например, реализующими метод Барти–Шнайдера.

УДК 004.451.42

С.В. Журавель; О.П. Мартинова, к.т.н.
(Національний авіаційний університет, Україна)

ТЕРМІНАЛЬНА АРХІТЕКТУРА ЯК МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Останнім часом широкого поширення набула технологія «тонкий клієнт», орієнтована на мінімізацію загальної вартості володіння та підвищення ефективності використання інформаційних систем.

В даний час склалося два основних види побудови обчислювальних систем за типом архітектури: централізований і розподілений. Принциповою відмінністю між ними є те, що при розподіленій архітектурі велика частина обчислень проходить на «клієнті», а при централізованій всі обчислення виконуються на центральному сервері. Система, заснована на терміналах, являє собою центральний обчислювальний майданчик, до якого під'єднуються термінальні клієнти. Причому клієнти можуть бути як стаціонарними, так і мобільними, і підключатися не тільки через LAN, а й через WAN. На центральному обчислювальному майданчику знаходиться термінальний сервер, він же, як правило, і є сервером додатків, який може бути пов'язаний з сервером баз даних. На майданчику також може знаходитися резервний термінальний сервер, що забезпечує підвищену відмовостійкість і високу готовність системи в цілому. При централізованій архітектурі особливо актуальне застосування технології «тонкий клієнт».

Таким чином, результатом застосування термінальної архітектури є: зменшення капіталовкладень - тонкі клієнти не потрібно модернізувати, вартість терміналів значно менше персональних комп'ютерів. Досить провести модернізацію серверу терміналів, якщо не вистачає обчислювальних ресурсів для термінальних клієнтів. Тонкі клієнти надійніші - надійність системи підвищується за рахунок відсутності механічних компонентів і спрощеної архітектури тонкого клієнта, термін служби терміналів більший, ніж у робочих станцій. Інформація зберігається безпечно - вихід з ладу тонкого клієнта не приведе до втрати інформації, тому що вона зберігається на сервері термінальних клієнтів, відсутність дисків і дисководів знижує ризики просочування інформації і занесення в систему вірусів, можливість несанкціонованого перехоплення унеможливлюється програмним шифруванням даних, зберігання даних і налаштувань на сервері тонких клієнтів спрощує процедури резервного копіювання. Адміністрування обчислювальної системи централізоване - клієнт термінального сервера не може порушити стабільність роботи сервера тонких клієнтів, термінальний доступ легко адмініструється, легко контролювати користувачів і керувати програмним забезпеченням; встановивши термінальний сервер, можна легко обмежити доступ до небажаних ресурсів. Швидкий доступ до робочого столу - користувач отримує доступ до свого віртуального робочого столу на будь-якому термінальному клієнтові; налаштування нового тонкого клієнта займає декілька хвилин. Локальна мережа не завантажена за рахунок вивільнення ресурсів - термінальний доступ відрізняється тим, що на тонкий клієнт передаються лише стани екрану, тоді як на ПК можуть передаватися значні об'єднання об'єми даних. Гарним прикладом таких програм є 1С. Коли сервер і клієнтська частина 1С знаходиться на одній машині, то не відбувається пересилка бази даних 1С по мережі і програми працюють набагато швидше.

УДК 004.2. 004.8.

В.Г. Зайцев, д.т.н.; М.В. Плахотний, к.т.н.; Є.І. Цибаєв
(НТУУ «КПІ», Україна)

АЛГОРИТМ ОЦІНКИ ЧАСУ ВИКОНАННЯ ПРОГРАМ В БАГАТОПРІОРИТЕТНИХ СИСТЕМАХ

Ефективність програмного забезпечення (ПЗ) спеціалізованих комп'ютерних систем (СКС) залежить від багатьох факторів: ефективності системи диспетчеризації; організації вирішення основних функціональних задач у реальному часі; визначення оптимальної системи пріоритетів при виконанні додатків та переривань. Виконання цих задач тісно пов'язане з побудовою і дослідженням моделей масового обслуговування СМО, де під заявками на обслуговування розуміють задачі, а під часом обслуговування – час їх виконання. Відповідно можна вважати, послідовності задач - потоками заявок, а інтенсивності виконання задач - інтенсивностями обслуговування. Відповідно можна говорити про середні інтенсивності потоку задач і закони їх розподілу, а також про середні показники часу виконання задач і відповідні закони розподілу. Однією із специфічних особливостей СКС є те, що у більшості випадків перелік функцій СКС є незмінними у весь час їх експлуатації. Це дозволяє вважати, що перелік задач попередньо відомий та відомі характеристики потоків задач, що вирішуються, і середній час їх виконання. Ще однією особливістю є те, що всі вимоги на виконання задач мають задовольнятися. Отже тут розглядаються тільки скінчені моделі.

Будемо вважати, що виконання функцій СКС забезпечуються певною кількістю задач, які підпорядковані певним пріоритетам. Характеристики потоків заявок і час їх виконання попередньо відомі. Слід визначити середній час виконання програми, включаючи перебування у черзі, у залежності від наданого пріоритету. Для цього необхідно розробити відповідні моделі СМО і запропонувати алгоритми їх дослідження.

Проблемі безпріоритетного і пріоритетного обслуговування для систем СМО із скінченними джерелами заявок присвячено дуже багато досліджень. Серед них слід визначити фундаментальні роботи [1-3]. При пріоритетному обслуговуванні розглядаються системи СМО з абсолютними, відносними та змішаними пріоритетами.

В роботі [2] зроблено дуже суттєвий висновок: при дисциплінах з абсолютним пріоритетом наявність вимог з більш низьким пріоритетом ніяк не впливає на процес обслуговування вимог з більш високим пріоритетом.

Дослідження пріоритетних СМО будується на визначенні циклу обслуговування [1] j-го класу для процесів з k класами, під яким розуміють проміжок часу між надходженням вимоги на обслуговування та моментом, коли обслуговуючий пристрій звільняється для того, щоб прийняти на обслуговування чергову вимогу того ж класу. Слід зазначити, що отримані результати дослідження у аналітичному вигляді, як стверджують самі автори, дуже складні у використанні і мають скоріше науковий, ніж практичний інтерес. Тому доцільно

спробувати отримати вирішення проблеми не у вигляді аналітичних формул, а у вигляді алгоритму.

Нехай у системі СМО задіяно n задач. Кожна i - та задача у довільний момент може виставити запит на обслуговування. Інтенсивність такого потоку вимог тоді дорівнює λ_i. Якщо обслуговуючий пристрій (процесор) вільний, він надається задачі. На її обслуговування (вирішення) витрачається середній час $\nu_i = \frac{1}{\mu_i}$. Якщо на момент виникнення вимоги процесор зайнятий, задача стає у чергу на виконання, на що витрачається додатковий час. Загальний потік від задач можна розглядати, як суперпозицію або об'єднання вимог. Будемо вважати, що ці джерела заявок взаємонезалежні. Стаціонарна поведінка такого потоку може визначатися об'єднаною функцією розподілу величини інтервалу часу до моменту виникнення чергового запиту. Визначимо цю функцію через $F(t)$, а через $F_i(t)$ – відповідну функцію для i-го джерела із n взаємонезалежних джерел. Тоді,

Позначимо

$$1 - F(t) = \prod_{i=1}^{n} [1 - F_i(t)]dt \tag{1}$$

$$H_i(t) = 1 - F_i(t); \qquad H(t) = \prod_{i=1}^{n} H_i(t). \tag{2}$$

Функції $A'(t)$, $H(t)$ та $H_i(t)$ є доповнюючими функціями розподілу.

$F(t) = H(t) = 0$ при $t < 0$. Якщо усі функції $H_i(t)$ неперервні, то, зважаючи на (2) можна записати, що

$$\frac{H'(t)}{H(t)} = \frac{H_1'(t)}{H_1(t)} + \ldots + \frac{H_n'(t)}{H_n(t)} \tag{3}$$

Як показано у [4], якщо проміжки часу між вимогами мають довільну, одну і ту ж функцію розподілу з єдиним обмеженням, що вона має неперервну похідну $A'(t)$, то

$$F(t) = \lambda \int_0^t 1 - A(n)\,dn, \tag{4}$$

де λ - математичне сподівання кількості вимог, що надходять у стаціонарному стані. Ця величина вказує середню інтенсивність вхідного рекурентного потоку.

З урахуванням (3) і (4) для $t = 0$, отримуємо

$$\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_n . \tag{5}$$

Якщо припустити, що усі джерела мають пуасонівський розподіл, тобто

$$H_i(t) = e^{-\lambda_i t},\ t > 0 \quad , \tag{6}$$

то з урахуванням (2),

$$H(t) = 1 - F(t) = e^{-\lambda t}, \quad \lambda = \sum_{i=1}^{n} \lambda_i . \tag{7}$$

Виходячи з результату (7) і те, що всі джерела є скінченними, модель СМО процесу обслуговування заявок при $\lambda = \lambda_1 = \lambda_2 = ... = \lambda_n$ може бути визначена як класична модель СМО загибелі та розмноження [3], граф випадкового процесу в якій представлений на рис.1

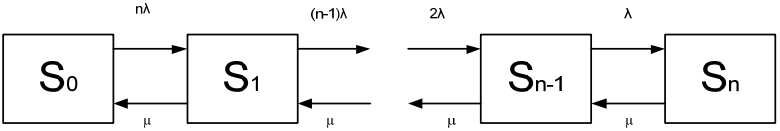


Рис.1. Граф моделі СМО загибелі та розмноження,
де S_i стани випадкового процесу СМО

Ця модель СМО добре вивчена [1,3]. За умови, що потоки заявок мають пуасонівський розподіл, а час обслуговування – показниковий розподіл (марківська модель) усі стаціонарні характеристики моделі можуть бути визначені через граничні імовірності станів P_i, як [3]:

$$\left.\begin{aligned} P_0 &= (1 + n\rho + n(n-1)\rho^2 + \dots\ n(n-1)\dots 1\rho^n)^{-1}, \\ P_1 &= n\rho P_0, \\ P_2 &= n(n-1)\rho^2 P_0, \\ &\dots\dots\dots \\ P_n &= n(n-1)\dots 1\rho^n P_0, \quad \text{де } \rho = \frac{\lambda}{\mu}. \end{aligned}\right\} \tag{8}$$

Оскільки припущення, про показниковий характер закону обслуговування досить умовне, виникає питання про залежність величини P_0 від виду закону розподілу. Експериментальне порівняння розрахунку величини P_0 для марківської моделі СМО і немарківської, при $\mu = const$, показало, що для n у межах 2÷100 та ρ від 0,01 до 0,50, максимальна розбіжність у результатах не перевищує 5%, що підтверджено в [1].

Таким чином, за основу приймемо марківську модель «загибелі та розмноження».

Визначимо середній час обслуговування запитів T, включаючи перебування у черзі:

$$T = \frac{1}{\mu} P_1 + \frac{2}{\mu} P_2 + \dots + \frac{n}{\mu} P_n ; \tag{9}$$

з іншого боку, середня кількість запитів, що вимагають обслуговування, дорівнює:

$$\omega = 1P_1 + 2P_2 + \dots + nP_n \tag{10}$$

або $T = \frac{1}{\mu}\omega$.

Як відомо, у [3] отримано інший вираз для ω:

$$\omega = n - \frac{1-P_0}{\rho}. \tag{11}$$

Тобто можна записати, що

$$T = \frac{1}{\mu}(n - \frac{1-P_0}{\rho}). \tag{12}$$

У загальному випадку ПЗ СКС буде відповідати декілька потоків заявок на обслуговування, кожен з яких може мати свій пріоритет. Перенумеруємо такі потоки і будемо вважати, що рівень пріоритету буде відповідати його номеру. Нехай всього буде m рівнів пріоритету. Тоді можна вважати, що загальна модель буде складатися з m моделей СМО «загибелі та розмноження», між якими існують певні залежності, а саме:
найбільш пріоритетні заявки першого рівня не залежать від заявок, пріоритет яких $j > 1$, а заявки 2-го рівня – тільки від заявок 1-го рівня.

Розглянемо, як можна врахувати цю залежність. Заявки 2-го рівня пріоритету можуть обиратися на обслуговування тільки у тому випадку, коли заявки 1-го рівня відсутні. Їх відсутність дорівнює $P_0^{(1)}$, де $P_0^{(1)}$ гранична імовірність відсутності заявок у моделі «загибелі та розмноження» з параметрами n_1, λ_1, μ_1.

Позначимо фактичну середню інтенсивність обслуговування заявок 2-го рівня пріоритету, що знаходиться у черзі, через μ_2^*. Вона буде дорівнювати μ_2 з імовірністю $P_0^{(1)}$ і нулю з імовірністю $1 - P_0^{(1)}$. Тоді, μ_2^* буде дорівнювати:

$$\mu_2^* = 0(1 - P_0^{(1)}) + P_0^{(1)}\mu_2 = P_0^{(1)}\mu_2 \tag{13}$$

Тобто, значення $P_0^{(2)}$ можна обчислити за наведеними формулами (8), використовуючи параметри (n_2, λ_2, μ_2^*). Заявки 3-го рівня пріоритету можуть обиратися на обслуговування тільки у тому випадку, коли відсутні заявки 1-го і 2-го рівнів пріоритетів. Позначимо відповідну імовірність через $P_0^{(1,2)}$. Її можна обчислити, якщо розглянути сумісну модель СМО для заявок 1-го і 2-го рівнів пріоритету. Таку об'єднану модель також можна представити, як на рис.1, при відповідній заміні параметрів (n, λ, μ):

$$\begin{aligned} n &= n_1 + n_2, \\ \lambda &= \frac{n_1\lambda_1 + n_2\lambda_2}{n_1 + n_2}; \quad \mu = \frac{1}{\nu}; \quad \nu = \frac{n_1\nu_1 + n_2\nu_2}{n_1 + n_2}, \end{aligned} \tag{14}$$

де ν_1 і ν_2 - середній час виконання програм 1-го та 2-го рівнів пріоритету.

Відповідно, для i –го рівня пріоритету, об'єднанні моделі для обчислення $P_0^{(1,2,3,\ldots,i-1)}$ слід використати параметри:

$$\begin{aligned} n &= n_1 + n_2 + \ldots + n_{i-1}, \\ \lambda &= \frac{n_1\lambda_1 + \ldots + n_{i-1}\lambda_{i-1}}{n_1 + n_2 + \ldots + n_{i-1}}, \quad \mu = \frac{1}{\nu}; \; \nu = \frac{n_1\nu_1 + n_2\nu_2 + \ldots + n_{i-1}\nu_{i-1}}{n_1 + n_2 + \ldots + n_{i-1}}, \end{aligned} \tag{15}$$

де $i = \overline{1,m}$. Якщо позначити через T_i середній час обслуговування заявок (вирішення задач) i –го пріоритету, то їх можна обчислити за допомогою (12) моделі СМО «загибелі та розмноження» (див.рис.1), відповідно заміняючи: $T = T_i$, $n = n_i$, $\lambda = \lambda_i$, $\mu = \mu_i P_0^{(1,2,\ldots,i-1)}$, $\rho = \frac{\lambda}{\mu}$.

Запропоновано метод обчислення середнього часу вирішення задач у багатопріоритетних спеціалізованих комп'ютерних системах. Метод базується на циклічному використанні класичної моделі СМО «загибелі та розмноження» шляхом багатократної заміни параметрів. Експериментальні дослідження алгоритму, розробленого на базі запропонованого методу, показали його високу ефективність у порівнянні з відомими обчисленнями за результатами аналітичних формул [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1.*Н. Джейсул*. Очереди с приоритетами. – М. «Мир», 1973, 280 с.
2. *Г.Вагнер*. Основы исследования операций, том 3. – М. «Мир», 1973, 504 с.
3. *Е.С. Вентцель*. Исследование операций. – М. «Мир», 1982, 386 с.
4. *Дж. Риордан*. Вероятностные системы обслуживания. – М. «Связь», 1966, 184 с.

УДК 004.2. 004.8.

В.Г. Зайцев, д.т.н.; М.В. Плахотний, к.т.н.; Є.І. Цибаєв
(НТУУ «КПІ», Україна)

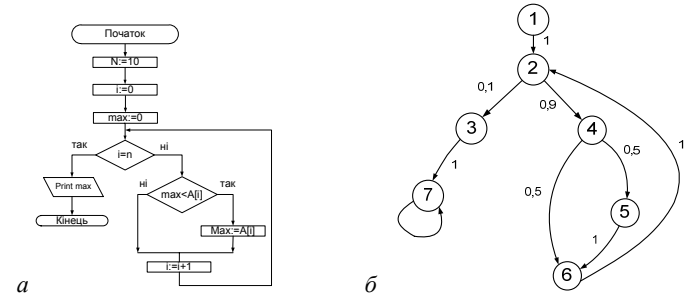
МОДЕЛЮВАННЯ ДИСКРЕТНОГО МАРКІВСЬКОГО ЛАНЦЮГА ЯК МЕТОД ОЦІНКИ ЧАСУ ВИКОНАННЯ ПРОГРАМ

Програмне забезпечення (ПЗ) спеціалізованих комп'ютерних систем має ряд особливостей, серед яких: виконання завдань у реальному часі; незмінність функцій ПЗ під час усього періоду експлуатації; необхідність обміну інформацією із зовнішнім абонентом.

Ці особливості на стадії проектування ПЗ [1] потребують виконати його оптимізацію та оцінити часові характеристики програм: середній час виконання; середню частоту виконання окремих блоків; перевірити можливість зациклювань і т.п. Існує декілька підходів до вирішення цих задач: створення декількох варіантів програмної системи і на основі реальних даних обрати оптимальний варіант; імітаційне моделювання; створення і дослідження математичних моделей. Перший підхід може виявитися дуже затратним та неприпустимим щодо часу розробки. Другий підхід у більшості випадків не може бути рекомендований на ранніх стадіях проектування, оскільки не можна точно визначити вхідні параметри моделей і розрахувати відповідні навантаження окремих блоків обчислюваної системи. Отже, створення і дослідження математичних моделей функціонування ПЗ є дуже перспективним підходом.

Метою роботи є створення математичної моделі функціонування ПЗ, за допомогою якої можна оцінювати такі характеристики програми (комплексу програм): відсутність можливості зациклювання; середній час виконання; середня частота виконання окремих блоків.

Поставимо у відповідність блок-схемі алгоритму програми орієнтований граф $G(i)$, у якому вершини i будуть співставленні блокам і розгалуженням, а орієнтованим ребрам - шляхи переходу алгоритму між окремими блоками. Будемо вважати, що процесу виконання програми будуть відповідати переходи з однієї вершини до іншої, а знаходженню у певній вершині – виконанню деякої команди або блоку програми. Як приклад на рис. 1, *а* наведено блок-схему алгоритму програми пошуку максимального елементу в одновимірному масиві, а на рис. 1 *б* відповідний граф $G(i)$.



а *б*

Рис. 1. Блок-схема алгоритму програми та можлива її інтерпретація графом $G(i)$

Зауважимо, що граф $G(i)$ може бути побудований для алгоритмів будь-якого рівня: рівень команд, модулів, процедур, операторів мови проектування програм PDL [1] і т.п. Використовуючи таку модель, можна розглядати виконання програми як існування деякого випадкового процесу $S(t)$ з дискретними станами і з дискретним або неперервним часом, якому відповідає граф $G(i)$. Зважаючи на особливості виконання програм, можна вважати, що переходи процесу $S(t)$ із стану i в стан j не залежать від того, яким чином він потрапив у стан i, а тільки залежить від перехідних імовірностей P_{ij}, якими навантажують (розмічають) відповідні ребра графа $G(i)$.

З урахуванням цього можна інтерпретувати процес виконання програми як випадковий марківский процес з дискретними станами, які пов'язані у марківський ланцюг матрицею перехідних імовірностей P.

Нагадаємо, що випадковий процес $S(t)$, який відбувається у системі, називається процесом з дискретним часом, якщо перехід з одного стану в інший відбувається тільки у попередньо визначені моменти часу $t(1), t(2), \ldots,$ що називаються кроками такого процесу. У проміжках між кроками система S зберігає свій стан. При цьому не виключається, що на деяких кроках система не буде змінювати свій стан. Як відомо [2], випадковий процес з дискретним часом можна представити випадковою послідовністю (по індексу k) таких подій

$$S_i(k), \quad \overline{i=1,n,}; \quad \overline{k=1,2\ldots,} \tag{1}$$

де n – кількість вершин графа $G(i)$.

Оскільки система $S_{(i)}$ у довільний момент часу t може перебувати тільки в одному із станів $S_1,\ldots,S_n$, то при кожному $k=1,2\ldots$ події $S_1(k),\ldots,S_n(k)$ несумісні і утворюють повну групу подій. Основними характеристиками марківських ланцюгів з дискретним часом є імовірність станів

$$P_i(k) = P(S_i(k)) \ , \ \overline{i=1,n} \ ; \ \overline{k=1,2\ldots,}$$

та імовірності переходів P_{ij}, що утворюють квадратну матрицю переходів порядку $n-P$.

$$P = \begin{bmatrix} P_{11}, P_{12}, \ldots, P_{1n} \\ P_{21}, P_{22}, \ldots, P_{2n} \\ P_{n1}, P_{n2}, \ldots, P_{nn} \end{bmatrix} \tag{2}$$

$$\sum_{i=1}^{n} P_i(k) = 1; \; k = 1,2,\ldots, \tag{3}$$

$$\sum_{j=1}^{n} P_{ij} = 1; \qquad \overline{i = 1,n} \tag{4}$$

Наявність на розміченому графі стрілок та визначень відповідних імовірностей переходів вказує на відмінність їх від нуля. Відсутність стрілок говорить про те, що відповідні імовірності дорівнюють нулю. Якщо сума

імовірностей, що виходять з певної вершини менше 1, це свідчить про імовірність затримки на певному кроці P_{ii}, яка дорівнює

$$P_{ii} = 1 - \sum_{j=1}^{n} P_{ij}; \quad i \neq j \tag{5}$$

Якщо $P_{ii} = 1$, це свідчить про те, що процес потрапив в так званий поглинаючий стан, з якого він вже вийти не може, блукання по станам завершується. Вектор - рядок станів у початковий момент дискретного часу $t(0) - P^{(0)} = (P_1(0), P_2(0), \ldots, P_n(0))$ називають вектором початкового розподілення імовірностей. Для наведеного прикладу (рис. 1 *б*) він дорівнює $(1,0,0,0,0,0,0)$. Як відомо [3], для визначення вектора - рядка імовірностей переходу від кроку k до кроку $k+1$ слід взяти добуток вектора - рядка переходу від стану $k-1$ до k на матрицю перехідних імовірностей $\mathbf{P}$, тобто

$$P^{(k)} = P^{(k-1)}\mathbf{P} \ , \tag{6}$$

у загальному вигляді

$$p^{(k)} = p^{(0)}\mathbf{P}^k$$

або [2]

$$P_i(k) = \sum_{j=1}^{n} P_j(k-1)P_{ji}; \quad \overline{i=1,n} \tag{7}$$

Як правило, тривалість часу між моментами переходу розглядається, як стала величина, тобто, $t(i) - t(i-1) = const$. Пов'яжемо тривалість між моментами переходу з попереднім станом процесу. Будемо вважати, що якщо процес переходить із стану S_i в стан S_j, то такий перехід можливий після завершення проміжку часу τ_i - знаходження процесу у стані S_i. Власне кажучи, у такому разі розглядаємо випадковий процес з дискретним часом, у якого переходи відбуваються через попередньо визначені, але нерівномірні інтервали часу.

Визначимо величину проміжку часу $T(k)$ між сусідніми кроками. Ця величина буде дорівнювати

$$T(k) = t(k) - t(k-1), \tag{8}$$

або $T(k)$ буде відповідати формулі

$$T(k) = \sum_{i=1}^{n} P_i(k-1)\tau_i \tag{9}$$

при нерівномірній дискретизації та $T(k) = \tau_i = const$ при рівномірній дискретизації. Якщо $\tau_i = 1$, то

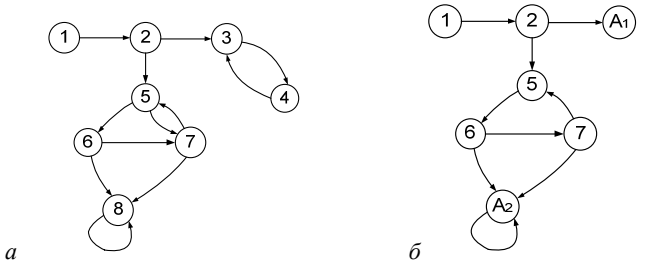
$$T(k) = \sum_{i=1}^{n} P_i(k-1) = 1, \tag{10}$$

що збігається з результатом (3).

Якщо кроки нерівномірні за часом, то величина $T(k)$ визначається за формулою (9) і буде залежатиме від τ_i.

Кожний алгоритм або програма мають початок і кінець. Таким чином, ця необхідна умова відповідає структурі графа $G(i)$. Як відомо [3], перетворюючи

алгоритм або програму у граф $G(i)$, можна попередньо побудувати діаграму порядку G_1, оскільки вона являє собою граф без контурів. При цьому, у графі G_1 можуть існувати тупикові вершини – вершини, з яких дуги не виходять за межі контуру. Підграфи, що відповідають тупиковим вершинам, називають ергодичними класами марківського ланцюга. Якщо ергодичний клас складається з однієї вершини, то такий стан називають поглинаючим. Наприклад, на рис. 2 наведено граф $G(i)$ та його діаграма порядку.



а *б*

Рис. 2. Граф переходів $G(i)$ – *а*, та його діаграма порядку – *б*

З діаграми порядку видно, що у графі $G(i)$ існує два ергодичні класи: $A_1 = \{3,4\}$ *та* $A_2 = \{8\}$. Клас A_2 є поглинаючим.

Під час блукання по графу з імовірністю 1, траєкторія марківського ланцюга опиниться в одному з ергодичних класів і вийти з нього не зможе. Якщо наведений граф $G(i)$ відповідає деякий конкретній програмі, то можна казати, що початку програми відповідає вершина 1, кінцю - вершина 8, ергодичний клас A_1 відповідає помилці – «зациклюванню» програми, яка має бути виправлена, а A_2 – поглинаючий.

За допомогою моделі програми у вигляді поглинаючого марківського ланцюга можна обчислити кількість звертань до окремих блоків програми, середній час виконання програми, середню кількість кроків до переходу у поглинаючий стан, що свідчить про завершення програми. Ці характеристики програм можна у подальшому використовувати для застосування методів профілювання коду. Як відомо, для визначення вказаних характеристик програм застосовувались методи імітаційного моделювання [4] і метод, заснований на побудові фундаментальної матриці, кожний з елементів якої дорівнює середній кількості раз потрапляння системи в той чи інший стан до поглинання [4]. Обидва методи досить складні у реалізації та мають проблеми із пошуком зворотних розріджених матриць $n \times n$. Тут запропоновано метод обчислень, побудований на використанні безпосередньо математичної моделі марківського ланцюга із дискретними станами та дискретним часом. Метод полягає у послідовному обчисленні імовірностей станів $P_i(k)$ *при* $k \to \infty$.

Критерієм завершення процедури обчислень служить:

$$P_n(k) \to 1, \text{ при } k \to \infty \ , \qquad (11)$$

якщо P_n відповідає поглинаючому стану.

Поняття $k \to \infty$ є математичною абстракцією. Як доведено на практиці, для відповідних розрахунків достатньо обрати $P_n(k) \approx 0{,}99999$.

Позначимо середню кількість кроків до поглинання через K. Тоді середній час виконання K кроків до завершення програми (попадання у поглинаючий стан) T можна обчислити як:

$$T = \sum_{j=1}^{K} T(j) . \tag{12}$$

Якщо уявити, що поглинаючий стан винесено за «кінець» алгоритму, то час його виконання τ_n в розрахунках має дорівнювати 0. Тоді з урахуванням (8) час T визначається як:

$$T = \sum_{j=1}^{K} \sum_{i=1}^{n} P_i(j-1)\tau_i . \tag{13}$$

Якщо уявити, що $\tau_i = const = 1; \quad \overline{i = 1, n-1}; \quad \tau_n = 0$; то з урахуванням (9)

$$T = \sum_{j=1}^{K} T(j) = K . \tag{14}$$

Визначимо загальний час перебування системи у стані $S_i - T_i$.
На кожному кроці система знаходиться у стані S_i середній час $P_i(j-1)\ \tau_i$.
Тоді за K кроків загальний час T_i визначається як:

$$T_i = \sum_{j=1}^{K} P_i(j-1)\tau_i \tag{15}$$

У середньому, кількість разів потрапляння системи у стан $S_i - K_i$ буде становити :

$$K_i = T_i \ / \ \tau_i \tag{16}$$

або

$$K_i = \sum_{j=1}^{K} P_i(j-1) . \tag{17}$$

Не важко бачити, що

$$K = \sum_{i=1}^{n} K_i \tag{18}$$

За результатами досліджень створена спеціальна програма обчислення вказаних характеристик. Наведемо приклад розрахунку параметрів *T, K* та K_i програми, наведеної на рис. 1

	1	2	3	4	5	6	7
1	0	1	0	0	0	0	0
2	0	0	0.1	0.9	0	0	0
3	0	0	0	0	0	0	1
4	0	0	0	0	0.5	0.5	0
5	0	0	0	0	0	1	0
6	0	1	0	0	0	0	0
7	0	0	0	0	0	0	1

Рис. 3. Матриця перехідних імовірностей P_{ij} .

Результати розрахунків для випадку:
матриця перехідних імовірностей, як на рис. 3;
τ_1 =10, τ_2 =20, τ_3 =50, τ_4 =20, τ_5 =10, τ_6 =20.

Результати: $T = 665,\ K = 34.5,\ K_1 = 1,\ K_2 = 10,\ K_3 = 1,\ K_4 = 9,\ K_5 = 4,5,\ K_6 = 9.$

Створено математичну модель і запропоновано метод обчислення часових характеристик програм. Згідно запропонованого методу, основною операцією обчислень є операція – добуток вектора на матрицю n x n, що достатньо просто реалізується для великих n,особливо зважаючи на те, що відповідні матриці сильно розріджені і для обчислень можна застосовувати спеціальні методи [5].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *М.Зелковиц, А.Шоу, Дж.Геннон*. Принципы разработки программного обеспечения. -М. «Мир».1982, 368с.
2. *Е.С.Вентцель*. Исследование операций. - М. «Советское радио», 1972, 552с.
3. *И.В.Романовский*. Дискретный анализ: Учебное пособие для студентов, 3-е изд, - СПб : «Невский диалект»; БХВ Петербург, 2003, 320с.
4. *Е.В.Бережная*. Математические методы моделирования экономических систем. -М. «Финансы и статистика», 2001, 368с.
5. *Р.Тьюарсон*. Разряженные матрицы. – М. «Мир», 1977, 192с.

УДК 621.391

С.В. Зайцев, к.т.н.
(Чернігівський державний технологічний університет, Україна)

МЕТОД ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ ПРОГРАМОВАНИХ БЕЗПРОВІДНИХ СИСТЕМАХ ЗА РЕЗУЛЬТАТАМИ АНАЛІЗУ ДЕКОДУВАННЯ ТУРБО КОДІВ

Сучасні та перспективні безпровідні системи повинні забезпечувати належну якість передачі інформації в складній радіоелектронній обстановці. Значне розширення за останнє десятиліття частотної смуги мереж передачі даних привело до появи нового класу безпровідних систем – розподілених програмованих безпровідних систем, які базуються на принципах SDR (software defined radio). Розподілені програмовані безпровідні системи містять декілька обчислювальних вузлів, об'єднаних високошвидкісним інтерфейсом передачі даних [1]. Зазначені системи використовують апаратні засоби для виконання функцій під керуванням програмного забезпечення.

На сьогоднішній день фізичний рівень безпровідних відомчих систем ґрунтується на використанні технологій розширення спектру сигналів та коригувальних кодів [2,3]. До основних методів розширення спектру сигналів, які широко застосовуються в сучасних безпровідних системах, відносяться метод безпосередньої модуляції несучої псевдовипадковою послідовністю та метод псевдовипадкової перебудови робочої частоти [2,3]. Розширення спектру є спосіб передачі, при якому сигнал займає полосу частот більш широку в порівнянні з полосою, мінімально необхідній для передачі інформації; розширення полоси частот сигналу забезпечується спеціальним кодом, який не залежить від інформації, що передається; для подальшого звуження полоси частот сигналу і відтворення даних в приймальному пристрої засобу безпровідного зв'язку також використовується спеціальний код, який аналогічний коду в передавачі і синхронізований з ним.

Сучасні засоби відомчого безпровідного зв'язку для підвищення достовірності передачі інформації застосовують розширення спектру методом безпосередньої модуляції несучої псевдовипадковою послідовністю та метод псевдовипадкової перебудови робочої частоти, в якості коригувальних кодів застосовуються коди Рида-Соломона.

В галузі сучасного безпровідного зв'язку загального призначення найбільшого розповсюдження отримали наступні інформаційні технології: розширення спектру методом безпосередньої модуляції несучої псевдовипадковою послідовністю, коригувальні турбо коди та LDPC-коди, ортогонально-частотне мультиплексування OFDM, технологія MIMO та інші.

Виникає необхідність в підвищенні достовірності передачі інформації та пропускної спроможності сучасних та перспективних відомчих безпровідних систем, які функціонують в умовах впливу навмисних завад, за рахунок застосування нових методів, алгоритмів та методик.

Метою роботи є розробка методу підвищення достовірності передачі інформації в розподілених програмованих безпровідних системах за результатами аналізу декодування турбо кодів.

Аналіз основних алгоритмів декодування турбо кодів показав, що рішення про декодований переданий біт приймається за інформацією про стан каналу, про прийняті інформаційні та перевірочні біти, а також за апріорною інформацією, яка

отримується за результатами декодування попереднім декодером. Надійність прийняття рішення про декодований біт інформації можна підвищити за рахунок використання системи Уолша перед кодуванням турбо кодом (ТК) переданої бітової послідовності. Кожен біт отриманої з використанням матриці Адамара кодової послідовності кодується окремим рекурсивним систематичним згорточним кодом (РСЗК) з різними на відміну від інших РСЗК параметрами коду та алгоритмами перемеження. Застосування системи Уолша та процедури незалежності кодування призведе до зменшення кореляції інформаційної послідовності та до отримання додаткової інформації при декодуванні турбо кодів, а отже до підвищення надійності прийняття рішення про переданий біт. Для підвищення пропускної спроможності розподілених безпровідних програмованих систем пропонується застосування технології OFDM з псевдовипадковою перебудовою піднесучих частот, алгоритм формування яких задається генератором псевдовипадкової послідовності. На приймальній стороні будуть відбуватися зворотні перетворення. Інформація про переданий біт приймається модифікованим декодером Уолша за результатами аналізу логарифмічних відношень функцій правдоподібності про переданий біт, які виробляються кожним декодером ТК, із застосуванням матриці Адамара.

Для дослідження характеристик достовірності передачі інформації з використанням запропонованого методу необхідно провести статистичне імітаційне моделювання. Моделювання проводилось за допомогою програмного продукту Borland C++ Builder 6.0 та пакету прикладних програм Matlab 7.12.0. Результати моделювання свідчать про те, що запропонований метод підвищує завадозахищеність розподілених програмованих безпровідних систем на 0,5-1,2 дБ, та підвищує достовірність передачі інформації.

За результатами дослідження зроблено наступні висновки:

методу підвищення достовірності передачі інформації в розподілених програмованих безпровідних системах за результатами аналізу декодування турбо кодів;

запропонований метод дозволяє підвищити завадозахищеність розподілених програмованих безпровідних систем на 0,5-1,2 дБ;

напрямком подальших досліджень є доцільним розробка методів структурної та параметричної адаптації для підвищення достовірності та завадозахищеності програмованих безпровідних систем.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Зайцев С.В.* Анализ принципов построения программируемых радиостанций / С. В. Зайцев, С. П. Ливенцев, А. И. Артюх // Зв'язок. – 2007. – № 5. – С. 46-54.

2. *Борисов В.И.* Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / Борисов В. И., Зинчук В. М., Лимарев А. Е. и др. – М.: Радио и связь, 2000. – 384 с.

3. *Борисов В.И.* Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей певдослучайной последовательностью / Зинчук В. М., Лимарев А. Е. и др. – М.: Радио и связь, 2003. – 640 с.

4. *Khan F.* LTE for 4G Mobile Broadband. Air Interface Technologies and Performance / Khan F. – Cambridge: Cambridge University Press, 2009. – 509p.

5. *Cho Y.* MIMO-OFDM Wireless Communications with Mathlab / Cho Y., Kim J., Yang W. [et al.]. – Singapore: John Wiley & Sons, 2010. – 457 p.

УДК 004.73(042.4)

В.А. Заруцкий
(Национальный авиационный университет, Украина)

МЕТОД КОРРЕКЦИИ ДРЕЙФА ПАРАМЕТРОВ ДАТЧИКОВ В СЕНСОРНЫХ СЕТЯХ

Проблема дрейфа параметров датчиков и его влияния на результирующую точность измерений весьма актуальна для беспроводных сенсорных сетей [1]. Задача совместного оценивания и коррекции дрейфа решается при следующих предположениях:

- на соседние датчики, расположенные в сравнительно малой окрестности сегмента сети, поступают коррелированные данные;
- датчики, находящиеся внутри сегмента, могут обмениваться между собой данными измерений;
- физические процессы, о которых датчики собирают информацию, являются пространственно коррелированными.

Для оценки параметров и состояния систем широко применяются фильтры Калмана [2]. В данной работе фильтр Калмана модифицирован с учетом случайного характера измеренных данных и параметров измерителя. Он назван фильтром Калмана со случайным поиском (ФСКП). Модель дрейфа описывается полиномиальным, экспоненциальным или гармоническим трендом. На рис. 1 представлена схема ФСКП.

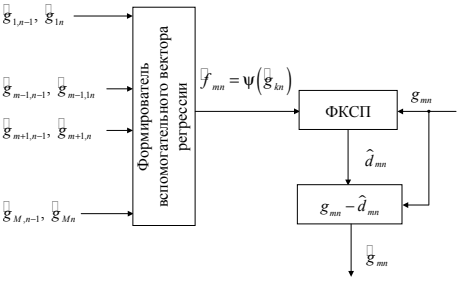


Рис. 1. Фильтр Калмана со случайным поиском

Здесь g_{mn} – исходные (сырые) измеренные данные, g_{mn} – данные, скорректированные по результатам измерений соседних датчиков; f_{mn} – предсказанные значения данных как функция результатов скорректированных измерений; $\hat{d}_{mn}$ – оценка величины дрейфа по результатам совместных измерений.

Размерность задачи определяется числом датчиков, данные с которых поступают на ФСКП. Благодаря применению метода случайного поиска можно значительно ускорить процессы совместного оценивания и коррекции дрейфа параметров при большой размерности вектора данных.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Takruri M., Challa S., Chakravorty R.* Recursive Bayesian Approaches for Auto Calibration in Drift Aware Wireless Sensor Networks // Journal of networks, Vol. 5, Nr. 7, July 2010. - PP. 823 – 832.
2. *Ван Трис Г.* Теория обнаружения, оценок и модуляции. Т. 1. Теория обнаружения, оценок и линейной модуляции. / Пер. с англ. под ред. проф. В.И. Тихонова. – М.: Советское радио, 1972. – 744 с.

УДК 004.728.4(045)

Ю.Ю. Искренко
(Национальный Авиационный Университет, Украина)

МОДИФИКАЦИЯ СХЕМ МНОЖЕСТВЕННОГО ДОСТУПА В ШИРОКОПОЛОСНОЙ БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ *WiMAX*

Актуальным вопросом является оптимальная настройка и моделирование работы антенн, используемых в качестве проводника для излучения или улавливания электромагнитной энергии из пространства в беспроводных широкополосных региональных сетях *WiMAX*. При двусторонней связи одна и та же антенна используется как для приема, так и для передачи сигнала. Увеличение количества антенн и правильное рассредоточение их в пространстве способно увеличить пропускную способность, радиус действия системы и уменьшить затухание сигнала. Моделирование и сравнение различных конфигураций расположения и настроек антенн способно существенно повысить эффективность функционирования сети и снизить стоимость на проектирование и внедрение.

При планировании и моделировании работы приемо-передающего оборудования мобильной беспроводной широкополосной компьютерной сети *Wimax* на основе множественного доступа (*MIMO*) необходимо особое внимание уделять следующим этапам:

– формирование диаграммы направленности (ДН) антенны с обратной связью, при формировании которой радиочастотные электрические импульсы передатчика с помощью антенны преобразуются в электромагнитную энергию, которая излучается по определенному принципу в окружающее пространство [1]. Для улучшения качества, зоны покрытия, пропускной способности системы и уменьшения вероятности нарушения связи система использует многоэлементные антенны на основе множественного доступа;

– пространственное – временное кодирование (без обратной связи) – техника передачи разнесенного радиоприема, поддерживает пространственное разнесение и уменьшает границы замирания сигнала [2];

– пространственное мультиплексирование, без обратной связи обеспечивает преимущества высокой скорости передачи данных и пропускной способности. Сравнивая с системами оборудованными единичными антеннами, приемник оборудованный многоэлементными антеннами может разделить различные потоки информации и функционировать с высокой пропускной способности. Особенно эффективно возможно использовать данное свойство при передаче мультимедийной информации, которая состоит из двух основных потоков – аудио и видео.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Варакин Л.Е. Системы связи с шумоподобными сигналами // Радио и связь. – М.: 1985. – 384 с.

2. Ластовченко М.М., Ярошенко В.Н., Биляк В.И. Математические аспекты проектирования интеллектуальных коммутационных систем передачи ММТ // Математ. машины и системы. – № 6. – 2001. – С. 56–69.

УДК 004.415(043.2)

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

ЗАДАЧА ПОШУКУ НАЙШВИДШОГО ШЛЯХУ

Задача пошуку найшвидшого шляху логічно виходить з задачі пошуку найкоротшого шляху. Хоча різні цілі диктують різні підходи, рішення цих задач мають спільні риси й навіть використовують одне одного в деяких питаннях. Наприклад, аби перетворити алгоритм A* на алгоритм Дейкстри, потрібно лише не враховувати в розрахунку параметру h параметр g. І навпаки, аби розрахувати коротший шлях на поверхні з різною швидкістю переміщення, в розрахунок параметру g додається змінна швидкості переміщення по поточній поверхні. Проте проблеми, які ставить дана задача, як то проблема комівояжера, є більш широкими й потребують детальніших алгоритмів, іноді навіть ціною швидкодії. У даній роботі пропонується метод, створений модифікацією алгоритму пошуку найкоротшого шляху, зі збереженням функціоналу унікальних компонентів та виконанням вимог, що поставлені задачею.

Де потрібна точність, там завжди зустрічається математика з букетом теорій та законів. За роки дослідження даної проблеми вченими-математиками створено ряд алгоритмів, які складають фундамент більшості з використаних в програмах рішень. Серед них такі, як:

- Мурашиний алгоритм
- Алгоритм Беллмана-Форда
- Алгоритм Дейкстри
- Хвильовий алгоритм

Алгоритм пошуку найкоротшого шляху, на основі якого створено метод, засновано на комбінації існуючих алгоритмів, але відрізняється від останніх тим, що задача пошуку в ньому виконується у наступні етапи:

3. Створюється граф на основі поділу простору на «клітинки» зі змінною відстанню, що надає йому гнучкості й точності в поєднанні з простотою реалізацій
4. До оцифрованого простору застосовується алгоритм A* з модифікацією на пошук «фаворитних точок».
5. Отриманний шлях скорочується до оптимального

Характерною рисою розробленого методу є те, що він дозволяє запам’ятовувати пройдені шляхи і включати останні в процес пошуку, та враховує такі аспекти, як змінна швидкість переміщення (в т.ч. під дією різних кутів нахилу), використання дорожньої системи та засобів транспорту, різних типів переміщення та обмежень, пов’язаних з їх використанням. Також, він може адаптуватись під зміни поверхні та використовувати архітектурні особливості місцевості для вирішення поставленої задачі. Алгоритми на основі цього методу можуть бути застосованими для вирішення класичних проблем виду «знайти оптимальний маршрут» та у прикладних задачах, пов’язаних з логістикою та транспортуванням.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. http://www.policyalmanac.org/games/aStarTutorial.htm
2. http://theory.stanford.edu/~amitp/GameProgramming/

УДК 004.73(042.4)

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

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАГРОЗ ПРИ АТАКАХ DDOS ТА BOTNET

Мережна безпека існує з того самого часу, коли технологія Інтернет отримала комерційний статус. Розглянемо два найбільш вживаних метода мережних атак – DDoS та BotNet.

DoS-атака (англ. Denial of Service) - це атака на ресурс з метою припинення його дії. Зазвичай, при відправленні запиту на сайт після DoS-атаки, користувач бачить на екрані помилки 404 (не знайдено сторінку) та 503 (сервіс тимчасово недоступний). Атаки поділяються на «зламування» сайту (відправка запиту неправильного виду, що призводить до критичної помилки і видає зломиснику повні дані ресурсу), недостатню перевірку даних користувача, атаку другого роду (фальшива атака для спрацювання системи безпеки) і, найчастіше, затоплення (перенавантаження ресурсу безглуздими запитами). Якщо атака ведеться з декількох машин, то її називають DDoS (англ. Distributed Denial of Service). Найпростіший метод навантажити цільову систему – пінг-запити (запит, що одразу ж відправляється сервером відправнику, показує користувачеві час затримки між відправленням й прийняттям відповіді).

Логічним продовженням розвитку DDoS став BotNet (англ. roBot Network) – та сама технологія, тільки замість користувачів, що свідомо причиняють шкоду ресурсу, використовуються комп'ютери людей, що можуть і не здогадуватись про свою роль у атаці. Останнім на комп'ютер за допомогою віруса-трояна заноситься програма-бот, що активується за «окликом» зловмисника і непомітно від користувача посилає запити на цільову сторінку. Середня мережа інфікованих комп'ютерів складає десятки тисяч машин, найбільша зареєстрована – понад 12 мільйонів. Понад 80% мирового трафіку спам-листів складає листування машин у BotNet'і заданою рекламою на випадкові адреси.

Ефективних методів протидії мільйонам користувачів, що одночасно відсилають запити на один й той самий ресурс, за визначенням не може існувати. Проте це не означає, що кожен атакований DDoS'ом чи BotNet'ом сайт неодмінно «рухне». Найбільш ефективними методами протидії атакам на сьогодні є:

1) поширення пропускної здатності каналу;
2) приєднання додаткових ресурсів (підключення додаткових серверів для обробки запитів);
3) перенаправлення трафіку на інші сервери за домовленістю;
4) встановлення програмного фільтру на певні види запитів та контратаки по цільових ресурсах атакуючих.

Деякі ресурси мають імунітет до такого роду злочину, бо вони заздалегідь розраховані на велику кількість відвідувачів, або не мають прямого виходу до мережі й працюють через т.н. проксі-сервери. Підприємствами з виробництва мережного обладнання йде розробка апаратних засобів протидії атакам, але поки що жоден з винаходів не отримав необхідної підтримки з боку потенційних користувачів.

УДК 004.73(042.3)

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

ОСОБЛИВОСТІ ОБМІНУ ДАНИМИ ЗА ТЕХНОЛОГІЄЮ P2P

З моменту появи мережі Інтернет було випробувано багато варіантів топології мережі (зірка, кільце, шина, повнозв'язне та ін.) Кожна мала свої позитивні й негативні риси, проте технологічно і економічно найбільш вигідною і, відповідно, поширеною виявилась концепція «клієнт-сервер». В наш час на кожен з таких «серверів» приходяться тисячі «клієнтів», й щодалі їхня кількість лише зростатиме, що незмінно викликає все більш актуальну проблему зменшення навантаження на сервери. Екстенсивне розвинення останніх не може бути нескінченним, тому актуальним є створення нових методів перенаправлення інформації між клієнтами з меншим навантаженням на сервери. Одним з таких методів є P2P.

P2P (peer-to-peer) – це обмін даними між клієнтами напряму, без очікування доки запит потрапить в чергу на обробку, буде оброблений й буде оголошено результат. Між клієнтами створюється потік (stream), через який вони відправляють й приймають данні. Аби «знайти» один одного посеред простору мережі Інтернет, вони відправляють свої «контактні дані» на сервер, який тепер виконує лише функцію довідника з адрес користувачів, що суттєво зменшує навантаження й дозволяє уникнути коштовного апгрейду. Особливо це стосується серверів, що пов'язані зі збереженням великого обсягу файлів медійних типів або від яких потребується обробка у реальному часі великого обсягу даних – бібліотеки фільмів, ігрові сервери, та ін..

В реалії виникає протиріччя між вимогами швидкодії та безпеки. На заваді стає технологія NAT, що захищає користувачів зі все більш поширеним динамічним IP від несанкціонованого доступу. Вона не пропускає пакети, що йдуть до користувача під її захистом, доки він сам не оповістить її, що ці пакети йому потрібні. Зазвичай таке відбувається, коли користувач сам ініціює передачу даних. Через це відкрити потік до користувача з нестатичним IP є неможливим, доки він сам не відкриє потік, але в той самий час, людина, до котрої він відкриває потік, теж може перебувати під надзором NAT'а і не прийняти запит. Хоче користувач того чи ні, він буде захищений від будь-якого втручання, навіть від того, яке йому потрібно.

Для подолання бар'єру NAT'у використовується технологія hole punch (англ. дирокол), яка завдяки одночасному створенню запитів від обох користувачів змушує NAT'и вважати, що саме їх користувач ініціював передачу даних й таким чином «робить дірку» в останніх для обміну інформацією між клієнтами. Цей обхід системи безпеки користувач проводить на свій страх й ризик, проте як результат, сервери лишаються непотрібного навантаження, швидкість обміну даними між клієнтами зростає, відкидається потреба в придбанні коштовного обладнання.

Можна очікувати, що P2P як метод прямої взаємодії між користувачами згодом стане більш масовим. Але з поширенням цієї технології доцільно очікувати, що питання безпеки передачі інформації, тимчасово відкладене у цілях збільшення швидкодії, знову стане актуальним.

УДК 004.728

В.О. Ігнатов, д.т.н.; М.М. Гузій, к.т.н.; О.А. Ладигіна
(Національний авіаційний університет, Україна)

ВЕРИФІКАЦІЯ МОДЕЛЕЙ НЕСТАЦІОНАРНОГО ТРАФІКУ КОМП'ЮТЕРНИХ МЕРЕЖ

В задачах аналізу, моніторингу, оптимального управління трафіком комп'ютерних мереж велике значення має побудова моделей трафіку, що найкращим чином відображають трафік в реальних умовах роботи [1]. Процедура оцінювання адекватності моделі вимірюваному трафіку отримала назву верифікації моделі.

Загальна постановка завдання верифікації моделей нестаціонарного трафіку за допомогою еталонного трафіку наступна. Відомі гаусовські закони розподілу випадкових параметрів поліноміального представлення еталонного трафіку. Методами теорії наближення функцій і математичного програмування потрібно оцінити ступінь адекватності відображення перших двох моментів еталонного нестаціонарного трафіку такими моделями квантування і марківської апроксимації різної розмірності, що є оптимальними за певними критеріями.

Верифікацію моделей пропонується проводити по вибраних критеріях адекватності моделі еталонному трафіку. В якості критеріїв вибрані показники конкордації $\rho(t_k)$ модельних і еталонних значень трафіку на інтервалі нестаціонарності виду:

$$\rho(t_k) = \frac{2 \cdot m(t_k) \cdot M(t_k)}{m(t_k)^2 + M(t_k)^2}, \qquad (1)$$

t_k – k-ий момент часу контролю трафіку,
$m(t_k)$ – математичне сподівання еталонного трафіку,
$M(t_k)$ - математичне сподівання модельного трафіку.

Для дискретного випадку введено середнє значення критерію конкордації моделі і еталону нестаціонарного трафіку вигляду

$$\rho 0(Z_1, Z_n) = \sum_{t_k=0}^{1} \frac{2 \quad m(t_k) \quad M(t_k)}{m(t_k)^2 + M(t_k)^2}, \qquad (2)$$

де Z1, Zт – оптимальні квантовані значення моделі трафіку розмірності n.

Для безперервного випадку введено інтегральний критерій конкордації моделі і еталону нестаціонарного трафіку вигляду

$$\rho 0(Z_1, Z_n) = \int_0^1 \frac{2 \quad m(t_k) \quad M(t_k)}{m(t_k)^2 + M(t_k)^2} dt_k \qquad (3)$$

Проведені обчислення критеріїв (2), (3) показали достатньо добре узгодження запропонованих моделей і еталону нестаціонарного трафіку.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Даниліна Г.В., Гузій М.М., Жуков І А., Ігнатов В.О.* Моделювання перехідних режимів трафіку комп'ютерної мережі // Информационные технологии и безопасность: Сборник научных трудов. – К.: Национальная академия наук Украины, Институт проблем регистрации информации, 2006. – Вып.9. – С. 84 – 87.

УДК 004.716:520.9(043.2)

Н.П. Кадет; А.Г. Коба
(Національний авіаційний університет, Україна)

ОСОБЛИВОСТІ МЕРЕЖ НАЗЕМНИХ ТА ОРБІТАЛЬНИХ ТЕЛЕСКОПІВ

На сьогоднішній день існує два види розміщення телескопів- наземний та орбітальний.

Телескоп має три основних призначення: збирати випромінювання від небесних світил на приймальний пристрій (користувач, фотопластинка, спектрограф тощо); будувати у своїй фокальній площині зображення об'єкта чи певної ділянки неба; збільшувати кут зору, під яким спостерігаються небесні тіла, тобто розділяти об'єкти, розташовані на близькій кутовій відстані й тому нероздільні неозброєним оком.

Оптичні телескопи обов'язковими складовими частинами своєї конструкції мають: об'єктив, який збирає світло і будує у фокусі зображення об'єкта чи ділянки неба; трубу (тубус), яка з'єднує об'єктив з приймальним пристроєм; монтування – механічну конструкцію, що тримає тубус і забезпечує її наведення на небо. У разі візуальних спостережень, коли приймачем світла є око користувача, світлові сигнали формуються окуляром. Через нього розглядається зображення, побудоване об'єктивом. А при фотографічних, фотоелектричних, спектральних спостереженнях окуляр не потрібний, тому що відповідні приймачі встановлюються безпосередньо у фокальній площині.

Цими характеристиками володіють як орбітальні так і наземні телескопи. Основним із аспектів наземного спостереження являється без хмарна погода та чистота неба від світлового забруднення. Якщо беручи до уваги дослідження зоряного неба методом спектрального аналізу то на землі інколи спектр може давати не правильні дані поскільки повітря в деяких чатинах чемлі дуже забруднене. А якщо розгляди орбітальний метод отримання спектру зірки то ця проблема відпадає.

Іще однією особливістю наземного телескопа є його обслуговування при поломці та налаштуванні - не потрібно запускати групу спеціалістів, яка буде здійснювати обслуговування апарату на орбіті.

Розглянувши деякі особливості цих двох видів телескопів можливо прийти до висновку, що для високоточної та більш детальної обробки інформації з телескопів необхідно використовувати принципи рекунфігурованих комп’ютерних мереж.

В космічних технологіях телескопи пов'язані в мережі центрами управління на основі комп'ютерних мереж, також вони мають програмне забезпечення яке допомагає в компютерному керуванні телескопами і це сприяє швидшій та точнішій обробці даних, що надсилають телескопи. На даний момент створюється дуже багато телескопів які можуть вести спостереження без втручання людини і це є значним проривом в розвитку ІТ-технологій.

УДК 621.396

Д.Ю. Кельса; І.І. Слюсарь
(ПолтНТУ ім. Ю. Кондратюка, Украина)

МЕРЕЖІ IP-ТЕЛЕФОНІЇ НА ОСНОВІ ТЕХНОЛОГІЙ БЕЗШОВНОГО РОУМІНГУ

На даний час багато компаній, що розвиваються, стикаються з проблемами організації якісної телефонної мережі на своєму підприємстві. Сучасне рішення в області корпоративної телефонії повинне відповідати визначеним вимогам. У відповідності до них в рамках концепції уніфікованих комунікацій (Unified Communications, UC) пропонується організація мережа IP-телефонії. З іншого боку, сучасною тенденцією є те, що середні та великі підприємства часто займають велику територіальну площу (частину поверху, поверх, часто й цілу будівлю офісного центру). Однак часто у масштабах цілого підприємства необхідна мобільність працівників, що не знімає необхідності постійно бути на зв'язку.

Як наслідок, виникає необхідність побудови такої безпроводової мережі на базі технологій Wi-Fi (IEEE 802.11 a/b/g/n/ac), яка зможе забезпечити покриття сигналом великої площі, а також забезпечити нерозривність зв'язку (іноді використовується термін «безшовний роумінг»). На підставі проведеного аналізу слід виділити два перспективних шляхи вирішення проблеми безшовного роумінгу у мережі IP-телефонії: побудова безпроводової MESH-мережі; побудова Wi-Fi-мережі з контролером. Реалізація першого варіанту повинна передбачати вирішена кількох суттєвих інженерно-технічних завдань, наприклад: затримка при пересилці інформації в мережі (через використання проміжних пунктів) і класифікація та надання пріоритету трафіку у вузлах (і в об'ємі всієї мережі) для досягнення максимальної продуктивності та забезпечення максимуму зручностей користувачів. Хоча безпроводові MESH-мережі знаходиться у стадії розвитку, вони вже демонструють значний потенціал в області створення ефективних комунікацій, що відповідають вимогам бізнесу. Другий варіант забезпечує безшовний роумінг між точками доступу, а також дозволяє виявити присутність стороннього абонента, який підключився до корпоративної мережі IP-телефонії. Однак, існують обмеження на впровадження цих рішень (не всі необхідні частотні діапазони для роботи зараз доступні в Україні).

Окремо слід виділити специфічні рішення по реалізації технології VoIP DECT (на базі SIP) з підтримкою наскрізної передачі абонента (handover). На сьогодні з'явилось кілька продуктів, що вдало конкурують з відомими брендами за функціоналом і мають на порядок нижчу вартість. При таких варіантах побудови корпоративної мережі, клієнт отримує можливість пересуватися територією об'єкту без розриву з'єднання VoIP, відповідно пов'язаних з цим розривів розмови та/або погіршення якості зв'язку. В ході проведених досліджень визначено основні параметри та специфікації існуючих комплексних рішень від всесвітньо відомих виробників мережного обладнання (Cisco, Mikrotik, Ubiquiti Networks і т. ін.). Особлива увага приділялась можливостям і характеристикам сучасного VoIP-обладнання (Cisco, Grandstream, D-Link і т. ін.).

Таким чином, впровадження концепції UC на основі запропонованого інструментарію повинно спиратися на вдале поєднання програмних і апаратних ресурсів, які постійно розвиваються.

УДК 681.322.067

Д.Ю. Кіяшко
(Національний авіаційний університет, Україна)

ПРОТИДІЯ WORM-АТАК НА ОСНОВІ ПОШИРЕННЯ ТРАФІКУ

Хробаки поширюються від комп'ютера до комп'ютера, але на відміну від вірусу, він має можливість подорожувати без будь-якої людської дії. Хробак використовує функції файлу або транспортної інформації про вашу систему, що і дозволяє йому пересуватися без сторонньої допомоги.

Найбільша небезпека черв'яка є його здатність копіювати себе на вашій системі, так що замість відправлення одного хробака, він може посилати сотні або тисячі копій самого себе, створюючи величезний руйнівний ефект. Прикладом може служити для хробака відправити копію себе на всі перераховані адреси електронної пошти в адресній книзі.

У зв'язку з копіюванням природи хробака і його здатністю подорожувати по мережі кінцевий результат у більшості випадків є те, що черв'як споживає занадто багато оперативної пам'яті (або пропускної здатності мережі), у результаті чого веб-сервери, і окремі комп'ютери перестають відповідати на запити.

Для того, щоб розвивати види контрзаходів від атак хробака, ми розглянемо прості і складні моделі атак і, отже, розробимо контрзаходи засновані на двох типах трафіку, що генерується хробаком. Зокрема, з тієї простої моделі, атаки хробака будуть генерувати поширення трафіку (тобто повідомлення, які мають намір визначити вразливі комп'ютери) безпосередньо. Для складних моделей, хробакового нападу спочатку спробуємо сформувати зондування повідомлення для того, щоб визначити місце розташування хробака.

Одним з контрзаходів базується на основі поширення трафіку. Враховуючи, атаки хробака, які приймають зворотний зв'язок механізмів контролю для управління розповсюдженням трафіку, щоб зробити його схожим на фоновий рух і обійти виявлення, ми розробляємо нові спектри на основі схеми захисту від таких атак. Наша конструкція заснована на спостереженні розуміння: в той час як трафік поширення хробака, та фоновий трафік ледь помітні у часовій області, їх відмінність ясна в частотній області, у зв'язку з повторенням маніпулятивного характеру таких хробаків. На схемі використовується спектральна щільність потужності (PSD) розподіл швидкості поширення трафіку і його відповідні спектральні вимірювання площинності (SFM), щоб відрізнити трафік поширення хробака, від не-хробака (фонового) трафіку. Наша пропонована схема може ефективно виявляти такі атаки хробака.

УДК 004.65+004.7(043.2)

А.В. Коваленко
(Національний авіаційний університет, Україна)

ПІДВИЩЕННЯ ШВИДКОСТІ ТА НАДІЙНОСТІ ПЕРЕДАЧІ ДАНИХ ВИКОРИСТАННЯМ ОСОБЛИВОСТЕЙ СТАНДАРТУ *IEEE 802.11n*

Проблема підвищення швидкості і надійності передачі даних є пріоритетною у безпровідних мережах.

Безпровідна мережа стандарту *IEEE 802.11n* об'єднує мобільність безпровідних мереж із швидкістю роботи дротяних, забезпечуючи дев'ятикратне збільшення продуктивності в порівнянні з мережами стандарту *IEEE 802.11 a/g.* Використання спеціальних радіочастотних технологій компанії *Cisco* корпоративного класу, таких як *CleanAir, ClientLink і VideoStream,* а також оптимізованих систем радіодоступу і антени підвищує швидкість передачі даних незалежно від місцезнаходження пристрою [1].

Сучасні безпровідні мережі *IEEE 802.11a/b/g* використовують частотні канали шириною 20 Мгц. Тоді як устаткування мереж *IEEE 802.11n* дозволяє об'єднувати два 20 Мгц каналу в один 40 Мгц. Це дозволяє підвищити пропускну спроможність частотного каналу в два рази. Найбільш ефективне таке об'єднання в діапазоні 5 ГГц, де може бути організовані до 19 частотних каналів, тоді як в діапазоні 2,4 ГГц тільки три. Технологія *IEEE 802.11n* збільшує ефективність використання частотних каналів, поміщаючи декілька пакетів з даними додатків в один кадр, що передається радіопередавачем. Ця технологія дозволяє істотно скоротити накладні витрати при передачі великого числа пакетів малого розміру. У стандартах *IEEE 802.11a/b/g* будь-який пакет рівня *MAC* поміщався в персональний кадр для передачі його по радіо. Переваги рішень стандарту *IEEE 802.11n:* підвищення пропускної спроможності безпровідних мереж *Wi - Fi* до десяти разів, особливо в діапазоні 5 ГГц; підвищення здатності навантаження - більше число безпровідних користувачів може одночасно працювати з однією точкою доступу *IEEE 802.11n*; розширення зони упевненого прийоми за рахунок ефективнішої антенної системи; можливість поетапної модернізації існуючих безпровідних мереж до рівня *IEEE 802.11n* с одночасною роботою облаштувань *IEEE 802.11a/b/g/n* на перехідному етапі. Використання стандарту *IEEE 802.11n* у безпровідних мережах дозволить значно підвищити швидкість і надійність передачі даних. Стандарт *IEEE 802.11n* є найбільш швидкісним для мереж малого радіусу дії (*SRD - short range devices*) і здатний забезпечити пропускну спроможність в 300 Мбіт/с в радіоканалі (без використання *MIMO*)[2].

Точки доступу *Cisco Aironet 1140* підвищують продуктивність безпровідної мережі, що дозволяє підтримувати більше мобільних пристроїв і мобільних додатків нового покоління, призначених для управління матеріальними засобами і перегляду великих рентгенівських знімків за допомогою звичайної системи зв'язку і архівації медичних зображень.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. 802.11n: самый быстрый WiFi. [Electronic resourse] / Интернет-ресурс. - Режим доступа: http://www.computerra.ru/vision/459101/ - Загл. с экрана.
2. Беспроводная сеть 802.11n – антикризисный вариант от Cisco. [Electronic resourse] / Интернет-ресурс. - Режим доступа: http://www.insotel.ru/article.php?id=37 - Загл. с экрана.

УДК 004.7

А.В. Ковальчук
((Національний авіаційний університет, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА ПРОМИСЛОВИХ МЕРЕЖ SCADAСИСТЕМ

SCADA (SupervisoryControlAndDataAcquisition) система - це сукупність апаратно-програмних засобів, що забезпечують можливість моніторингу, аналізу і керування параметрами технологічного процесу людиною. Вона є складовою частиною автоматизованої системи.

Системи SCADA вимагають особливої уваги до питань інформаційної безпеки, так як потенційні кібератаки та інформаційні зловживання можуть призвести до катастрофічних наслідків, починаючи від втрати конфіденційної інформації і аж до порушення технологічного процесу, поломок устаткування і великих аварій.

Як правило SCADA системи фізично відокремлені від основної інфраструктури підприємства та мережі Інтернет. Однак, підприємства все частіше підключають свої SCADA мережі до потенційно небезпечних сегментів корпоративної мережі для обміну оперативною інформацією та зниження витрат на приватні канали зв'язку. Навіть при застосуванні жорстких корпоративних політик, що обмежують доступ до таких систем, може відбуватися ненавмисне з'єднання публічної мережні та мережі управління, що створює додаткові ризики виходу з ладу критичних систем.

У роботіпроведено аналіз існуючих технологічних рішень в галузі інформаційної безпекикомп'ютерних мереж.

Запропоновано впровадження комплексних заходівбезпеки на мережевому рівні, необхідних для захисту мережевого компонента SCADA системи:

- Міжмережеві екрани
- Застосування технології VPN
- Сегментування мережі і використання буферних ділянок
- Багаторівнева ідентифікація та аутентифікація
- Оперативний моніторинг і реагування на прояви вірусної активності і атак на системи підприємства

Детально розглянуті можливості та переваги використання технологіїVPNSSL для безпечного віддаленого управлінняSCADAсистемами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. P. Karlton The SecureSocketsLayer (SSL) ProtocolVersion 3.0 // 1-st. — RTFM, Inc., August 2011. — № 1. — P. 67.

2. Understanding SCADA systemsecurityvulnerabilities, Riptech, Inc. 2001 January

3. Астахов А. Искусство управления информационными рисками, - ДМК Пресс, GlobalTrust , 2009. - 312с

УДК 004.65+004.7(043.2)

О.М. Ковезюк
(Національний авіаційний університет, Україна)

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ КОМПЛЕКСНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПЕНСІЙНОГО ФОНДУ

Створення єдиного інформаційного простору, вимагають від сучасних організацій, до яких відноситься пенсійний фонд (ПФ), швидкого реагування на сучасні вимоги до інформаційних систем. Досягти необхідного ефекту можна тільки за рахунок впровадження прогресивних технологій. Без ефективних інформаційних технологій робота будь-якої організації практично неможлива.

Інформаційну систему також можна визначити як сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів (абонентів). Для обробки всіх таких даних ПФ потрібні певні організаційні і технічні засоби, тобто комплексна інформаційна система. Розуміння цінності інформації привело до необхідності її виникнення.

Комплексна інформаційна система забезпечує інформаційну підтримку всієї діяльності ПФ. Інформаційні системи, що використовують бази даних – це основний засіб постачання співробітників і керівництва ПФ своєчасною інформацією. Інформаційні системи, що використовують бази даних, підтримують цілісну, централізовану структуру даних, дозволяють позбутися від проблем надмірності і слабкого контролю даних. Оскільки ПФ має територіальне розташування, тому широко використовується архітектура віддаленого доступу до даних (архітектура «клієнт-сервер»).

Плануючи і регулюючи інформаційну архітектуру ПФ, необхідно забезпечити найбільш ефективне її управління. Ефективна інформаційна архітектура полегшує пошук і збереження інформації і робить її якіснішою.

Успішному впровадженню інформаційної архітектури сприяють наступні чинники: простота пошуку інформації; методи зберігання і витягання інформації; методи відкриття даних користувачами; наявність резервної або такої, що повторюється інформації; доступні для кожного типу інформації метадані; шаблони, використовувані для створення інформації; якість управління інформаційною архітектурою.

Завдання і принципи впровадження інформаційної архітектури залежать від типу створюваного вирішення даних завдань. При цьому необхідно дотримуватися наступних рекомендацій: при розробці інформаційної архітектури сайту порталу обчислювальної мережі можна зосередитися на використанні метаданих для класифікації контенту сайту, організації контенту на сайтах і в бібліотеках документів, доступності контенту сайтам порталу і шаблонах для створення контенту; при розробці інформаційної архітектури веб-сайту присутності в Інтернеті можна зосередитися на організації ієрархічних дочірніх сайтів і веб-сторінок на сайті, відкритті ієрархії для функцій переходу по сайту і простоті пошуку контенту на сайті [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Підсистема “Реєстри та НДІ”, вер.1.3.1. Експлуатаційна документація. ПФУ. К.: 2010.− 128 с.

УДК 004.65+004.7(043.2)

Є.Є. Кокорін
(Національний авіаційний університет, Україна)

ОПТИМІЗАЦІЯ ПРОЦЕСУ ПЕРЕДАЧІ ДАНИХ В КОМП'ЮТЕРНІЙ МЕРЕЖІ В РАМКАХ *TCP*-СЕАНСІВ

Сучасні мультисервісні телекомунікаційні мережі (ТКМ) розвиваються в напрямку впровадження концепції мереж наступного покоління *NGN (Next Generation Network)*. Використання ТКМ в структурі центру обробки даних організації забезпечують необхідну ефективність обміну даних. Ефективність ТКМ в основному залежить від результативності постановки та вирішення завдань, пов'язаних з управлінням мережевими ресурсами.

В основу *NGN* відповідно до рекомендації Міжнародного союзу електрозв'язку серії *Y 2000* закладається стек протоколів *TCP/IP*, в рамках якого важливу роль відіграють функції, що виконуються транспортним рівнем EMBBC. Зокрема, основними завданнями протоколу *TCP (Transmission Control Protocol)* є гарантія успішної доставки даних та забезпечення обміну даними між процесами, що виконуються на кінцевих системах (пристроях, вузлах), за допомогою служби обміну даними, що надається протоколом мережевого рівня. Протокол *TCP* є ефективним засобом управління потоками даних, мережі збалансованого навантаження.

Актуальним завданням є оптимізація *TCP*-сеансів у мультисервісних ТКМ, що пов'язано з необхідністю обґрунтованого вибору чисельних значень параметрів протоколу *TCP* і параметрів взаємодіючих з ним засобів боротьби з перевантаженнями, таких як *RED (Random Early Detection)*, *WRED (Weighted Random Early Detection)* і т.д.

В основу пропонуємого методу, пов'язаного з оптимізацією вибору параметрів протоколу *TCP* і алгоритмів *RED*/*WRED*, покладено рішення завдання оптимізації, в ході якого здійснюється мінімізація (максимізація) деякого цільового функціоналу втрат. З точки зору пошуку компромісу між необхідністю врахування фізики процесів передачі даних в рамках *TCP*-сеансів, з одного боку, і можливістю отримання чисельних результатів розрахунку в рамках відомих оптимізаційних процедур.

В ході постановки оптимізаційної задачі вироблено задоволення таких важливих вимог до протоколу *TCP*, як облік динамічності, багатопотоковості і мультирежимності процесу передачі даних; забезпечення узгодженості з роботою інших засобів боротьби з перевантаженням з можливістю вибору тієї чи іншої моделі блокування пакетів [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Стивенс У.Р.* Протоколы TCP/IP. Практическое руководство / У.Р. Стивенс; пер. с англ. и комментарии А.Ю. Глебовского. – СПб.: «Невский диалект»-«БХВ-Петербург», 2003. – 672 с.

УДК 004.73(042.4)

М.А. Колопац
(Национальный авиационный университет, Украина)

ИЕРАРХИЧЕСКАЯ МАРШРУТИЗАЦИЯ ПОТОКОВ РАЗНОРОДНОГО ТРАФИКА

Как известно [1], размер таблиц маршрутов, поддерживаемых маршрутизаторами, увеличивается пропорционально увеличению размеров сети. При этом требуется не только большее количество памяти для хранения этой таблицы, но и большее время центрального процессора для ее обработки. Кроме того, возрастает размер служебных пакетов, которыми обмениваются маршрутизаторы, что увеличивает нагрузку на линии. В определенный момент сеть может вырасти до таких размеров, при которых перестанет быть возможным хранение на маршрутизаторах записи обо всех остальных маршрутизаторах. Поэтому в больших сетях целесообразно применять иерархическую маршрутизацию, как это делается в телефонных сетях.

Рассмотрим пример маршрутизации в двухуровневой иерархии с пятью регионами. Полная таблица маршрутизатора состоит из 17 записей. При использовании иерархической маршрутизации таблица, как и прежде, содержит сведения обо всех локальных маршрутизаторах, но записи обо всех остальных регионах концентрируются в пределах одного маршрутизатора, поэтому размер таблицы маршрутов уменьшается с 17 до 7 строк. Чем крупнее выбираются регионы, тем больше экономится места в таблице.

Платой за уменьшение размеров таблицы маршрутов является увеличение длины пути. Поэтому оптимальное количество уровней иерархии для подсети, состоящей из N маршрутизаторов, равно $\ln N$. При этом потребуется $e \ln N$ записей для каждого маршрутизатора. Увеличение длины эффективного среднего пути, вызываемое иерархической маршрутизацией, довольно мало и обычно является приемлемым.

При этом следует различать иерархическую маршрутизацию исеть с иерархической структурой. В этом случае целесообразно использовать статистический подход с учетом статистики сетевого трафика, в частности, степени его самоподобия. По нашему мнению, достаточно общей оценкой является средняя сложность иерархической маршрутизации для двух узлов, равномерно распределенных внутри автономного (кругового) сегмента с нормированным радиусом. Нормировка осуществляется по физическому расстоянию между узлом-источником и узлом-получателем. Другими словами, можно применять геометрический подход к оцениванию сложности иерархической маршрутизации. При стремлении к бесконечности числа узлов внутри сетевого сегмента ошибка оценивания асимптотически приближается к нулю.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Tanenbaum, A.S.* Computer Networks, 5th Ed. / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 pp.

УДК 004.056.32

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

РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МОДЕЛІ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ

Інформація сьогодні є важливим елементом промисловості та однією з основ сучасного суспільства. Інформаційно-комунікаційні системи та мережі служать для розширення доступу користувачів до інформаційних ресурсів та надання широкого спектру сервісів. Але крім корисних функцій та надання різноманітних послуг інформаційно-комунікаційні системи та мережі можуть стати каналом несанкціонованого доступу до комп'ютерів користувачів. Тому комп'ютерні мережі та задачі інформаційної безпеки нерозривно пов'язані між собою та потребують постійного вдосконалення відповідно до зростаючого рівня загроз.

Ключовим елементом для дослідження комп'ютерних мереж є запропонована Міжнародною організацією зі стандартизації (ISO) модель взаємодії відкритих систем (OpenSystemsInterconnection, OSI) [1]. Модель OSI складається із семи рівнів, на кожному з яких існують загрози для інформаційної безпеки. Побудова комплексних систем захисту інформації потребує не тільки протидії загрозам на кожному рівні моделі OSI, а також створення цілісної багатошарової системи захисту інформації із розробкою політики безпеки, інструкцій та рекомендацій для користувачів інформаційно-комунікаційних систем та мереж [2]. Розроблена більше тридцяти років тому модель OSI потребує певного розширення та доповнення, з урахуванням проблем інформаційної безпеки [3].

Потужний функціональний комплекс сучасних інформаційно-комунікаційних систем та мереж надає велику кількість сервісів користувачам та має значну кількість вразливостей, протидія яким здійснюється на різних рівнях моделі OSI. Але застосування лише окремих механізмів та заходів захисту інформації не дає можливості побудувати повноцінну захищену комп'ютерну систему та описати її.

За результатами досліджень проведена класифікація вразливостей сучасних інформаційно-комунікаційних систем та мереж та заходів захисту інформації відповідно до семирівневої моделі OSI. Встановлено, щосемирівнева модель досить повно описує обмін інформацією у мережі, але не охоплює всього переліку проблем інформаційної безпеки. З метою побудови комплексних систем захисту інформації для інформаційно-комунікаційних систем та мереж пропонується розширити семирівневу модель до дев'ятирівневої – за рахунок восьмого рівня - рівняполітик та дев'ятого - рівнякористувачів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы (4-е издание). – Питер, 2010. – 943 с.

2. *Шаньгин В.Ф.* Защитакомпьютернойинформации. – М.:ДМК Пресс,2008. – 544 с.

3. *Kachold Lisa.* Layer 8 LinuxSecurity: OPSEC forLinuxCommonUsers, DevelopersandSystemsAdministrators // Linuxgazette.net,July 2009 (#164).

УДК 681.3

А.В. Корочкин, к.т.н.; О.В. Русанова, к.т.н.
(НТУУ "КПИ", Украина)

ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ С МНОГОЯДЕРНОЙ АРХИТЕКТУРОЙ

Современные параллельные системы основываются на использовании многоядерных процессоров. Это касается как производительных рабочих станций, так и мощных распределенных (кластерных) систем. Совершенствование многоядерных процессоров связано с увеличением числа ядер, использованием кэш-памяти различных уровней, а также системы связей ядер. Наряду с использованием общей памяти, планируется использование и прямой передачи данных между ядрами.

Это усложняет организацию вычислительных процессов в компьютерных системах с многоядерной архитектурой (КСМА), так как такая организация тесно связана с особенностями структуры КСМА. Кроме того, кластерные КСМА характеризуются большим количеством узлов и используемых в них ядер.

Современный подход к организации вычислений в КСМА основывается на использовании математических моделей вычислений, которые позволяют учесть особенности архитектуры КСМА и особенности используемой модели организации процессов и их взаимодействия [1].

Данная работа является развитием подхода, предложенного в [2], где в качестве основы для формирования математической модели вычислений в КСМА рассмотрено использование теории взаимодействующих последовательных процессов (CSP теории Ч.Хоара).

В работе рассматриваются вопросы построения и использования моделей вычислений для сложных КСМА. Использование CSP теории позволяет описать различные формы взаимодействия процессов с учетом используемой архитектуры КСМА. Основное внимание уделено проблеме возникновения и преодоления тупиковых ситуаций. Сформулирован ряд правил, позволяющих с помощью анализа математической модели избежать возникновения тупиковых ситуаций при организации взаимодействия процессов.

В работе показано, что предложенный подход к построению математической модели при разработке приложений для КСМА, позволяет сократить время их проектирования, а также повысить их качество за счет выявления на ранних этапах проектирования проблем, связанных с организацией взаимодействия процессов, таких, как возникновение тупиковых ситуаций.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Топорков В.В.* Модели распределенных вычислений / Топорков Виктор Васильевич. – М.: ФИЗМАТЛИТ, 2004. – 320 с.

2 *Растгу Садег.* Методи та засоби підвищення ефективності обчислень у кластерних системах з мультиядерною архітектурою: автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.05 “Комп’ютерні системи та компоненти” / Растгу Садег. - К., 2009.

УДК 004.73(042.4)

П.А. Кренц
(Национальный авиационный университет, Украина)

КРИТЕРИЙ ОПТИМИЗАЦИИ КАЧЕСТВА СЕРВИСА ПРИ ОБМЕНЕ ДАННЫМИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ АВИАКОМПАНИИ

Для нормального функционирования компании необходим обмен данными как между удалёнными офисами, находящимися в разных странах, так и между воздушными судами, в воздухе и на земле. При этом в распоряжении сотрудников и экипажей находятся различные средства передачи данных, такие как радиосвязь, сотовая связь, спутниковая связь и Интернет, которые привязаны к соответствующему оборудованию.

В данной работе предложен метод уменьшения затрат и повышения надежности благодаря объединению всех доступных каналов связи с применением программного коммутатора (*Softswitch*), под управлением алгоритма выбора оптимального для конкретных условий канала передачи данных [1].

Для решения поставленной задачи в качестве целевой функции предлагается использовать отношение "эффективность/стоимость" – достижение желаемого результата с минимально возможными издержками. В рассматриваемой задаче полезным результатом является передача данных с требуемым качеством сервиса, а издержками являются затраты на передачу данных по выбранному каналу. Таким образом, решается задача многокритериальной оптимизации, где первой целевой функцией является надежность, а второй – стоимость передачи блока информации:

$$\min_{i,j}\left\{\frac{1}{P_i^m + P_j^c}, S_i\right\};\ S_i > 0, P_i^m > 0, P_j^c > 0, i = 1,2,..,N, j = 1,2,..,M\ . \quad (1)$$

В качестве количественной оценки надежности возьмем величину, обратную вероятности отказа.

Предложенную формулировку задачи можно упростить путем ввода ограничения на минимально приемлемую надежность $R_{\min}$. Переведем критерий надежности из разряда целевых функции в область допустимых значений. Благодаря этому задача упростится и сведется к задаче дискретной оптимизации с одним критерием:

$$\begin{cases} \min\limits_i \{S_i\}; \\ \dfrac{1}{P_i^m + P_j^c} \ge R_{\min}; \end{cases} \quad S_i > 0, P_i^m > 0, P_j^c > 0, i = 1,2,..,N, j = 1,2,..,M; \quad (2)$$

Так как конечная цель работы заключается в оценке преимуществ предложенного метода оптимизации перед классическим подходом, подобное упрощение представляется вполне допустимым.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Кренц П. А.* Метод повышения эффективности обмена данными в информационно-вычислительной сети авиакомпании // Наукові записки УНДІЗ, №4(20), 2011. – С. 89–92.

УДК 338.484:519.6

И.П. Кудзиновская, к.т.н.
(Национальный авиационный университет, Украина)

СВОЙСТВА ДИАГОНАЛЬНО-ДОМИНИРУЮЩИХ МАТРИЦ И АЛГЕБРАИЧЕСКАЯ ПРОБЛЕМА СОБСТВЕННЫХ ЗНАЧЕНИЙ

Проблема чувствительности собственных значений и ее влияния на результирующую устойчивость решения весьма актуальна для матриц различных видов [1]. В теоретическом и прикладном матричном анализе наиболее часто рассматриваются две основные задачи:

- решение системы линейных уравнений $\mathbf{AX} = \mathbf{F}$, где $\mathbf{A}$ – матрица коэффициентов, $\mathbf{X}$ – вектор неизвестных, $\mathbf{F}$ – вектор правых частей;

- вычисление собственных значений $\lambda_i \ \ i = \overline{1, N}$, и собственных векторов $\mathbf{V}$ матрицы $\mathbf{B}$: $\mathbf{BV} = \lambda \mathbf{V}$.

В обоих случаях существенный интерес представляет поиск решений для матриц специального вида – так называемых матриц с доминирующей диагональю [2]. В данной работе рассмотрена задача оценивания спектрального радиуса матрицы со строгим диагональным преобладанием, т.е.

$$|a_{ii}| > \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}|, \ i = 1, 2, \ldots, n, \tag{1}$$

и слабым диагональным преобладанием:

$$|a_{ii}| \geq \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}|, \ i = 1, 2, \ldots, n. \tag{2}$$

Условие второго типа преобладания, по существу, совпадает с ослабленным условием регулярности Адамара $|a_{ii}| - \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}| \geq 0$. При выполнении условия (1) собственные значения локализованы в кругах Гершгорина [2], которые не соприкасаются друг с другом. Если выполняется условие (2), круги Гершгорина соприкасаются. Вследствие этого могут возникать ошибки локализации корней из-за случайных возмущений исходных данных и ошибок численного решения. В работе исследована асимптотическая устойчивость решений основных задач и установлено, что имеет место линейно пропорциональная зависимость ошибки решения от произведения амплитуд возмущений элементов матрицы и чисел обусловленности.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Vinogradov Nick*. An analysis of singularity of the matrices of priorities and sensibility of decisions as key performance indicators of the analytic hierarchies process // Nick Vinogradov, Vladimir Drovovozov, Alina Savchenko, Inna Kudzinovskaya. – Journal of Qafqaz University (Mathematics and Computer Sciences), Nr. 32, 2011. – PP. 40 – 48.

2. *Воеводин В.В.* Матрицы и вычисления / В.В. Воеводин, Ю.А. Кузнецов. – М.: Наука, 1984. – 320 с.

УДК 004.896:629

С.О. Кудренко, к.т.н.
(Національний авіаційний університет, Україна)

АНАЛІЗ ПРОЕКТУВАЛЬНИХ ЗАДАЧ ГЕТЕРОГЕННИХ АЕРОКОСМІЧНИХ КОМПЛЕКСІВ

Створити проект об'єкту означає вибрати (синтезувати) структуру об'єкту, визначити значення параметрів всіх його елементів і представити результати у встановленій формі. Проектну процедуру, що направлена на наукове обґрунтування, розробку та вибір структури об'єкта, називають структурним синтезом, а розрахунок (або вибір) значень параметрів елементів називають процедурою параметричного синтезу.

Головною метою автоматизації проектування є створення комплексних автоматизованих систем підготовки виробництва, виконуючих, окрім рішень задач структурного і параметричного синтезу, розрахунку значень параметрів елементів, вибір оптимальних конструкторських і технологічних рішень, компоновку елементів.Теорія автоматизації проектування знаходиться в стадії інтенсивного розвитку. Дотепер були автоматизовані, головним чином, різні обчислювальні операції, пов'язані з конструюванням. Накопичений досвід показує, що автоматизація проектування – це область ефективного використання комп'ютерних систем. В той же час стало вже ясно, що головний напрям тут — не автоматизація окремих етапів проектування, не розробка окремих алгоритмів інженерних розрахунків, а «зав'язка», наукове обґрунтування проекту, коли тільки промальовуються контури майбутньої конструкції, яка повинна відповідати початковим задумам. Такий підхід ґрунтується на прагненні досягти основної мети — підвищити якість і ефективність прийняття проектних рішень на ранніх етапах за рахунок застосування методів оптимального проектування.

Проектування виступає як комплексна проблема, в якій в складному взаємозв'язку переплітаються задачі синтезу, моделювання, аналізу, оцінки, оптимізації і відбору альтернатив. Для вирішення таких комплексних проблем необхідне застосування методології системного підходу. При використовуванні методології системного підходу для формалізації процесу проектування слід виходити з того, що специфіка складних об'єктів і процесів не вичерпується особливостями його складників і елементів, а відображена в характері зв'язків і відносин між ними. Розширення початкової бази за рахунок таких понять, як, наприклад, структура, функція, організація, зв'язок, відношення, надлишковість забезпечує певні переваги системного підходу перед традиційними методами досліджень і дозволяє створювати адекватніші дійсності моделі складних об'єктів і процесів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Горбань О.М.* Основи теорії систем і системного аналізу: Навчальний посібник / Горбань О.М., Бахрушин В.Є. – Запоріжжя: ГУ "ЗІДМУ", 2004. – 204 с.
2. *Кудренко С.О.* Чисельно-аналітичні методи автоматизованого проектування оптимальних векторних гетерогенних аерокосмічних комплексів/ Кудренко С.О. Проблеми інформатизації та управління. – К.: НАУ, 2010. – С. 113–118.

УДК 004.627(043.2)

К.О. Курінь, к.т.н.
(Національний авіаційний університет, Україна)

АЛГОРИТМ ВІДНОВЛЕННЯ ЗОБРАЖЕНЬ НА БАЗІ ІНВАРІАНТНИХ МЕТОДІВ СТРУКТУРНОГО КОДУВАННЯ

Головною функцією сучасних інформаційно-комунікаційних систем (ІКСМ) є організація оперативного й надійного обміну інформацією між абонентами й скорочення витрат часу на передачу даних. Для скорочення часу передачі даних розробляються спеціальні стандарти, протоколи й методи обробки, що формують інформаційне й програмно-математичне забезпечення функціонування ІКСМ.

Основними причинами завищених витрат часу на передачу даних є, по-перше, обмежені характеристики технічного забезпечення ІКСМ, а по-друге – обсяги цифрових даних, що обробляються та передаються в них.

Як відомо, найбільша частка інформації міститься відео- та графічних даних. Тому частка інформаційного потоку на базі графіки займає до 90% від загального потоку інформації, що обробляється в ІКСМ. Разом з тим суттєвим недоліком графічних даних є їх значний об'єм, який може змінюватися в широкому діапазоні.

Модернізація та установка сучасних технічних телекомунікаційних засобів частіше за все є високозатратним напрямом підвищення ефективності функціонування ІКСМ, а отже окрім удосконалення технічної бази необхідно проводити модернізацію інформаційного забезпечення ІКСМ.

Інтеграції технологій стиснення в системи передачі даних є одним з напрямів такої модернізації.

Таким чином одним з найважливіших завдань сучасної теорії інформації є розробка і реалізація нових методів стиснення, що забезпечують максимальний ступінь компресії з одночасною мінімізацією рівня спотворень даних у відновленій інформаційній структурі.

Метою дослідження є розробка алгоритму відновлення зображень на базі методу декодування двійкових послідовностей за кількістю бітових переходів (дКБП). При цьому до задач статті відноситься:

- визначення основних етапів процедури відновлення інформації декодером при формуванні декодованого потоку даних;
- оцінка розбіжності відновлених та вихідних зображень.

Наукова новизна дослідження полягає в наступному: вперше розроблено алгоритм відновлення зображень на базі інваріантного методу структурного кодування. В процесі дослідження були визначені основні етапи процедури відновлення інформації декодером при формуванні декодованого потоку даних.

Проведено оцінку розбіжності відновлених та вихідних зображень на підставі значення пікового співвідношення сигнал/шум. Отримані результати дозволяють дійти висновку, що запропонований алгоритм стиснення-відновлення кольорових зображень згідно значенню пікового співвідношення сигнал/шум вносить у відновлене зображення викривлення у допустимих межах чутливості людських органів

УДК 004.73(042.4)

А.И. Кустов
(Национальный авиационный университет, Украина)

ВЫБОР КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ФУНКЦИОНИРОВАНИЯ ПРИ ПРОЕКТИРОВАНИИ КОМПЬЮТЕРНЫХ СЕТЕЙ ДЛЯ ОТРАСЛИ ЗДРАВООХРАНЕНИЯ

Развитие ИКТ стало движущей силой современной медицины и стремительно изменяет как способы диагностики и лечения, так и саму методику взаимодействия врачей с пациентами и друг с другом, организацию лечения и восстановления здоровья. Мониторинг уровня применения ИКТ и современных медицинских технологий в медицинских учреждениях, уровня компьютерной грамотности медработников, а также использования медицинских услуг на основе ИКТ населением города нацелен на формирование информационной базы принятия решений в области управления здравоохранением [1].

Одним из наиболее важных аспектов при проектировании сетей является обеспечение достаточной пропускной способности для передачи больших объемов данных в пиковые периоды.

В табл. 1 приведены основные типы данных и соответствующая нагрузка на сеть. При проектировании сети необходимо учитывать требования к передаче больших объемов данных и регулярность доступа к данным.

Таблица 1

Текстовые данные		Изображения	
Рецепт, предписание лечащего врача	Десятки килобайт	Магнито-резонансная томография	около 500 Кб × 100 листов (400Мбит на каждое исследование)
Электронное письмо большого объема	Около 20 Кбайт	Рентгенография грудной клетки	около 30 Мб (каждый лист – около 240 Мбит)
		Эхокардиограмма	около 300 Кб × 10 листов (24 Мбит на каждое исследование)

Кроме того, при проектировании компьютерной сети для медицинского учреждения выдвигаются следующие основные требования:

- бесперебойная работа сети;
- пропускная способность и качество обслуживания (*QoS*);
- избыточность сети и меры по предотвращению системных сбоев;
- безопасность и надежность сети.

Для упрощения эксплуатации и повышения эффективности контроля сетевых устройств целесообразно использовать протокол *SNMP* (*Simple Network Management Protocol*) или *CMIP* (*Common Management Information Protocol*) в зависимости от объема циркулирующих в сети данных.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Илюшин Г.Я.*, Ершова Т.В. Использование ИКТ в здравоохранении // “Информационное общество”, 2004, вып. 3–4, сс. 99–109.

УДК 004.057.4

С. Б. Литовка; А.І. Гуля; Д.Б. Бур'янцев
(Національний авіаційний університет, Україна)

ПЕРЕХІД НА ПРОТОКОЛ IPv6

Протокол IP використовується для забезпечення обміну даними в комп'ютерних мережах. Кожному комп'ютеру присвоюється IP-адреса, унікальна для глобальної або локальної мережі. На даний момент більшість вузлів в Інтернеті використовують протокол IP четвертої версії (IPv4), в якому довжина IP-адреси складає 4 байти (32 біт), а сама адреса представляється у вигляді чотирьох десяткових чисел, розділених крапками. Однак кількість комп'ютерів у світі зростає, а ось доступних IP-адрес більше не стає. Для вирішення цієї проблеми було впроваджено протокол IPv6.

Протокол IPv6 був розроблений Інженерною радою Інтернету (IETF), відповідальною за розвиток протоколів і архітектури Всесвітньої мережі. На відміну від попередньої версії, довжина адреси в протоколі IPv6 становить 128 біт, що дозволяє забезпечити унікальними адресами більшу кількість вузлів. На даний момент нову версію протоколу використовують понад 9000 мереж у всьому світі.

Протокол IPv6 не тільки збільшує діапазон доступних IP-адрес. З нового протоколу були прибрані речі, які ускладнюють роботу маршрутизаторів, зокрема, контрольна сума і розбиття пакету на частини. Були впроваджені і деякі інші поліпшення.

Розробка нового протоколу почалася ще в 90-х, коли стало ясно, що вичерпання IPv4-адрес неминуче. Всередині Google перехід на IPv6 почав здійснюватися вже в 2008 році. У червні 2011 року відбувся Міжнародний день IPv6 - захід, присвячений тестуванню готовності до масового переходу на новий протокол. 6 червня 2012 відбувся всесвітній запуск нової версії протоколу IP.

Що це означає? Більшість компаній, так чи інакше пов'язаних з Інтернетом і мережами, будуть поступово переходити на новий протокол.

Проте повна відмова від використання протоколу IPv4 не планується, тому що величезна кількість пристроїв поки що не підтримують протокол IPv6. Обидва протоколи будуть використовуватися паралельно, просто частка трафіку IPv6 у порівнянні з IPv4 буде поступово збільшуватися. Були розроблені спеціальні технології, які здійснюють перетворення адрес в обох напрямках і таким чином дозволяють мережам IPv6 здійснювати комунікацію з мережами IPv4, а саме: Teredo, IPv6 Rapid Deployment, Intra-Site Automatic Tunnel Addressing Protocol.

Перехід на протокол IPv6 - це тільки питання часу. Як ми говорили, протокол IPv4 не зникне найближчим часом, але частка таких адрес в мережі поступово зменшуватиметься. Нове обладнання і нові версії операційних систем за замовчуванням підтримують IPv6.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Новини* інформаційних технологій українською мовою. [Electronic resource] / Інтернет ресурс. – Режим доступу: http://it-tehnolog.com – Загол. з екрану.

УДК 004.046+004.27+004.75

А.В. Луговой, к.т.н.;
Ж.Ю. Зеленцова
(Кременчугский национальный университет им. М.Остроградского, Украина)

УНИФИЦИРОВАННАЯ ТЕХНОЛОГИЧЕСКАЯ МОДЕЛЬ КОНВЕРГЕНТНОЙ ИНФРАСТРУКТУРЫ

Развитие мировой глобальной сети – информационного вычислительного пространства (ИВП) – инициировало поиск новых решений в сфере управления и организации доступа к её составляющим. За последние десятилетия сформировалось архитектурное видение ИВП, но унифицированы и согласованы только отдельные его компоненты [1].

Современная архитектурная идея организации ИВП состоит в создании единого логического пространства независимо от географического расположения вычислительных ресурсов. Подобный системный подход реализован в рамках конвергентной инфраструктуры отдельных поставщиков решений. Созданы глобальные сервисные конвергентные системы – Amazon Web Services, Windows Azure, Apple iCloud, Google Cloud Platform, Oracle (Facebook), а также корпоративные: WMware, HP, Cisco, Sun, Dell.

В настоящей работе сделана попытка объединить все использованные технологические решения в рамках унифицированной технологической модели конвергентной инфраструктуры (рис. 1). Предложенная модель определяет единый подход к технологическому развертыванию систем, согласованию решений и последующей стандартизации.

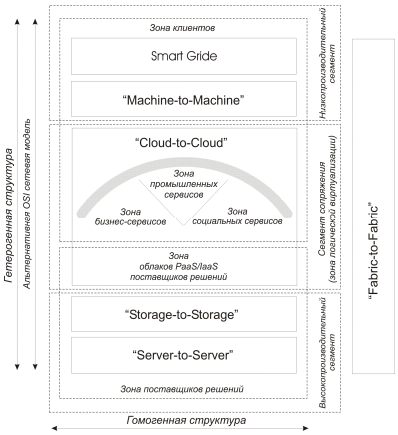


Рис. 1. Технологическая модель конвергентной инфраструктуры

Она получена на основе анализа крупнейших конвергентных решений и описывает конвергентные системы как совокупность взаимодействующих компонентов путем раскрытия их сущности, функциональности и характера взаимодействия. Модель может рассматриваться как эталонная базовая. Она может быть использована для разработки согласованных конвергентных решений и последующей стандартизации конвергентной инфраструктуры.

В рамках модели объединено два вычислительных сегмента – высокопроизводительный и низкопроизводительный. Речь идет об обеспечении доступа пользователей посредством низкопроизводительных ресурсов – PC и non-PC устройств – к высокопроизводительным ресурсам – суперкомпьютерам и клас-

терам, крупным хранилищам данных. Доступ осуществляется с помощью сервисного слоя, который является одновременно слоем сопряжения и виртуализации.

Виртуализация впервые начала применяться для обеспечения разделенного доступа пользователей к вычислительным ресурсам мейнфрейма. Портируемость программных приложений в гетерогенных средах и сопряжение разных аппаратных интерфейсов в большинстве случаев обеспечивается также с помощью виртуализации. Виртуализацию принято разделять на аппаратную и логическую. Слой виртуализации конвергентной инфраструктуры по аналогии также разделен на два сегмента – зону аппаратной и зону логической виртуализации. Функциональность сегментов обеспечивается преимущественно с помощью двух технологий – технологии вычислительной ткани (*fabric computing*) и технологии облачных вычислений (*cloud computing*) соответственно [2].

В зоне аппаратной виртуализации вычислительная ткань образует коммутируемые шины аппаратных ресурсов с общим адресным пространством и протоколами унифицированного взаимодействия. Технология позволяет создавать высокоскоростные гомогенные вычислительные структуры различных топологий, не ограниченные реализацией отдельных компонентов, их физической конфигурацией и географическим положением. В настоящий момент в рамках конвергентных решений широко применяются ткани, объединяющие серверы – вида «server-to-server» – и системы хранения – модели «storage-to-storage». Для устройств низкопроизводительного сегмента разрабатывается стандарт M2M с топологией объединения «machine-to-machine».

В вычислительную ткань также могут быть объединены абстракции и компоненты зоны логической виртуализации. Для коммутации сервисов и упрощения процесса получения услуг в зоне виртуализации могут создаваться ткани с топологией «cloud-to-cloud», объединяющие вычислительные облака, а также ткани с топологией «fabric-to-fabric» для объединения отдельных решений в открытую конвергентную инфраструктуру с соответствующей сетевой моделью взаимодействия на базе вычислительных тканей. К обязательным тканям, обеспечивающим портируемость конвергентных решений в открытой инфраструктуре, относятся коммутационные шины типов: «server-to-server», «storage-to-storage», «cloud-to-cloud», «machine-to-machine», а для объединения конвергентных решений - «fabric-to-fabric». Таким образом, в вертикальном разрезе конвергентная инфраструктура является гетерогенной структурой, а по горизонтали – гомогенной, что значительно упрощает доступ и к ее компонентам, и повышает его скорость.

По определению в вычислительную ткань могут быть объединены любые компоненты одного типа. Прикладная модель конвергентной инфраструктуры или отдельного облака помимо предложенных базовых может иметь произвольное число функциональных вычислительных тканей.

Наличие зон высокопроизводительных и низкопроизводительных ресурсов предполагает разделение инфраструктуры на зону клиентов и зону поставщиков решений. Клиентская зона разделена на три основных сегмента – зону бизнес-сервисов, социальную и промышленную зону – и предоставляет сервисы виртуа-лизации в рамках этих сегментов. Архитектура предложенной технологической модели позволяет обеспечить прозрачный высокоскоростной доступ к любым плементам сети и неограниченную масштабируемость решений. Может быть фун-кционально расширена за счет универсальной модели облаков и её прикладных реализаций.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Луговой А.В.. Зелениова Ж.Ю.. Луговая О.В.* «Эра мегаданных. Состояние и эволюция мирового информационно-вычислительного пространства». // Вісник Кременчуцького національного університету імені Михайла Остроград-ського. – Кременчук: КрНУ, 2012. – Випуск 1/2012 (72). Частина 1. – С. 36-42.
2. *Stephen Prentice. Gvanee Dewnarain.* “The Future of the Internet: Fundamental Trends, Scenarios and Implications to Hee”, Gartner, 2012. - http://www.gartner.com/technology/core/products/research/topics/emergingTrendsTechnologies.jsp.

УДК 004.046+004.27+004.75

А.В. Луговой, к.т.н.;
Ж.Ю. Зеленцова
(Кременчугский национальный университет им. М.Остроградского, Украина)

УНИВЕРСАЛЬНАЯ ТЕХНОЛОГИЧЕСКАЯ МОДЕЛЬ ОБЛАКА

Развитие и широкое распространение технологии облачных вычислений обуславливают необходимость разработки универсальной технологической модели облака и последующей её стандартизации.

Первый опубликованный стандарт представлен NIST, в нем содержится несколько базисов, определяющих универсальную архитектуру облака [1]. В разрабатываемой модели учтены пять особенностей облака: самообслуживание по требованию, глобальный сетевой доступ, объединение ресурсов в рамках гетерогенных сред, их эластичность, а также автоматическое предоставление услуг непрерывно, в неограниченных объемах и неограниченно по времени. Рассмотрены три сервисные модели облаков: «Программное обеспечение как услуга» (Software as a Service, SaaS), «Платформа как услуга» (Platform as a Service, PaaS), «Инфраструктура как услуга» (Infrastructure as a Service IaaS). Трехслойная архитектура облака NIST подразумевает: сервисный слой, слой абстракций и контроллинга, слой физических ресурсов и услуг. Согласно стандарту NIST доступ к облаку осуществляется с помощью виртуальной машины.

В работе предложена более полная универсальная технологическая модель облака (рис.1). В модели учтено, что вычислительные облака – это, прежде всего, область сервис-ориентированной виртуализации аппаратных и логических ресурсов. Их клиентами на условиях самообслуживания могут быть конечные пользователи, осуществляющие доступ посредством низкопроизводительных устройств, устройства, сервисы и облака [2, 3].

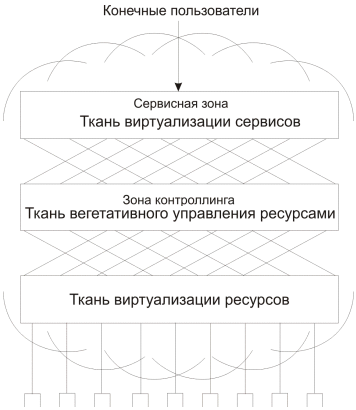


Рис. 1. Универсальная технологическая модель облака

Вычислительные облака являются частью конвергентной инфраструктуры, где прозрачный доступ ко всем компонентам сети обеспечивается за счет применения технологии вычислительной ткани (*fabric computing*) [4]. Последняя образует высокоскоростные коммутационные шины аппаратных и логических ресурсов с общим адресным пространством. Помимо базисных тканей типа «server-to-server», «storage-to-storage» применяются ткани программных приложений (AppFabric,

Windows Azure), сетевых сервисов и т.д. Таким образом, основу универсальной технологической модели облака составляет вычислительная ткань.

Предложенная модель содержит три базовых вычислительные ткани. Одна из них виртуализирует аппаратные и логические ресурсы, с целью предоставления услуг клиентам облака. Вторая ткань представляет собой обслуживающий слой (зона контроллинга), в котором применяется агентно-ориентированное программирование. Агенты реализуют вегетативные функции, значительно улучшающие автономность облака. Третья ткань является сервисно-ориентированной (сервисная зона) и обслуживает конечных пользователей. Доступ к облаку обеспечивается с помощью интерфейса API и вспомогательных облачных служб, а также интерфейса VM (Virtual Machine). Применение агентно-ориентированного программирования позволяет создавать интеллектуально-автономные среды (ИАС) виртуализации в облаке.

Применение агентно-ориентированного подхода в облаке объясняется необходимостью наличия автономных функций в открытых сетевых средах. К основным свойствам агентов относят: автономность, адаптацию к внешним условиям, способность к самостоятельным действиям, гомогенность и гетерогенность, подразумевающие обработку как гомогенных, так и гетерогенных структур [5]. Это также отражает сущность технологической модели конвергентной инфраструктуры. Агенты, как и виртуальные машины, могут перемещаться на другую сервисную площадку, что является проявлением эластичности сервисных функций.

Предложенная универсальная технологическая модель облака полностью соответствует опубликованным стандартам в области облачных вычислений, сервисным моделям, а также особенностям применения в развернутых на негодняшний день конвергентных решениях Amazon Web Services, Windows Azure, Google Cloud, Apple iCloud и др. Она создана на основе системного анализа глобальных конвергентных решений, технологической модели конвергентной инфраструктуры и базовых принципов формирования вычислительной архитектуры.

Технологическая модель облака предполагает полную инфраструктурную интегрируемость в предлагаемую унифицированную модель конвергентной инфраструктуры, является её неотъемлемой частью и функциональным расширением.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. «NIST Cloud Computing Standards Roadmap» (NIST-SP 500-291), NIST, July 2011. –http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909024, 2012-02-28.
2. *Луговой А.В., Зелениова Ж.Ю.* Вычислительная архитектура пятого поколения. Принцип гипервиртуализации. Збірник наукових праць Міжнародної заочної конференції «Пошук концептуальних засад розвитку сучасних наук». Частина 2. – К.: Центр Наукових публікацій, 2012. – С.100-105
3. *Луговой А.В., Зелениова Ж.Ю.* «Подходы и принципы разработки гибридного облака системы мониторинга с многомерными объектами исследова-ния». // Вісник Кременчуцького національного університету імені Михайла Остро-градського. – Кременчук: КрНУ, 2012. – Випуск 6/2011 (71). Частина 1. – С.56-62
4. *Stephen Prentice, Gyanee Dewnarain*, "The Future of the Internet: Fundamental Trends, Scenarios and Implications to Hee". Gartner, 2012. - http://www.gartner.com/technology/core/products/research/topics/emergingTrendsTechnologies.jsp.
5. *Yoav Shoham*, "Multiagent systems: Algorithmic, Game-Theoretic, and Logical Foundations = Artificial Intelligence: A Modern Approach". – Cambridge: Cambridge University Press, 2009. – 504 c.

УДК 004.73(042.3)

В.В. Лукашенко, к.т.н.
(Національний авіаційний університет, Україна)

СТОХАСТИЧНІ АЛГОРИТМИ МАРШРУТИЗАЦІЇ У МЕРЕЖАХ З ВИСОКОЮ ТОЛЕРАНТНІСТЮ ДО ЗАТРИМОК

Мережі з високою толерантністю до затримок (мережі, толерантні до затримок, Delay-Tolerant Networks) – це інформаційно-обчислювальні мережі спеціального призначення, основною особливістю яких є можливість зберігати накопичені дані невизначений час та забезпечувати гарантії їх доставляння, незважаючи на раптові розриви з'єднань або тимчасову відсутність мережних та комутаційних вузлів [1]. За таких умов функціонування задачі мережного управління та маршрутизації є стохастичними за визначенням. Процеси визначення маршруту представляють собою марківські процеси дифузійного типу.

У свою чергу, процес просування блоків даних (bundles) можна представити як випадковий процес, керований стохастичним диференційним рівнянням [2]. При цьому кількість апріорної інформації про параметри та стан мережі може змінюватися у широких межах. Крайні випадки, які на практиці не можуть мати місця – це наявність повної апріорної інформації та повна відсутність будь-якої інформації.

При достатній кількості апріорної інформації (коли можна зробити обґрунтовані передпосилання про клас імовірнісних розподілів та апріорні імовірності наявності та відсутності мережного вузла) доцільно застосовувати для визначення маршрутів доставляння даних байєсівські методи з адаптацією в умовах параметричної невизначеності.

При наявності мінімальної апріорної інформації, коли неможливо зробити припущення навіть про клас імовірнісних розподілів параметрів мережі (за умов так званої непараметричної невизначеності) найбільш придатними методами визначення маршрутів доставляння даних є методи адаптивного максимально правдоподібного оцінювання або використання інформаційно-ентропійних оцінок. При цьому накопичену на поточних кроках оцінювання інформацію доцільно вводити в алгоритми адаптивного керування та визначення маршрутів доставляння даних, що, по суті, зводиться до методу дуального управління А.А. Фельдбаума.

Таким чином, задачі аналізу ефективності мереж, толерантних до затримок, по суті, є задачами теорії імовірності та математичної статистики.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Jimmy Ray*. Delay Tolerant Networking: How to use Twitter and Hulu on long Space Missions to Mars [Електронний ресурс]. Режим доступу: http://www.networkworld.com/community/node/43557 [Feb.16, 2011]
2. *Дынкин Е.Б.* Управляемые марковские процессы и их приложения. / *Е.Б. Дынкин, А.А. Юшкевич* – М.: Наука, 1975. – 338 с.

УДК 656.7.052.001.76(043.2)

М.В. Лупандін, к.т.н; Ю.В. Лавриненко;
І.А. Безкровна; І.М. Юр'єва
(Національний авіаційний університет, Україна)

АВТОМАТИЗАЦІЯ ЗАДАЧ АНАЛІЗУ ТА КОНТРОЛЮ ІНТЕНСИВНОСТІ ПОВІТРЯНОГО РУХУ

Для автоматизації задач аналізу та контролю інтенсивності польотів в зоні відповідальності авіапідприємств, що виконує аеронавігаційне обслуговування повітряного руху, розроблено програмне забезпечення автоматизованого робочого місця «Інтенсивність», В програмі формуються SQL запити до бази даних і відображаються результати їх виконання для подальшого аналізу та контролю використання повітряного простору(ПП).

У програмі використані стандартні методи, створення, виклику, відображення форм управління і виводу, що надаються середовищем DELPHI. До спеціально розроблених методів можна віднести алгоритм динамічного формування SQL запиту на підставі заданих параметрів.

Структурно програма складається з модулів, які виконують функції управління, відображення, діалогу і спеціальні модулі, що забезпечують функціональність програми. Модулі управління забезпечують вибір параметрів управління програмою. Модулі відображення, відповідно, забезпечують виведення вихідної інформації у виді доступному для аналізу. Модулі діалогу забезпечують вибір або вихід із різних станів. Спеціальні модулі служать для забезпечення функціонального призначення програми.

Програма "ІНТЕНСИВНІСТЬ" реалізована у вигляді набору форм управління SDI (SIMPLE DOCUMENT INTERFACE) додатком. Це означає, що якщо якась форма викликає форму-наследник, то інша форма не може бути відкрита до повернення у форму-предок. Положення на екрані і розмір усіх форм управління може змінюватися стандартними методами WINDOWS.

Вхідними даними програми «Інтенсивність» є база даних з інформацією про структуру ПП та рух повітряних суден, яка має умовно- постійний і змінний характер і сховище даних DATA WARE HOUSE, створене на її основі.

База даних виконана на СУБД ORACLE. Доступ виконується через клієнтську частину ORACLE, яка повинна бути встановлена на робочій станції, з якої виконується програма.

Вихідними даними програми «Інтенсивність» є відображення планованої та фактичної інтенсивності повітряного руху по елементах ПП, відображення списків конкретних рейсів, що виконуються в заданий період по усіх елементах ПП та аеропортах, відображення параметрів польоту для обраних рейсів, кількості планованих та фактичних зльотів і посадок по аеропортах, візуальні вихідні форми програми і можливість перетворення їх у формати MICROSOFT EXCELL, які надають можливість їх перетворення і виведення твердої копії.

Користувачу програми «Інтенсивність» надана можливість зіставляти планові і фактичні дані, для подальшої оцінки безпеки повітряного руху.

УДК 004.65+004.7(043.2)

Б. Г. Масловський, к.т.н.;
В.І. Дрововозов, к.т.н.
(Національний авіаційний університет, Україна)

КОМП'ЮТЕРНА СИСТЕМА ЯК ЛЮДИНО-МАШИННИЙ КОМПЛЕКС

Забезпечення впровадження сучасних технологій проектування засобів комп'ютерних систем (КС) на усіх етапах розробки являється актуальною проблемою.

При проектуванні нової і модернізації існуючої техніки особливо важливо заздалегідь і з максимально доступною повнотою враховувати можливості і особливості людей, які нею користуватимуться. При використанні та розвитку технологій проектування технічних систем взагалі і комп'ютерних систем зокрема дуже важливе значення має враховувати взаємодію людини з КС та її компонентами. Тому значну увагу треба приділяти питанням діяльності людини у людино-машинних системах та інженерно-психологічному і ергономічному проектуванню інтерфейсів «людина – машина» [1]. Усвідомлення цього вимагає, по-перше, нового погляду на склад самого об'єкту проектування – у даному випадку комп'ютерної системи, по-друге застосування новітніх методів і технологій проектування КС та її складових.

На основі аналізу сучасних інформаційних джерел, пов'язаних з технологіями ергономічного проектування засобів комп'ютерних систем запропоновано така структура КС, в якої наряду з традиційними складовими входять користувач (оператор або інша КС), а також інтерфейс користувача (рис. 1).

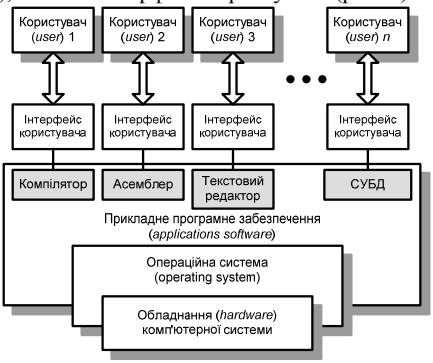


Рис. 1. Структура комп'ютерної системи

Віднесення людини-користувача до компонентів КС сучасна реальність: будь-який користувач фактично стає частиною обчислювальної системи в процесі своєї роботи. Врахування особливостей пропонуємої структури при використанні сучасних технологій ергономічного проектування КС та її складових має важливий вплив на ефективність процесу проектування.

ВИКОРИСТАНІ ДЖЕРЕЛА

1) *Шлаен П. Я.* Эргономика для инженеров: Эргономическое обеспечение проектирования человеко-машинных комплексов: проблемы, методология, технологии / П. Я. Шлаен, В. М. Львов. – Тверь: ТвГУ, 2004.

УДК 004.7 (043.2)

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

МОДЕЛЬ КОНТРОЛЮ ДОСТУПУ І АРХІТЕКТУРА СИСТЕМИ БЕЗПЕКИ ДЛЯ ХМАРНИХ ОБЧИСЛЕНЬ

Модель контролю доступу для SaaS повинна враховувати кілька сервіс-провайдерів, користувачів та сервіс-ресурсів. На рис. 1 представлено динамічну модель контролю доступу з суб'єктами і об'єктами на основі множини атрибутів (MADAC) для підтримки складних умов.

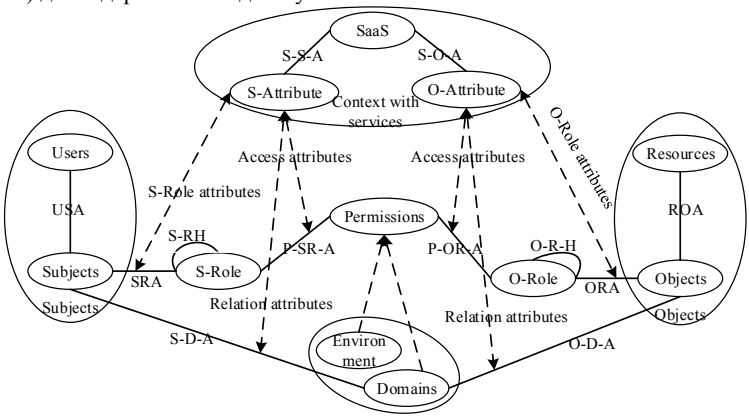


Рис. 1. MADAC для хмарних обчислень.

Користувачі включають у себе унікального користувача, користувачів групи або організаторів. Вони відображаються на відповідний суб'єкт в MADAC.

В якості запропонованого сценарію виконання MADAC представлено загальну архітектуру системи контролю доступу. Ідентифікація і контроль доступу у SaaS повинні підтримувати два інтерфейси для користувачів і постачальників SaaS для обробки кожної дії. Три шари архітектури: користувацький SaaS шар, шар контролю доступу і шар послуг. 1) користувацький SaaS шар. Він складається з чотирьох елементів групи. UID = {UserID, UserGroupID, UserEPID, PIN}. 2) шар контролю доступу: він відповідає за обробку авторизації користувачів і політику контролю. 3) SaaS шар постачальника послуг: коли кілька типів SaaS завантажені і опубліковані, даний шар показує загальний інтерфейс для шару контролю доступу. Постачальник SaaS відповідає тільки за послуги публікації і надання управління.

УДК 004.453,3:044,738(043,2)

С.С. Мащенко; С.С. Балацкий;
Е.Е. Бондарь; А.А. Соляр
(Национальный авиационний университет, Украина)

АНАЛИЗ ТЕХНОЛОГИИ VPN И ЕЕ ПОСТРОЕНИЕ

Из пункта А в пункт Б необходимо передать информацию таким образом, чтобы к ней никто не смог получить доступа. Вполне реальная и часто возникающая на практике ситуация, особенно в последнее время. В качестве пунктов А и Б могут выступать отдельные узлы или целые сегменты сетей. В случае с передачей информации между сетями в качестве защитной меры может выступать выделенный канал связи, принадлежащей компании, информация которой требует защиты. Однако поддержание таких каналов связи - очень дорогое удовольствие.Проще и дешевле, если информация будет передаваться по обычным каналам связи (например, через Интернет), но каким-либо способом будет отделена или скрыта от трафика других компаний, циркулирующего в сети. Но не следует думать, что потребность в конфиденциальной передаче информации возникает только в глобальных сетях. Такая потребность может появиться и в локальных сетях, где требуется отделить один тип трафика от другого (например, трафик платежной системы от трафика информационно-аналитической системы).Целью данной работы является изучение защиты нескольких локальных сетей, связанных через Internet, с Proxy-серверами и Координаторами на них. Объектом исследования является защита локальных сетей, связанных через Интернет. Одним из основных методов защиты локальных сетей, связанных через Интернет является использование технологии VPN, возможности и реализация которой будут рассмотрены в данной работе. В данной работе была сформирована структура защищённой сети, а также произведена настройка Координатора в соответствии с предъявленными требованиями.

Для настройки Координатора потребовалось проанализировать режимы безопасности сетевых интерфейсов - правила, в соответствии с которыми производится фильтрация трафика.

Нами были выбраны подходящие настройки интерфейса и правила фильтрации для исходной незащищенной сети.

И, в самом конце рассмотрели тонкости взаимодействия Proxy-сервера и Координатора и выбрали возможные режимы работы, которые, при необходимости, можно менять.Таким образом, в было завершено формирование защищённого туннеля для наших сетей.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Конев И.Р., Беляев А.В. Информационная безопасность предприятия - СПб: БХВ - Петербург 2007. - 752с.

2. *Биячуев Т.А. под ред. Л.Г. Осовецкого* Безопасность корпоративных сетей. - СПб: СПб ГУ ИТМО, 2006 - 161 с.

УДК 004.048

А.З. Меликов, член-корр. НАНА, д.т.н.
(НАА, Азербайджан)

ЧИСЛЕННЫЙ ПОДХОД К РАСЧЕТУ ХАРАКТЕРИСТИК МОДЕЛЕЙ СОТОВЫХ СЕТЕЙ СВЯЗИ

В последние годы появились работы [1]-[3], в которых изучаются модели сотовых сетей связи (ССС) с различными стратегиями доступа. В них изучены модели без очередей. В ССС различаются четыре типа вызовов: хэндовер речевые вызовы (hv-вызовы), новые речевые вызовы (ov-вызовы), хэндовер вызовы данных (hd-вызовы) и новые вызовы данных (od-вызовы).

В настоящей работе предложен унифицированный численный подход к исследованию моделей ССС при различных стратегиях доступа. Предполагается, что имеется возможность организации очереди вызовов данных обоих типов. Здесь вводятся параметры, которые учитывают требования разнотипных вызовов. Разные вызовы предъявляют разные требования к показателям качества обслуживания (Quality of Service, QoS). Для решения задач выбора надлежащих значений параметров используемых стратегий доступа необходимо разработать методы расчета указанных показателей. Предложенный подход позволяет вычислить значения искомых показателей QoS при любых значениях нагрузочных и структурных параметров изучаемых сетей. Другим отличающимся моментом этой работы от работ [1]-[3] состоит в том, что здесь для анализа системы используется подход, основанный на теории фазового укрупнения состояний двумерных цепей Маркова [4]. С использованием этого подхода разработаны простые вычислительные процедуры для нахождения всех показателей QoS изучаемой системы.

Важным достоинством предложенного подхода состоит в том, что он может быть использован для моделей любой размерности, так как искомые показатели вычисляются с помощью явных формул. Кроме того, он может быть использован для изучения моделей с конечными и бесконечными очередями, а также для моделей, в которых возможны нетерпеливость вызовов в очереди.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Carvalho G.H.S., Martins V.S., Frances C.R.L., Costa J.C., Carvalho S.V.* Performance analysis of multi-service wireless network: An approach integrating CAC, and buffer management // Computers and Electrical Engineering. 2008. Vol.34, P. 1235–1252.

2. *Ahme M.H.* Call admission control in wireless networks: A comprehensive survey // IEEE Communication Surveys & Tutorials. 2005. Vol.180, no.1. P.50-69.

3. *Ghaderi M., Boutaba R.* Call admission control for voice/data integration in broadband wireless networks // on Mobile Computing. 2006. – Vol.5, no.3. P. 193–207.

4. *Ponomarenko L., Kim C.S., Melikov A.* Performance analysis and optimization of multi-traffic on communication networks. – Heidelberg, Dordtrecht, London, New York: Springer, 2010. – 208 p.

УДК 004.048

А.З. Меликов, член. корр. НАНА, д.т.н.; Б.Г. Исмайлов, к.т.н.
(НАА Азербайджан)

АНАЛИЗ РЕЗУЛЬТАТОВ ИМИТАЦИОННОЙ МОДЕЛИ. ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ РАСПРЕДЕЛЕННОЙ СЕТИ

Проблема защиты информации в сети с каждым днем становится более значимой. Большинство негативных воздействий на распределенные сети (РС) осуществляется извне, в основном из глобальной сети Internet, превратившуюся не только в средство поиска информации, но и в средство распространения вирусов, троянских коней и других вредоносных программ. Кроме того, защита информации в РС усложняется из-за различных причин, как большое число пользователей и их переменный состав. Анализ показывает, что защита на уровне имени и пароля пользователя недостаточно для предотвращения входа в сеть посторонних лиц, а большое число потенциальных каналов проникновения в сеть еще усложняет защиту информации в сети. Порождаются новые проблемы связанные с защитой информации, когда осуществляется соединение с другими сетями и подключения к сети Internet и, следовательно, при этом увеличивается возможность поражения сети компьютерными вирусами [1]

Анализ показывает, что перечисление возможных угроз сети практически невыполнимо из за нескончаемых их количеств. Поэтому задача определения характеристик систем зашиты информации (СЗИ) решается в рамках проведенные нами классификации возможных угроз сети.

При решении проблемы связанной с защитой информации в РС предлагается решение задачи по определению оптимальной программно-технической структуры системы защиты информации, рассмотрением ее как многоканальная система массового обслуживания (СМО). Рассмотренная СЗИ создается между РС и глобальной сетью, которые инспектируют и фильтруют проходящую через них информацию. Такая структура позволяет резко снизить угрозу несанкционированного доступа в РС извне, применяя при этом способ маскарада (masquerading), когда весь исходящий из РС трафик посылается от имени СЗИ делая РС практической невидимой. С целью защиты информации в РС от внешних воздействий возникают задачи организации СЗИ имеющие современные программные технические структуры. СЗИ позволяет вести контроль над передачей информации и комплексную защиту информации от различных воздействий. СЗИ могут содержать комплекс программ, который требуют определенный объем памяти.

Периодическое проведение анализа эффективности характеристики СЗИ является одним из основных задач РС. Совершенствование и оптимизация характеристик СЗИ позволяет разработать достаточно простую и эффективную СЗИ, которую трудно преодолеть даже опытному злоумышленнику.

В работе проведены анализ результатов модели имитации исследования СЗИ как СМО. Модели имитации построены с применением языка моделирования General Purpose Simulation System.Проведены эксперименты и получены результаты. Эти результаты могут быть применены при построении РС различного назначения.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / Под ред.В.Ф. Шаньгина.-2-е изд., перераб. и доп. - М.: Радио и связь, 2001. - 376 с.

УДК 621.396.2: 621.396.931

И.В. Мишарин
(Национальный авиационний университет, Украина)

ПОСТАНОВКА ЗАДАЧИ СИНТЕЗА ОБНАРУЖИТЕЛЯ-ИЗМЕРИТЕЛЯ ДЛЯ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

В общем случае в задаче синтеза системы съема информации беспилотным летательным аппаратом (БПЛА) ставится цель получения схемы измерителя, который определяет текущие координаты наблюдаемого объекта. С учетом характера решаемой задачи синтезированное устройство представляет собой обнаружитель – измеритель сигнала точечной цели на фоне пространственно-распределенных помех [1].

В соответствии с этим представим обобщенную структурную схему замкнутой системы измерения местоположения объекта (рис. 1). Система содержит следующие блоки:

1 – обнаруживаемый объект;

2 - нелинейный преобразователь вектора сигналов $S[t, X(t)]$;

3 – устройство приема и оптимальной обработки сигналов;

4 – формирователь управляющих сигналов.

Введем обозначения: $\mathrm{X}_{\ddot{\imath}}(t)$ - вектор координат – переменных состояния; $U_{â}(t)$ - возмущения, действующие на объекты; $N(t)$ - вектор возмущений (помех); $M_{\ddot{\imath}}(t)$ - совокупность сигналов, определяющих параметры обнаружителя; $W_{ó\ddot{\imath}}(t)$ - вектор управляющих сигналов; $X(t) = \begin{vmatrix} X_{\ddot{\imath}}(t) \\ X_{ñ}(t) \end{vmatrix}$ - вектор состояния, представляющий собой совокупность полезных и помеховых переменных состояния.

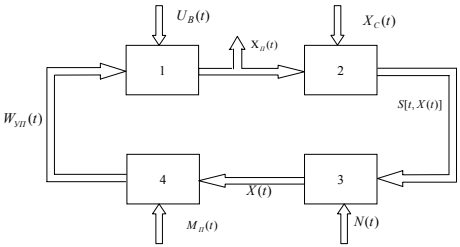


Рис. 1**.** Структурная схема системы измерения местоположения объекта

Таким образом, оценивая полезные и помеховые сигналы как переменные в пространстве состояний, можно синтезировать оптимальный обнаружитель-измеритель сигналов точечного объекта на фоне пространственно-распределенных помех.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Van Trees H. L.* Detection, Estimation, and Modulation Theory, Part IV. – Optimum Array Processing. – John Wiley & Sons, Inc., New York, 2002. – 1443 PP.

УДК 004.73(042.4)

С.Ю. Модэнов
(Национальный авиационний университет, Украина)

МЕТОДЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ МОБИЛЬНЫМИ ТЕРМИНАЛАМИ

В настоящее время все шире применяются методы дистанционного управления компьютером с помощью мобильных терминалов. Функции управления реализуются через беспроводные сети Wi-fi или Bluetooth в ручном и автоматическом режиме. Также существуют программы для создания пультов управления, предназначенных для «телефонного контроля». Они основаны на использовании «горячих клавиш», позволяют программировать собственные пульты управления и имеют систему поддержки пользователей

Наибольший интерес представляют следующие сервисные функции.

Basic Input – выполняет функцию удалённого тачпада

File Manager – позволяет открывать компьютер и просматривать его содержимое.

Keyboard – виртуальная клавиатура

Power – операции с питанием компьютера (выключение, перезагрузка и др.)

Slide Show – для управления мультимедийными презентациями.

Start – позволяет получить доступ к программам, расположенным в меню «Пуск»-> «Все программы»

Task Manager – выводит на экран список выполняемых программ из диспетчера задач.

Windows Media Center – пульт управления Windows Media Center.

Windows Media Player – пульт управления Windows Media Player.

В настройках можно выставить несколько пультов для быстрого переключения между ними: Preferences -> «Quick Switch»

Соединение по Bluetooth к компьютеру более удобно в настройке, но дальность действия и стабильность сигнала не так велики, как по wi-fi. По wi-fi можно добиться уверенной передачи сигнала, если завязать подключение на точку доступа или уже имеющуюся локальную wi-fi сеть. В случае наличия и wi-fi и Bluetooth, при выходе из зоны действия блютуза вы сможете сменить соединение на wi-fi.

Важной проблемой является обеспечение надежной, а главное – безопасной связи с компьютером. Для решения этой проблемы в первую очередь необходимо реализовать такие функции управления, как авторизация и аутентификация.

Второй, не менее важной проблемой является аппаратная реализация метода. Для этого необходимо согласовывать требования к оборудованию объекта управления (удаленного терминала) и управляющего устройства (мобильного терминала). Эта задача, по существу, представляет собой задачу управления, оптимального по быстродействию, и может решаться методами общей теории управления с учетом специфики рассматриваемой задачи.

УДК 004.78 (043.2)

О.С. Моісейкін
(Національний авіаційний університет, Україна)

ЗАСТОСУВАННЯ ВІРТУАЛЬНИХ ВИДІЛЕНИХ СЕРВЕРІВ ПРИ РОЗРОБЦІ ТА ОБСЛУГОВУВАННІ ВЕБ-ДОДАТКІВ

На сьогодні основним джерелом здобуття інформації є глобальна мережа Інтернет. Багато мільйонів користувачів кожен день обробляють терабайти інформації та надсилають тисячі запитів на сервери, що розташовані в різних куточках планети. Принцип роботи веб-серверів створює безперешкодний доступ до будь-якого контенту.

Зручним методом обміну в мережі є використання веб-сайтів з вільним доступом, на яких в подальшому розміщується текстовий та мультимедійний контент. При розробці виникає питання де і як розміщувати створений ресурс.

Найпоширенішим варіантом є використання послуг хостингу, що представляє собою місце на жорстких дисках та обмежений набір налаштувань програмної частини серверу. Цей варіант зручно використовувати при малій кількості ресурсів з невеликим потоком користувачів.

Іншим, але дорожчим, варіантом є використання віртуального виділеного серверу, який по свої суті не відрізняється від хостингу, але має деякий фізичний зміст. Через це він є доречним у тих випадках, коли необхідно розміщувати та обслуговувати багато ресурсів у яких велика кількість користувачів.

Використання виділених віртуальних серверів представляє собою роботу з серверною машиною, але не існуючої у фізичному світі. Серед переваг слід відмітити: повний контроль над дисковим простором, свобода вибору операційної системи серверу, вільний доступ до налаштувань програмної частини, змога змінювати параметри мережевої ідентифікації серверу.

З описаного вище, стає зрозумілим, що використання віртуальних серверів надає розробнику усю повноту прав при створенні веб-додатків. Також слід пам’ятати, що перед використання цієї технології, знання розробника повинні супроводжуватися попереднім досвідом роботи з серверними машинами, так як деякі операції по налагодженню можуть мати суттєві відмінності.

УДК 519.876.5

А.О. Москаленко, к.т.н.; Г.В. Сокол, к.т.н.; В.М. Глушко
(ПолтНТУ, Україна)

МАТЕМАТИЧНА МОДЕЛЬ ДИСКРЕТНОГО КАНАЛУ ЗВ'ЯЗКУ З N-ВИМІРНОЮ CCSK-МОДУЛЯЦІЄЮ ДЛЯ ДОСЛІДЖЕННЯ СТРУКТУРНОЇ ТА ЕНЕРГЕТИЧНОЇ СКРИТНОСТІ СИСТЕМ БЕЗДРОТОВОГО ЗВ'ЯЗКУ

Важливими характеристиками систем бездротового зв'язку спеціального призначення є структурна та енергетична скритність їх сингалів. Перспективним методом широкосмугової модуляції є CCSK (Cyclic Code Shift Keying, модуляція циклічним зсувом коду) [1]. Після удосконалень, запропонованих в роботах [2,3] даний метод модуляції має значні переваги перед конкурентними методами за рахунок забезпечення більш високої швидкості передачі інформації та простоти кореляційної обробки. Проте, даний вид модуляції не може бути використаний в перспективній технології радіоінтерфейсу DC MC-CDMA. Авторами було запропоновано метод N-вимірної CCSK-модуляції що призначений для використання в радіоінтерфейсах типу DC MC-CDMA.

З метою отримання характеристик сигналів, синтезованих методом N-вимірної CCSK-модуляції, було розроблено математичну модель дискретного каналу зв'язку з N-вимірною CCSK-модуляцією.

До складу моделі входять: передавач, приймач, середовище розповсюдження. В передавачі формуються сигнали N-вимірної CCSK-модуляції у відповідності до інформаційних біт, що генеруються випадковим чином. В приймачі відбувається цифрова кореляційна обробка сигналів N-вимірної CCSK-модуляції, підрахунок загальної кількості переданих інформаційних біт, кількості біт прийнятих з помилкою, ймовірності помилкового прийому інформаційних біт, структурної та енергетичної скритності сигналів. Підсистема "Середовище розповсюдження" дозволяє вносити адитивні та мультиплікативні, широкосмугові та вузькосмугові перешкоди, а також моделювати багатопроменеве розповсюдження радіохвиль з можливістю зміни амплітуд і часу затримки віддзеркалених променів.

Використання запропонованої моделі дозволяє досліджувати перешкодостійкість, структурну та енергетичну скритність сигналів N-вимірної CCSK-модуляції в різних умовах розповсюдження радіохвиль.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *G.M. Dillard et all.,* Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique // IEEE Trans. Aerosp. Electron. Systems., vol. AES-39, July 2003, pp. 786 -798.

2. *Гепко И.А.* Новый класс ортогональных кодов для телекоммуникационных систем CDMA и метод их корреляционного приема, минимизирующий вычислительную сложность цифрового сигнального процессора /И.А. Гепко, А.А.Москаленко// Зв'язок. – 2007. - № 6. – С. 33-39.

3. *Гепко И.А*. Свойства ортогональных сигналов с прямым расширением спектра на основе совершенных двоичных матриц и алгоритма их корреляционной обработки /И.А. Гепко, А.А.Москаленко// Радиоэлектроника (Изв. вузов). – 2008. – № 1-2. – С. 49-60.

УДК 004.272

В.М. Опанасенко, д.т.н.; О.О. Баркалов
(Інститут кібернетики ім. В.М. Глушкова НАН України)

СИНТЕЗ МІКРОПРОГРАМНИХ АВТОМАТІВ НА БАЗІ ПЛІС З ПЕРЕТВОРЕННЯМ ОБ'ЄКТІВ

Пристрої управління (ПУ) є важливою частиною будь-якої цифрової системи. Для синтезу ПУ широко використовуються моделі мікропрограмних автоматів (МПА) Міли та Мура. Методи синтезу ПУ базуються на роботах В.М. Глушкова та інших вітчизняних й закордонних вчених. Важливе значення для методів синтезу ПУ має елементний базис, що використовується.

Сучасний базис реалізації схем ПУ представлено програмовними логічними інтегральними схемами (ПЛІС), які підрозділяються на два основних сімейства: CPLD (Complex Programmable Logic Devices) на основі макрокомірок типу ПМЛ (програмовна матрична логіка); ПЛМ (програмовна логікова матриця). Для реалізації системи мікрооперацій МПА доцільно використати вбудовані внутрішні або зовнішні блоки пам‘яті.

Однією з важливих задач для структурного синтезу МПА є задача зменшення апаратних витрат в схемі автомата. Особливості ПЛІС типу CPLD потребують адаптації відомих й розробки нових методів синтезу МПА для цього базису. Основною ціллю цих методів є зменшення кількості макрокомірок, що використовують схеми мікропрограмного автомата.

Запропоновано методи структурного синтезу логічних схем МПА Мілі та Мура, які засновано на перетворенні кодів станів і додаткових змінних у коди наборів мікрооперацій. При цьому для кодування наборів використовуються три методи: унітарне, максимальне і кодування полів сумісних мікрооперацій. Подібні МПА названо автоматами першого роду. Крім того, розроблено методи перетворення кодів наборів мікрооперацій у коди станів МПА. У випадку МПА цей підхід припускає використання додаткових змінних. Подібні МПА названо автоматами другого роду. Запропонований принцип перетворення кодів дозволяє зменшити кількість додаткових змінних в багаторівневих схемах мікропрограмних автоматів, а методи на основі цього принципу дозволяють зменшити кількість макромірок кристалу ПЛІС в схемах МПА в зрівнянні з відомими аналогами.

Модифіковані методи синтезу МПА в базису замовних матриць дозволяють зменшити площу матричних схем автоматів в зрівнянні з відомими аналогами за рахунок зменшення кількість змінних у підсхемі, що формує вихідні функції МПА. Розроблено також структурні схеми МПА Мілі й Мура першого та другого родів, які орієнтовано на базис ASIC.

Структурні схеми МПА Мілі та Мура в базисі ПЛІС із архітектурою CPLD, що побудовано за допомогою запропонованих методах, дозволяють зменшити кількість використаних макрокомірок ПЛИС (до 40%) в зрівнянні з відомими методами.

Автомати першого роду забезпечують мінімум вартості пристроїв управління, а автомати другого роду – максимум швидкодії. Вибір типу автомата залежить від критеріїв ефективності при синтезу пристроїв управління.

УДК 004.896 (043.2)

О.В. Панфьоров
(Національний авіаційний університет, Україна)

АНАЛІЗ СХЕМИ РОЗТАШУВАННЯ УЛЬТРАЗВУКОВИХ СЕНСОРІВ НА РУХОМИХ ПЛАТФОРМАХ

Для забезпечення роботизованих систем засобами орієнтації в просторі винайдено чимало сенсорів, що спрощують задачу побудови картини навколишнього середовища, але завжди постає задача коректного розташування сенсорів. Залежно від призначення системи, від умов оточення, елементної бази та десятків інших властивостей, перед розробником виникає розмаїття варіацій, для кожного потрібно окреме дослідження і сфера застосування.

Із усього розмаїття сенсорів, представлених на ринку, найдоступнішими та досить простими є HC-SR04. Найголовнішими параметрами будь-якого сенсора є область охоплення та ефективна відстань. HC-SR04 охоплює конусоподібну область перед приймачем, тому саме приймач формує робочу зону сенсора. Ефективна відстань сягає трьох метрів.

Особливості конструкції сенсорів HC-SR04 накладають обмеження на використання – приймач та передавач розташовані на відстані двох сантиметрів один від одного.

Частково ця проблема може бути вирішена встановленням сенсорів вертикально, або використанням сенсорів із поєднаними приймачами та передатчиками. Застосувавши ці рішення сліпі зони буде зменшено майже у два рази, незалежно від обраної схеми розташування.

В результаті проведеного дослідження було виявлено, що раціонально розташовані сенсори, незалежно від кількості, можуть формувати робочу зону з мінімальними сліпими зонами, в яких об’єкт не буде зафіксовано. Втім, кількість сенсорів значним чинов впливають на сумарний кут, на якому сенсори будуть ефективно працювати. Але тоді постає проблема опитування сенсорів та потужності процесора, що використовується.

Важливим фактором є спосіб розташування сенсорів – вертикально розташовані сенсори демонструють кращі результати, ніж аналогічні, розташовані горизонтально. Також виявлено, що роздільні приймач та передавач є менш ефективними, ніж сенсори з тими самими параметрами, але з поєднаними приймачем і передавачем.

Було враховано рівні шуму сенсорів та запропоновані методи фільтрації з оптимальним часом спрацювання.

УДК 004.56.5(043.2)

А.Б. Петренко; В.О. Борозніченко
(Національний авіаційний університет, Україна)

КЛАСИФІКАЦІЯ ФОРМАЛЬНИХ МЕТОДІВ АНАЛІЗУ ІНФОРМАЦІЙНИХ РИЗИКІВ

На сьогоднішній день не існує єдиного засобу та методу захисту автоматизованих систем. Так як, для кожної системи має бути встановлений комплексний захист, відштовхуючись від необхідності захисту властивостей інформації. Тому постає проблема дослідження, вибору існуючих та розробки досконаліших методів аналізу інформаційних ризиків. Для побудови ефективної методики аналізу ризиків необхідно використовувати різні методи такі, як повний, базовий, експертний.

Комплекс засобів захисту для автоматизованих систем, де протікає інформація з обмеженим доступом, інформація, яка є державною таємницею, або власністю держави, та для автоматизованих систем, де циркулює конфіденційна інформація повинні істотно відрізнятись.

Було розглянуто такі провідні методики аналізу інформаційних ризиків, як CRAMM, Risk Watch, Cobra, Авангард, OCTAVE. На сьогоднішній день вони є надійними засобами аналізу інформаційних ризиків, але в свою чергу кожен з них має певні недоліки та переваги.

Кожна комплексна система захисту інформації має бути ієрархічною. Базовий рівень інформаційної безпеки є обов'язковим для кожної системи. Для забезпечення мінімального рівня безпеки необхідно перевірити систему на відповідність виконання вимог певного стандарту такого, як ISO 17799 (Информационные технологи.Технологии безопасности. Практические правила менеджмента информационнной безопасности), ISO 13335 (Методы и средства обеспечения безопасности), ISO 27001 (Информационные технологии. Методы защиты. Системы менеджмента защиты информации.Требования), ISO 27005 (Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности). Перевірка автоматизованої системи на відповідність стандартам дає не чітку оцінку інформаційних ризиків.

Для детальної оцінки існує потреба в використанні спеціальних програмних засобів оцінки ризиків. В вище наведених програмних засобах оцінки інформаційних ризиків присутні такі недоліки:

1. неузгодженість з вітчизняними стандартами;
2. продукти не мають гнучкий інтерфейс та можливість налаштування під певні особливості системи;
3. результати перевірки не є очевидними.

Для кращого результату оцінки інформаційної безпеки можна використовувати комбінований метод оцінки, який складається з базового та повного методу оцінки ризиків. Використання експертних методів полягає в наданні експертної оцінки певній системі ,по шкалі «високий-середній-низький», але не є ефективним при використанні, як самостійного методу.

Під час порівняння методів та методик аналізу інформаційних ризиків був прийнятий висновок про необхідність використання комплексної методики аналізу ризику методів якісної, кількісної оцінки та формалізації проведення аналізу інформаційного ризику.

УДК 510.645:004.032.26

Н.К. Печурин, д.т.н.
(НАУ,Украина);
Л.П. Кондратова , к.т.н.;
С.Н. Печурин, к.т.н.
(УНК «ИПСА» НТУУ «КПИ», Украина);
Н.Н. Яценко
(НАУ,Украина)

ЗАЩИТА ИНФОРМАЦИИ В БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ЭТАЛОННОЙ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ

Защиту информации в беспроводных компьютерных сетях обеспечивают контроль доступа по MAC-адресам и механизм WEP для аутентификации с разделяющим ключом и шифрования данных. Широкое применение в военной связи для улучшения безопасности беспроводной передачи в последние 50 лет имеет технология DSSS в частотном диапазоне 2,4 ГГц, в рамках которой поток данных разворачивается по каналу с помощью схемы ключей дополнительного кода [1]. Межуровневое взаимодействие в эталонной модели (ЭМ) взаимосвязи открытых систем реализуется с использованием процедур инкапсуляции/деинкапсуляции данных и заголовков. На каждом уровне перед передачей данных на более низкий уровень в заголовок помещается дополнительная информация, формируя ряд вложенных заголовков. $(N-1)$ преобразований (N - число уровней ЭМ), заложенных в ЭМ, представляются последовательным формированием предложений формальных метаязыков с $(N-1)$ разных грамматик. Функции обеспечения взаимодействия MAC-станций на подуровне PLCP физического уровня для систем с технологией DSSS реализуются путем формирования предложений некоторого формального метаязыка. Формируются предложения в виде:

$$PPDU \rightarrow ЗАГОЛОВОК \quad А \mid Б \ldots; \quad PDU \rightarrow А \mid Б \ \ldots \ ТРЕЙЛЕР\,; \quad ЗАГОЛОВОК \rightarrow ЗАГОЛОВОК \quad А \mid .$$

Здесь заголовок представляет поля с указанием типа модуляции и скорости передачи, определением ранее зарезервированных битов в некоторых модификациях стандарта 802.11, указанием времени передачи в микросекундах, значения CRC-16.

Предлагаемая модель трансляции для обеспечения надежного обмена информации является адекватной.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Иманкул М.Н. Защита беспроводной компьютерной сети // Вестник ЕНУ им. Л.Н.Гумилева. – 2011. - №6. – С.39-46.

УДК 519.688:004.7

М.В. Плахотний, к.т.н.; М.В. Наливайчук;
О.Ю. Наливайчук, м.н.с.; В.В. Микитенко
(НТУУ "КПІ", Україна)

ОСОБЛИВОСТІ ПРОГРАМУВАННЯ ТА ЗАСТОСУВАННЯ MULTITOUCH ПАНЕЛЕЙ В МУЛЬТИМЕДІЙНИХ ДОДАТКАХ

Із розвитком та розширенням можливостей мультимедіа до інтерфейсу користувача ставляться все більш високі вимоги, що заставляє досліджувати нові способи взаємодії користувачів із мультимедійними додатками.

В роботі розглянуто декілька напрямків забезпечення взаємодії з мультисенсорними панелями: використання жестів, окремих дотиків, а також використання додаткових засобів, що надають більше можливостей та спрощують розробку програмного забезпечення.

Розглянуто способи створення додатків для систем Windows XP/Windows7.

Для прикладу розглядається сенсорна панель фірми PQ Labs - Multi-Touch G3 Plus та SDK для цієї моделі.

Можливі декілька підходів до розробки додатків, орієнтованих на використання сенсорних панелей, а саме: використання native API системи та використання бібліотек розробника (SDK).

Для системи Windows 7 розглянуті наступні можливості реалізації:

Використовуючи мову C++:

Для native API розглядається розпізнавання жестів та простих маніпуляцій за допомогою отримання повідомлень WM_GESTURE, WM_TOUCH від панелі, та їх обробка в обробнику подій Windows-програми WndProc.

Концепція використання мультисенсорних панелей надає ряд можливостей для користувача при взаємодії з мультимедійними додатками.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. http://multi-touch-screen.com/sdk.html - PQLabs MultiTouch SDK
2. http://msdn.microsoft.com/en-us/library/ms754130.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd562197.aspx

УДК 004.73(042.4)

А.В. Пономаренко, к.т.н.
(Национальный авиационний университет, Украина)

ВЫБОР ВЕСОВОЙ ФУНКЦИИ АЛГОРИТМА ВЕЕРНОГО ПРЕОБРАЗОВАНИЯ РАДОНА

При определении источников акустических шумов применяются методы дистанционного зондирования с комбинированным (линейным и угловым) сканированием датчиков акустических шумов. Требуемой точности измерений можно достичь путем применения методов реконструктивной вычислительной томографии, модифицированных для случая пространственно разнесенных приемников. При обработке данных в области пространственных частот имеем совокупность точек пространственного спектра $\tilde{f}(\rho,\theta)$ в полярном растре, т.е. в координатах (ρ,φ). В работе [1] показано, что для рассматриваемой задачи наиболее приемлемым методом томографической обработки данных от разнесенных датчиков системы обнаружения утечек является метод интегрирования фильтрованных обратных проекций. При комбинированном сканировании датчиков для вычисления координат источника утечки необходимо применять обратное преобразование Радона [2]: $f(x,y)=\int_{-\infty}^{\infty}\int_{0}^{\pi}\tilde{f}(\rho,\theta)e^{2i\pi\rho(x\cos\theta+y\sin\theta)}d\theta|\rho|d\rho$. По функции $f(x,y)$ определяется пространственное положение источника акустического шума, а функция $|\rho|$ под знаком внешнего интеграла представляет собой якобиан преобразования при переходе от декартовых координат к полярным.

Для уменьшения уровня боковых лепестков предлагается применять вместо функции $|\rho|$ сглаженную функцию, в качестве которой выбран модуль первой производной гауссовской функции $g(x)=a\cdot\exp(-bx^2)$, где a, b – константы, выбираемые в соответствии с размерами области интегрирования преобразования Радона. Выражение для весовой функции имеет вид:

$\left|\frac{d}{dx}\left[a\cdot\exp(-bx^2)\right]\right|=ab\cdot\left|2x\cdot\exp(-bx^2)\right|$. На рис. 1 изображена пространственно-частотная весовая функция, а на рис. 2 – сечение соответствующей функции $f_w(x,y)$ точечного источника акустического шума.

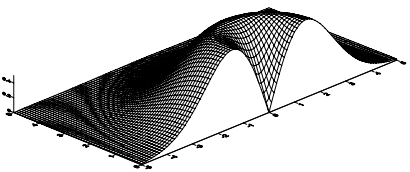


Рис. 1. Весовая функция

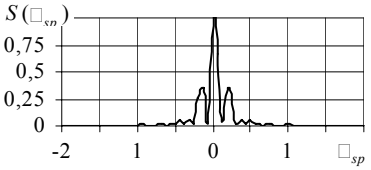


Рис. 2. Отклик точечного источника шума

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Пономаренко А.В.* Алгоритм обнаружения и измерения координат источ-ника акустических шумов // Наукові записки УНДІЗ. – 2012. – №2(22). С. 70 – 75.
2. *Хелгасон С.* Преобразование Радона. – М.: Мир, 1983. – 152 с.

УДК 621.391

В.В. Приступа
(Інститут телекомунікацій та глобального інформаційного простору НАН України, Україна)

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ОРТОГОНАЛЬНО-ЧАСТОТНОГО МУЛЬТИПЛЕКСУВАННЯ В РЕКОНФІГУРОВАНИХ БЕЗПРОВІДНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ В УМОВАХ ПОСТАНОВКИ НАВМИСНИХ ЗАВАД

В сучасних умовах активної радіоелектронної протидії постає задача забезпечення заданої достовірності передачі інформації за умов максимальної пропускної спроможності реконфігурованих безпровідних інформаційно-телекомунікаційних мереж [1]. Сучасні безпровідні системи, які призначені для роботи в умовах впливу навмисних завад, для протидії навмисним завадам використовують розширення спектру сигналів методом псевдовипадкової перебудови несучої частоти, коригувальні коди Рида-Соломона та двопозиційні модульовані сигнали [2,3]. Недоліком зазначених систем є те, що вони не враховують зміни завадової обстановки, а також забезпечують низькошвидкісну передачу інформації. Постає завдання розробки нових методів, моделей та алгоритмів, спрямованих на підвищення завадозахищеності та пропускної спроможності зазначених систем в умовах активної радіоелектронної протидії та динамічної зміни завадової обстановки.

Метою роботи є розробка технології ортогонально-частотного мультиплексування з внутрібітовою псевдовипадковою перебудовою піднесучих частот для підвищення пропускної спроможності реконфігурованих безпровідних інформаційно-телекомунікаційних мереж в умовах динамічної зміни завадової обстановки.

Для подавлення безпровідних систем з розширенням спектру сигналу постановником завад можуть застосовуватися різні види навмисних завад, які при певних умовах здатні ефективно впливати на характеристики завадозахищеності систем [2,3]. Основними видами завад, які найбільш часто реалізуються в системах постановки навмисних завад, є: шумова загороджувальна завада, шумова завада в частині смуги, полігармонійна завада та завада у відповідь, моделі яких представляють собою білий гаусівський шум [2].

Основна ідея методу OFDM полягає в тому, що смуга пропускання каналу розбивається на групу вузьких смуг (субканалів), кожна зі своєю піднесучою. На всіх піднесучих сигнал передається одночасно, що дозволяє забезпечити велику швидкість передачі інформації при невеликій швидкості передачі в кожному окремому субканалі [4]. Сигнал OFDM складається із N ортогональних піднесучих, модульованих N паралельними потоками даних.

Формування підканалів з ортогональними піднесучими відбувається за допомогою процедури зворотного дискретного перетворення Фур‘є (ДПФ) [4]. На практиці процедури зворотного ДПФ (на передаючій стороні) та прямого ДПФ (на прийомній) реалізуються за допомогою алгоритму швидкого перетворення Фур‘є (ШПФ) та виконуються процесором ШПФ [4,5]. Функції OFDM-модулятора зводяться до формування складового неперервного сигналу, який містить N піднесучих, більша частина з яких модульовані інформаційними символами на

інтервалі тривалості символу. Формування сигналу OFDM з внутрібітовою ППППЧ відбувається за допомогою розширення Уолша.

Система з ортогонально-частотним мультиплексуванням (OFDM) з внутрібітовою псевдовипадковою перебудовою піднесучих частот (ППППЧ) складається з передавальної та приймальної частин. Передавальна та приймальна частини мають у своєму складі наступні елементи: кодер (декодер) прямого розширення спектру за допомогою кодів Уолша (розширення/звуження Уолша), модулятор (демодулятор) OFDM з ППППЧ, формувачі псевдовипадкових послідовностей. За допомогою кодів Уолша та модулятора сигналу OFDM з ППППЧ формується саме система OFDM з внутрібітовою ППППЧ.

Для динамічної зміни параметрів системи OFDM з внутрібітовою ППППЧ пропонуються застосовувати контур параметричної адаптації, тобто за результатами аналізу завадової обстановки здійснюється динамічна зміна розміру розширюючих послідовностей Уолша.

За допомогою розробленої математичної моделі доказана ефективність запропонованої технології.

Представлена в роботі технологія побудови системи OFDM з внутрібітовою псевдовипадковою перебудовою піднесучих частот дозволяє наступне:

здійснювати адаптивну зміну розміру розширюючих послідовностей, тим самим звужуючи або розширюючи частотний діапазом сигналу OFDM, що необхідно для підвищення завадозахищеності в умовах активної радіоелектронної протидії;

формувати коди Уолша необхідної довжини;

здійснювати більш ефективну оцінку каналу зв'язку шляхом розбиття інтервалу оцінювання на M інтервалів.

За результатами дослідження зроблено наступні висновки:

розроблено інформаційну технологію побудови систем OFDM з внутрібітовою псевдовипадковою перебудовою піднесучих частот, які б ефективно функціонували в умовах впливу навмисних завад;

розроблена технологія дозволить підвищити завадозахищеність та пропускну спроможність діючих радіозасобів в умовах активної радіоелектронної протидії;

напрямком подальших досліджень вважаємо доцільним додати до розробленої схеми коригувальні коди та пристрій оцінки каналу.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Зайцев С.В.* Анализ принципов построения программируемых радиостанций / С. В. Зайцев, С. П. Ливенцев, А. И. Артюх // Зв'язок. – 2007. – № 5. – С. 46-54.

2. *Борисов В.И.* Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / Борисов В.И., Зинчук В.М., Лимарев А.Е. и др. – М.: Радио и связь,2000. – 384 с.

3. *Борисов В.И.* Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей певдослучайной последовательностью / Зинчук В. М., Лимарев А. Е. и др. – М.: Радио и связь, 2003. – 640 с.

4. *Khan F.* LTE for 4G Mobile Broadband. Air Interface Technologies and Performance / Khan F. – Cambridge: Cambridge University Press, 2009. – 509p.

5. *Cho Y.* MIMO-OFDM Wireless Communications with Mathlab / Cho Y., Kim J., Yang W. [et al.]. – Singapore: John Wiley & Sons, 2010. – 457 p.

УДК 681.3.07

М.М. Проценко, к.т.н.
(Національний авіаційний університет, Україна)

АДМІНІСТРУВАННЯ СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Історія системного адміністрування нараховує декілька десятиліть, починаючи з обчислювальних комплексів (своєрідних аналогів локальних мереж), які складалися з центрального комп'ютера (мейнфрейма) з підключеними терміналами користувача. Адміністрування таких систем зводилося до налаштування багатозадочного режиму з одночасним доступом багатьох користувачів.

Адміністрування сучасних обчислювальних систем і комп'ютерних мереж - досить складний процес, який вимагає від системного адміністратора не тільки досить високої кваліфікації, але і виконання великого обсягу рутинної роботи.

Внаслідок розростання і ускладнення структури комп'ютерної мережі, появи технологій розподіленої обробки даних і зберігання інформації, замість однорідного середовища адміністраторам прийшлось мати справу з великим різноманіттям ресурсів: апаратними і програмними платформами, мережним обладнанням і мережним трафіком. Змінився обсяг роботи системних адміністраторів і розширився спектр виконуваних ними робіт. До традиційних об'єктів системного адміністрування додалися мережеві операційні системи, розподілені бази даних і сховища даних, мережні додатки і, в кінцевому підсумку, користувачі. Враховуючи профіль робіт, фахівців, які працювали з мережами, стали називати мережними адміністраторами.

Неминучим виявився процес інтеграції системного і мережевого адміністрування. Очевидно, що управління роботою складної гетерогенної мережі є складнішим завданням, ніж, наприклад, контроль за функціонуванням мережевих принтерів. Тому системне адміністрування слід розглядати як складову частину адміністрування мережного, оскільки мережа містить у своєму складі об'єкти системного адміністратора.

Адміністрування комп'ютерної мережі - це процес управління функціонуванням мережі в цілому і окремих її підмереж та мережного обладнання, який призваний забезпечити ефективне і надійне виконання мережею поставлених перед нею задач. Функції адміністрування мережею покладаються на одну або декілька осіб (фахівців) - мережних адміністраторів.

Завдання, що вирішуються мережними адміністраторами, слід розподілити на такі групи:

- контроль за роботою і управління ресурсами (облік, контроль використання ресурсів і встановлення прав доступу до них);
- управління функціонуванням і конфігурацією мережі в цілому, спрямоване на забезпечення надійного і ефективного функціонування усіх компонентів мережі;
- контроль і управління продуктивністю (збір і аналіз інформації про роботу окремих ресурсів, прогнозування міри задоволення потреб користувачів/додатків, заходи по збільшенню продуктивності);
- захист даних (забезпечення цілісності даних, управління їх шифруванням, обмеження доступу);

- вирішення проблемних ситуацій (діагностика, локалізація і усунення несправностей, реєстрація помилок, проведення тестування);
- управління доступом користувачів до мережі.

Ефективна робота мережного адміністратора стала неможливою без використання як спеціальних засобів автоматизації адміністрування, так і певних стратегій та технологічних прийомів управління. Проекти розвитку адміністративних механізмів зазвичай включали постановку завдань стратегічного управління, розробку політики інформаційного забезпечення і доступу до інформаційних ресурсів, а також створення програмно-апаратних засобів, систем і комплексів, вдосконалення безперервного управління.

Мережні адміністратори отримали програмні інструменти для конфігурації, моніторингу, діагностування або супроводу кожного окремого компонента мережі. Однак ці інструменти були розрізненими. Порівняно з ними ефективним засобом автоматизації адміністрування мережею стали платформи управління мережею (Network Management Platform) - комплекси програм, призначених для управління мережею і системами, що входять в неї або базуються на ній, наприклад, інформаційними системами. До таких платформ, які стали дієвим засобом автоматизації адміністрування слід віднести HP OpenView, SunNet Manager, NetView 6000 та Cabletron Spectrum.

Платформа зазвичай включає підтримку протоколів взаємодії менеджера з агентами – SNMP і рідше CMIP, набір базових засобів для побудови менеджерів і агентів, а також засобу графічного інтерфейсу для створення консолі управління. У набір базових засобів зазвичай входять засоби побудови карти мережі, фільтрації повідомлень від агентів, ведення бази даних.

Наприклад, OpenView є усеосяжним засобом управління IT-інфраструктурою підприємства будь-якого розміру і напряму діяльності. Надає широкі можливості по моніторингу і управлінню локальними обчислювальними мережами, серверними платформами (такими, як HP-UX, Solaris, AIX, Novell, Linux, увесь спектр Windows-платформ), додатками (SAP, Oracle, Sybase, MS SQL, Exchange, DB2, Informix, MS Active Directory), робочими місцями користувачів (інвентаризація, видалена установка ОС, оновлення програмного забезпечення, налаштування користувачів, контроль за використанням програмних засобів).

Поряд зі створенням технічних засобів адміністрування розробляються технології, які дозволяють спросити сам процес адміністрування комп’ютерних мереж. Спрощення процедур досягається різними способами, наприклад, зміною політики адміністрування, реорганізацією структури мережі, використанням спрощених методик. спрощених методик. Наприклад, будь-які комп'ютери мережі і ресурси, які розділяються, можна об'єднувати в групи, що називаються доменами - логічними групами комп’ютерів в мережі з однаковим іменем.

Зміну політики, що призводить до спрощення адміністрування, можна розглянути на прикладі реалізації політики формування і обміну ключами криптографічного захисту. Реорганізація процедури обміну ключами, виключення користувачів з участі в процесах генерації нових ключів призводить до спрощення адміністрування криптографічного захисту.

УДК 681.324

М.М. Проценко, к.т.н.; Є.І. Безвершенко; С.О. Бесараб
(Національний авіаційний університет, Україна)

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ В РОЗПОДІЛЕНІЙ КОМП'ЮТЕРНІЙ СИСТЕМІ

Виявлення спроб несанкціонованого доступу до інформаційних ресурсів комп'ютерної мережі в реальному масштабі часу є актуальною задачею при створенні систем захисту інформації. Важливими компонентами комплексної системи захисту інформації в комп'ютерних мережах є міжмережеві екрани, системи виявлення атак, системи виявлення та попередження вторгнень. Дослідження та розробка методів і алгоритмів функціонування систем виявлення атак на основі централізованого управління являє науковий та практичний інтерес.

На підставі результатів аналізу сучасних підходів щодо забезпечення безпеки комп'ютерних систем запропонована модель захищеної розподіленої комп'ютерної системи, структура та алгоритми її функціонування. Розподілена система виявлення атак (СВА) побудована згідно концепції відкритих систем, удосконалена і доповнена додатком-агентом автоматичного оновлення баз даних сигнатур атак. В дослідженні розроблена структура СВА, описані компоненти СВА, розроблені алгоритми виявлення атак. Результати моделювання роботи запропонованої розподіленої СВА підтвердили ефективність запропонованого підходу у порівнянні з традиційними сигнатурними мережевими СВА (рис. 1).

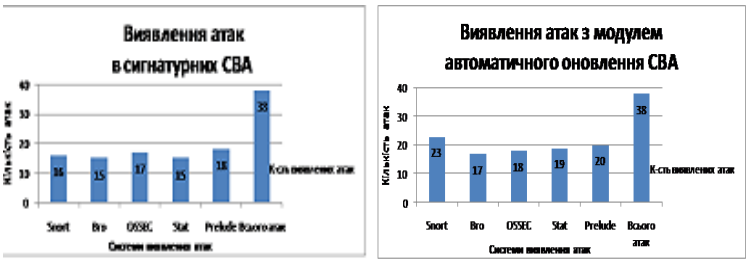


Рис. 1. Виявлення атак СВА

В роботі наведено рекомендації щодо реалізації ядра СВА, які дозволяють зменшити залежність продуктивності СВА від повноти БД ознак вторгнень, а також визначені варіанти практичного застосування розподіленої СВА. Розроблена модель захищеної розподіленої системи є достатньо універсальною і може використовуватися в інших задачах, де потрібно забезпечити захищену інформаційну взаємодію фізично або логічно розподілених суб'єктів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *А. Лукацкий.* Обнаружение атак. Из-во БХВ-Петербург, 2003, 596 с.

УДК 004.7

А.С. Савченко, к.т.н.
(Национальный авиационний университет, Украина)

МЕТОД ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

При проектировании корпоративных мультисервисных сетей основным является обеспечение качества обслуживания для разнородного трафика. Основными интегральными показателями качества функционирования сети являются [1]:

• количество потерянных пакетов – для TCP сети 1-5% потерянных пакетов, согласно экспертным оценкам, находится в пределах нормы, 40% потерянных пакетов – пороговое значение, при котором сеть практически не работает;

• количество пакетов, переданных с ошибками;

• время задержки доставки пакетов;

• вариация задержки доставки пакетов (джиттер) – особенно важна для мультимедийных приложений.

При этом каждый из типов трафика характеризуется рядом критичных и некритичных параметров. Например, для мультимедийного трафика (IP-телефония, видеоконференции и т.д.) критичными являются показатели времени задержки и вариация задержки, а для трафика данных (электронная почта, передача файлов и т.д.) – количество потерянных и искаженных пакетов.

Качество решения поставленной задачи зависит от наявных средств управления сетью. Поэтому разработка эффективного метода управления корпоративной сетью является актуальной задачей.

Эффективность управления характеризуется способностью не устранять последствия сбоев в работе, а предотвращать их. Для этого необходимо проводить анализ и прогнозирование состояний сетевой среды основываясь на интегральных показателях качества.

Предлагаемый метод управления сетью [2] основан на том, что по результатам анализа параметров и структуры сети строится двухуровневая эталонная модель (ЭМ) сегмента сети. Первый уровень которой отвечает за активное оборудование, второй – за состояние сети. Такой подход позволяет отделить задачу управления надежностью оборудования от задачи анализа и управления топологией сети. На базе ЭМ выполняется прогноз состояния. Полученные данные являются основой для формирования и выбора оптимальной стратегии управления администратором и экспертной системой. Анализ эффективности работы администратора проводится посредством сравнения стратегии управления выбранной администратором, предложенной экспертной системой и полученных в результате управления состояний сети.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Олифер В.Г.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / В.Г. Олифер, Н.А. Олифер. – СПб: Питер, 2010. – 944 с.

2. Савченко А.С. Концептуальная модель системы управления крупной корпоративной сетью / А.С. Савченко // Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2011. – Вип. 2(34). – С. 120-128.

УДК 004.78 (043.2)

М.С. Савченко; А.Б. Коцюр
(Національний авіаційний університет, Україна)

ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ В ОСВІТІ З МЕТОЮ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СПРИЙНЯТТЯ ІНФОРМАЦІЇ

Зростання технологічних винаходів значно прискорює науково-технічний прогрес. Таким чином перед сучасною педагогами постає важливе завдання - підготувати та виховати підростаюче покоління, яке буде здатне включитися в новий етап розвитку сучасного суспільства, пов'язаний з інформатизацією, вільно буде орієнтуватися у світовому інформаційному просторі, мати знання для обробки та зберігання інформації з використанням комп'ютерної техніки

Значна увага нині стала приділятися і впровадженню інформаційних технологій в освітній процес, розгортанню системи освіти на підставі використання найсучасніших інформаційних технологій. Сучасні освітні технології зумовлені трьома основними розділами технічного розвитку: комп'ютерною технікою, інформаційними мережами, мультимедійними засобами.

Дуже часто перед студентами постає проблема розуміння ступеню необхідності інформації та можливостей її застосування, адже, пошук та відбір необхідної інформації у мережі та оцінка її якості здебільше стає саме обов'язковим предметом навчання в рамках навчальної програми. Проблема використання інформаційних технологій – це пошук, відбір і застосування дійсно цінної інформації з нескінченного інформаційного потоку, тобто отримання знань з інформації, орієнтуватися в інформаційному середовищі, яке швидко розширюється.

Для того щоб поліпшити ефективність навчання необхідно створити для кожної спеціальності певний набір електронних та мультимедійних підручників. По-перше це поліпшить успішність – кожний студент зможе шукати саме потрібну для нього і предмету інформацію. По-друге це зменшить проблему сприймання та запам'ятовування інформації.

Ще один спосіб для покращення ефективності сприймання інформації та перевірки отриманих знань це певні тести або тренажери. Наприклад авіа симулятор. Це жанр відеогри, який може симулювати літальний апарат будь-якого типу. Такий симулятор призначений для професійної підготовки льотчиків, тож ще одна його назва це авіаційний тренажер.

УДК 681.5(042.3)

В.В. Семко, к.т.н.
(Інститут телекомунікацій і глобального інформаційного простору НАН України, Україна);
В.О. Темніков, к.т.н.
(*Національний авіаційний університет, Україна)*

ЗАХИЩЕНА ОПЕРАЦІЙНА СИСТЕМА. ДОСВІД СТВОРЕННЯ

Розробка, а тим більше супроводження, абсолютно нової операційної системи (надалі - ОС) на поточний час не є виправданою. Тому під час створення захищеної операційної системи (надалі - ЗОС) було визначено за доцільне використання накопичених доробок відкритого програмного коду таких ОС як Linux та FreeBSD Unix.

З метою забезпечення можливості використання напрацьованих на поточний час програмних доробок системного характеру ЗОС підтримує підмножину загальної множини системних викликів згідно специфікацій POSIX та X-Openta, а також мінімально необхідну підмножину специфічних системних викликів, які притамані ОС FreeBSD та Linux.

Основою побудови ЗОС є об'єктно-реляційний підхід до архітектури ОС. Обчислювальні процеси, які здійснюються під час функціонування ЗОС виконуються на рівні ядра та на рівні процесу.

На рівні ядра забезпечується функціонування необхідного набору системних компонент та компонент диспетчера доступу, які за визначенням є об'єктами ЗОС.

Взаємодія між активними та пасивними об'єктами здійснюється виключно на рівні програмних компонент диспетчера доступу, що забезпечує необхідні умови реалізації комплексного підходу до функціонування сервісів комплексу засобів захисту ЗОС.

На рівні процесу здійснюється обробка інформації, що циркулює в межах самої ЗОС, а саме: функціонування стандартних сервісних служб, функціонування системи управління мережевими обчисленнями (мережевого каталогу, брокерів запитів, тощо), забезпечення взаємодії користувачів та ініційованих ними процесів з операційною системою та процесів, тощо.

В цілому на рівні ядра ЗОС забезпечується функціонування програмних компонент основних підсистем: управління процесами, управління захистом файлової системи, управління драйверами загального призначення, управління драйверами підтримки вітчизняних апаратних засобів криптографічного захисту інформації, забезпечення функціонування модуля підтримки шифрування мережевого трафіку, забезпечення функціонування модуля перевірки цілісності ядра, управління та забезпечення функціонування мережевого екрану, управління та забезпечення функціонування ядра системи антивірусного захисту, тощо.

Обробка інформації на рівні процесу здійснюється в ЗОС шляхом забезпечення функціонування стандартних сервісних служб, системи управління мережевими обчисленнями (мережевого каталогу, брокерів запитів, тощо), системи забезпечення користувачів та їх процесів, тощо. Процес ЗОС відповідає формальній моделі Хорнінга-Ренделла і використовує в якості агента віртуальну машину ядра під управлінням диспетчеру доступу ЗОС.

УДК 004.896 (043.2)

Р.М. Скакун
(*Національний авіаційний університет, Україна)*

МЕТОД УЛУЧШЕНИЯ ВОСПРИЯТИЯ ИК - ДАТЧИКОВ ЗА СЧЁТ КУСОЧНО-ЛИНЕЙНОЙ АППРОКСИМАЦИИ

ИК-датчики - доступные, эффективные и простые в использовании сенсоры, позволяющие определять расстояние до объекта или препятствия, по этому эти датчики очень часто применяются в робототехнике.

Проблематика определения расстояния состоит в том, что ИК-датчик имеет нелинейный выход: при линейном увеличении расстояния, сигнал на аналоговом выходе увеличивается/уменьшается нелинейно. Это затрудняет процесс определения расстояния микроконтроллером (порог срабатывания АЦП), тем самым требует лишних процессов преобразования, что замедляют роботу всего алгоритма.

Стандартный АЦП преобразует произвольное аналоговое значение, в байты, которое находится между 0 и 255 (256 вариаций). Поэтому нужно преобразовать функциональную кривую(только активные зоны) в совокупность функций которые имеют линейный характер.

Определив наиболее ровные участки наложим касательные функции, чем больше линейных участков тем больше памяти будет занимать наша обработка, но тем точней будет результат.

Для этого применяется общее уравнение прямой (1.1):

$$y=kx+b, \qquad (1.1)$$

где k — угловой коэффициент прямой ($k = tg\varphi$), где φ — угол между прямой движения и осью Ox, b — точка пересечения прямой и оси Oy

Описав следующие прямые по формуле (1.1) получим следующие выражения, которые описывают каждый активный участок (для ИК-датчиков их всего три – $[0;56) \cup (56;118) \cup (118;255]$):

Коэффициенты нужно подобрать такие, чтобы прямая не только максимально плотно легла на исходную кривую, но и чтобы они были как можно ближе к степени двойки. Чтобы можно было делить и умножать сдвигами.

После каждого прогона значение на выходе имеет линейную диаграмму направленности расстояния, не имея лишних искажений, тем самым повышает процесс обработки от датчика.

УДК 004.78 (043.2)

Б.Д. Скочинський
(*Національний авіаційний університет, Україна)*

ОРГАНІЗАЦІЯ НЕЧІТКИХ ПОШУКОВИХ ЗАПИТІВ В БАЗАХ ДАНИХ

У зв’язку зі зменшенням вимог до користувачів баз даних програміст може йти трьома шляхами при розробці інтерфейсу роботи з базами даних:

1) постійно додавати нові запити, щоб в повній мірі реалізувати потреби замовника (такий шлях найпростіший, але вимагає постійної участі в проекті);

2) підняти рівень користувача за рахунок гнучких настроювань системи і можливості формування власних запитів з використанням елементарного конструктора (нажаль, практично неможливий, у зв’язку з тим, що переважна більшість користувачів не бажає розвиватись самостійно для полегшення своєї праці);

3) підняти рівень “інтелектуальності” інтерфейсу за рахунок внесення автоматичних настроювань з мінімальним опитуванням користувача (це доволі складний шлях, але при реалізації дозволяє програмісту залишити працювати програму в автономному режимі без внесення змін доволі довгий час).

Хоча більша частина даних, які обробляються в сучасних інформаційних системах, і носить чіткий, числовий характер. Але при вирішенні проблеми перетворення запитання від кінцевого користувача в запит до баз даних, коли у запитаннях, які намагається формулювати користувач, часто присутні неточності і невизначеності, неможливо обійтися без механізму нечіткої логіки. Даний механізм дозволяє використовувати терміни "молодий", "не дуже дорого", "близько", що мають розмитий, неточний характер. Для вирішення даної задачі використовується метод генерації нових лінгвістичних термів на основі базової терм-множини, який реалізується на основі збережених процедур в межах СКБД.

Але великим недоліком нечітких запитів є відносна суб'єктивність функцій приналежності. Тому що все залежить від коректності функції приналежності. Але, за можливості включення автоматичного аналізу, можна будувати функцію приналежності в автоматичному чи напівавтоматичному режимі, коли користувачу будуть представлені основні параметри трапецеїдальних функцій, які можна розрахувати на основі вихідних даних.

УДК 004.73(042.4)

А.А. Скрипниченко
(*Національний авіаційний університет, Україна)*

МЕТОДЫ СТАТИСТИЧЕСКОГО СИНТЕЗА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ АПРИОРНОЙ НЕОПРЕДЕЛЕННОСТИ

В процессе создания информационно-коммуникационных систем и сетей необходимо учитывать множество различных ограничений, параметров и условий оптимизации проектных решений. Часто в качестве критерия оптимизации компьютерной сети выбирают стоимость, а такие критерии, как среднее время задержки передачи сообщений, надежность и т.д., используют в качестве ограничений. Но для сетей масштаба мегаполиса или крупной корпорации данный подход не может дать оптимального решения, т.к. при эксплуатации и модернизации возникают отказы элементов и сбои в работе. Поэтому для таких сетей необходимо учитывать и ряд других критериев: производительность, надежность и безопасность, расширяемость и масштабируемость, прозрачность и безопасность, гибкость и поддержка разных видов трафика, управляемость и совместимость. Среди условий оптимизации и принятия концептуальных проектных решений в формальном отношении иногда предлагают выделить следующие разновидности: условия полной определенности, вероятностно-определенные и условия неопределенности [1]. К сожалению, условия полной определенности являются некоторым идеальным построением, которое носит чисто умозрительный характер и не встречается на практике.

Гораздо более реалистичным нам представляется деление на параметрическую и непараметрическую неопределенность [2]. В первом случае можно сделать достаточно обоснованные предположения об априорных параметрах и параметрах наблюдения. Применительно к информационным сетям, например, можно говорить о статистике сетевого трафика, в частности, о его самоподобии (фрактальности). Круг априорных распределений значительно сужается и сводится к не экспоненциальному семейству (распределениям с «тяжелыми» хвостами). При этом широко применяется байесовский подход. При непараметрической неопределенности приходится задаваться наименее благоприятными распределениями типа распределений с максимальной энтропией и получать некие асимптотические оценки ожидаемой эффективности. Для синтеза системы с оптимальной структурой можно применять минимаксный или адаптивный байесовский подход. Выбор того или иного конкретного метода зависит не только от масштаба информационной системы, но и от круга решаемых с ее помощью задач.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Сафонова И. Е. Методы формирования и принятия проектных решений в системах автоматизированного проектирования корпоративных компьютерных сетей // Известия высших учебных заведений. Поволжский регион Технические науки. Информатика, вычислительная техника. – № 4, 2008. – С. 41 – 49.
2. Репин В.Г., Тартаковский Г.П. Статистический синтез при априорной неопределенности и адаптация информационных систем. – М.: Сов. Радио, 1977. – 432 с.

УДК 004.03.052

А.В. Соловьев; Д.В. Майструк; В.Н. Бондаренко, к.т.н.
(НТУУ "КПИ", Украина)

ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ ГОЛОСОВОГО ТРАФИКА В КОРПОРАТИВНЫХ IP СЕТЯХ

В связи с возрастанием объемов голосового трафика (VoIP) в корпоративных IP сетях и обилием предложений от провайдеров IP-телефонии становится актуальной задача маршрутизации голосовых вызовов с учетом требований к качеству, стоимости и защищенности канала связи. В большинстве телефонных сетей используется статическая маршрутизация, основанная на общем международном телекоммуникационном плане нумерации [1]. В данной схеме любые изменения нумерации или маршрутизации – это длительный процесс, не отвечающий запросам сегодняшнего динамичного рынка телекоммуникаций.

Цель работы – формулировка требований к протоколу маршрутизации голосового трафика на основе анализа протоколов динамической маршрутизации, используемых в IP сетях и современных системах IP-телефонии (VoIP сетях): пограничная маршрутизация *BGP* [2], обмен шаблонами телефонных номеров *Cisco SAF/CCD* [3], маршрутизация по критерию наименьшей стоимости *LCR,* маршрутизация с контролем параметров качества связи *ASR*, *ACD*.

Проведенный анализ доступных протоколов маршрутизации позволяет сформулировать требования к протоколу динамической маршрутизации вызовов:

- анонсирование диапазона доступных номеров телефонов соседним маршрутизаторам;
- анонсирование стоимости и прочих параметров доступных маршрутов соседним маршрутизаторам;
- исследование параметров внешних каналов в режиме реального времени;
- выбор наилучшего маршрута и составление таблицы маршрутизации на основании множества параметров;
- обновление данных между пограничными маршрутизаторами только при изменении какого либо параметра (оптимизация загрузки сети);
- наличие в таблице маршрутизации и декларация минимум двух (основного и резервного) маршрутов для направления;
- возможность организации транзитного трафика;
- возможность безопасной авторизации между пограничными маршрутизаторами (защита от мошенничества с имитацией «суперканала»).

Удовлетворение перечисленных требований позволит при сохранении конкурентных преимуществ IP-телефонии поднять качество обслуживания на более высокий уровень.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. ITU-T Recommendation E.164 (11/2010)/ Интернет-ресурс: http://www.itu.int/rec/T-REC-E.164-201011-I/en
2. RFC 4271. A Border Gateway Protocol 4 (BGP-4). Tools. ietf. org. 2006-04-01.
3. *Левичев А.* Динамическая маршрутизация телефонных звонков с помощью SAF / CCD / Интернет-ресурс: http:// dbenda.blogspot.com/2011/12/saf-ccd-1.html

УДК 351.814.331:519.711.3

П.А. Станко
(Национальный авиационний университет, Украина)

МАТРИЦА КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ФУНКЦИОНИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

При оптимизации операционных систем реального времени (ОС РВ) в состав целевой функции входит большое количество основных и дополнительных параметров, от которых зависят ключевые показатели качества сервиса *KQIs*. Оптимизируемыми параметрами задачи являются следующие:

- оценки топологической и информационной сложности программ c_{ti} ;
- оценки надежности программных систем c_r ;
- оценки производительности ПО c_{sr} ;
- оценки уровня языковых средств c_{ll} ;
- оценки трудности восприятия и понимания программных текстов c_{per} ;
- оценки производительности труда программистов c_{lp} :
- метрика размера программы по Холстеду c_{sz} ;
- цикломатическое число Маккейба c_M :
- сетевые программные ошибки c_{ne} .

В табл. 1 приведены коэффициенты корреляции параметров оптимизации для гипотетической ОС РВ. Данные для расчета взяты из работы [1]. Для расчетов использовалась стандартная программа множественного корреляционного анализа, приведенная в [2].

Таблица 1

Коэффициенты взаимной корреляции оптимизируемых параметров

Параметр	Коэффициенты корреляции									
c_{ti}		1,0								
c_r		0,76	1,0							
c_{ll}		0,52	0,47	1,0						
c_{sr}		0,77	0,54	0,39	1,0					
c_{per}		0,34	0,28	0,55	0,77	1,0				
c_{lp}		0,72	0,91	0,22	0,78	0,46	1,0			
c_{sz}		0,38	0,88	0,75	0,72	0,63	0,56	1,0		
c_M		0,21	0,19	0,27	0,57	0,41	0,40	0,21	1,0	
c_{ne}		0,88	0,91	0,92	0,77	0,66	0,75	0,82	0,46	1,0
		c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}

Анализ корреляции между основными ключевыми параметрами необходимо проводить с учетом как статистических данных, так и физической природы возникающих ошибок. Результаты корреляционного анализа служат также ключевым индикатором мониторинга и регулирования потоковых данных в ОС РВ. Это необходимо для обеспечения своевременного обмена данными, прогнозирования и предотвращения перегрузок контролируемого сегмента ОС фрагмента. Таким образом, текущий мониторинг и управление уровнем эффективности работы ОС РВ является неотъемлемой частью задачи общего управления качеством сервиса *KQIs*.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. *Kreher R.* UMTS Performance Measurement: A Practical Guide to KPIs for the UTRAN Environment. - John Wiley & Sons, Ltd, 2006. – 227 pp.
2. Библиотека численного анализа НИВЦ МГУ http://www.srcc.msu.su/num_anal/lib_na/libnal.htm

УДК 004.65+004.7(043.2)

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

ЗАСТОСУВАННЯМ НЕЙРОННИХ МЕРЕЖ В СИСТЕМАХ ВИЯВЛЕННЯ АНОМАЛІЙ

Інформація в сучасному інформаційному суспільстві є найважливішим ресурсом людства і стає пріоритетним об'єктом уваги і результатом діяльності людини. Це породжує прагнення до володіння цим ресурсом, використовуючи різноманітні засоби здійснення несанкціонованого доступу до інформаційних ресурсів організацій, компаній та звичайних користувачів (алгоритмічні, програмні, апаратні та ін.), їх знищення, зміна або розголошування нелегальне використання ресурсів інформаційної системи, або приведення системи в недієздатний стан — усе це має украй небажані наслідки для власників цієї інформації. Тому проблема захисту інформаційних систем від зловмисного вторгнення, створення ефективних адекватних засобів інформаційного захисту є надзвичайно актуальною.

Сучасні системи управління є системами критичних застосувань з високим рівнем комп'ютеризації і виявляються дуже уразливими з точки зору дії інформаційної зброї [1], різноманітність його форм і способів дії, особливостей появи і застосування визначають гранично високу складність завдань інформаційного захисту.

З широкого спектру методів і засобів штучного інтелекту у сфері інформаційного захисту і інформаційного протидії в якості теоретичного базису ефективно використовуються штучні нейронні мережі, М-мережі, експертні системи і системи, засновані на знаннях, еволюційні і генетичні технології, мультиагентні технології та ін.

Особливо актуальним завданням у сфері інформаційної безпеки, що зажадала використання потужного арсеналу методів і засобів штучного інтелекту, стало завдання виявлення вторгнень і атак на автоматизовані інформаційні системи. Сучасні засоби виявлення вторгнень неминуче повинні включати інтелектуальні підсистеми, основу яких найбільшою мірою складають експертні системи і штучні нейронні мережі.

Одним з шляхів вирішення цієї проблеми є виявлення аномалій поведінки користувача або атак на комп'ютерну систему в реальному часі. Саме для цього і призначені системи виявлення вторгнень (*intrusion detection systems — IDS*). *IDS* зазвичай ділять на системи, які реагують на вже відомі атаки (так звані системи виявлення зловживань) і системи виявлення невідомих раніше аномалій. Для виявлення зловживань зазвичай використовуються експертні системи, робота яких заснована на реалізації набору відомих заздалегідь правил логічного висновку [2,3].

Системи виявлення аномалій, на відміну від експертних систем, є гнучкішими. Вони будуються на припущенні, що усі дії зловмисника обов'язково чимось відрізняються від поведінки звичайного користувача і їх можна розглядати як аномалії поведінки. Роботі системи виявлення аномалій передує період накопичення інформації, впродовж якого складається деяка концепція нормальної активності системи або користувача. Вона вважається еталоном (шаблон

нормальної поведінки), відносно якого оцінюються усі подальші дії. Проте інформація, генерована у великих системах, може досягати значних об'ємів і її необхідно найчастіше обробляти в реальному часі. Слід зазначити також, що виявлення аномальної поведінки користувача, погано формалізується. Тому аналіз аномальної поведінки користувачів необхідно проводити на основі використання інтелектуальних методів обробки даних, у тому числі із застосуванням нейронних мереж.

Ідея застосування нейронних мереж в системах виявлення аномалій, полягає в тому, щоб настроїти мережу на деякій "повчальній" безлічі значень вхід-вихід, яке характеризує поведінку користувача або системи взагалі. В якості виходу мережі може служити деякий прийнятий коефіцієнт "нормальності поведінки" або один з параметрів системи. В процесі налаштування нейронної мережі виявляються і фіксуються приховані закономірності, присутні у вхідних даних. Після навчання така нейронна мережа зможе аналізувати інформацію, що поступає, про роботу користувачів і виявляти відхилення від їх звичної поведінки в системі. Якщо реальна поведінка користувача відрізняється від очікуваного нейронною мережею, то робиться висновок про наявність аномалії в системі і можливому порушенні її безпеки [4,5,6].

Для повнішої і досконалішої побудови шаблону поведінки користувача можна запропонувати разом з переліком команд користувача враховувати послідовність їх виконання і здійснювати ідентифікацію поведінки користувача на основі цієї послідовності і виявляти аномальну діяльність користувачів в системі, заснованій на застосуванні нейронних мереж.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Гриняев С.Н.* Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.
2. *Denning D.* An Intrusion-Detection Model// IEEE Transactions on Software Engineering, Vol. SE-13, 1987, No. 2, P.276-283.
3. *Sebring M., Shellhouse E., Hanna M.*, Whitehurst R. Expert Systems in Intrusion
Detection: A Case Study//Proc. of the 11th National Computer Security Conference (Washington, USA), 1988, P. 315-321.
4. *Минаев Ю.Н.* Идентификация аномальных состояний трафика компьютерных сетей на основе парадигмы многомерных сетей / Ю.Н. Минаев, О.Ю. Филимонова, Н.Н. Гузий // Проблеми інформатизації та управління: зб. наук. праць. – 2010. – №3 (31). – С. 115-121.
5. *Мінаєв Ю.М.* Інтелектуальні технології ідентифікації аномальних станів комп'ютерних мереж / Ю.М. Мінаєв, О.В. Толстікова // Інтелектуальні технології лінгвістичного аналізу: матеріали міжнар. наук.-техн. конф., 26-27 жовтня 2010 р.: тези доп. – К., 2010. – С. 24.
6. Беляев А., Системы обнаружения аномалий: новые идеи в защите информации / А. Беляев, С. Петренко // Экспресс-электроника. – 2/2004. – [Електрон.ресурс].–Режим
доступу:http://citforum.ru/security/articles/anomalis/.

УДК 004.65+004.7(043.2)

О.С. Топиха
(Національний авіаційний університет, Україна)

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ UMTS ДЛЯ ПІДВИЩЕННЯ ШВИДКОСТІ І НАДІЙНОСТІ ПЕРЕДАЧІ ДАНИХ У БЕЗПРОВІДНИХ МЕРЕЖАХ

Для підвищення ефективності функціонування обчислювальної мережі шляхом підвищення надійності і швидкості передачі даних у безпровідних мобільних мережах зв'язку розглянемо використання універсальної системи мобільного зв'язку *UMTS* та проаналізуємо методики стандарту, що дозволяють розширити технологічні можливості сучасних мобільних облаштувань передачі великих об'ємів мультимедійної інформації.

На сучасному етапі розвитку технологій передачі даних по мобільних безпровідних мережах пріоритетною є проблема підвищення швидкості і надійності передачі інформації у реальному часі відповідно вимогам до систем критичного застосування.

Стандарт *UMTS* (*Universal Mobile Telecommunications System* - універсальна система мобільного зв'язку) знайшов найбільше поширення серед інших стандартів покоління *3G* на території Європи.

Технології мобільного зв'язку безперервно удосконалюються. Основний напрям розвитку цієї області пов'язаний зі збільшенням швидкості передачі і поліпшенням якості зв'язку.

Модернізація мереж мобільного зв'язку *UMTS* дозволяє надавати абонентам широкий перелік послуг: відеодзвінки, відеоконференції; високоякісні голосові дзвінки; завантаження файлів з високою швидкістю; мережеві ігри, мобільна комерція. Сама ж мережа стала більш місткою і можливість перевантаженості мережі зводиться до нуля.

Тільки у разі функціонування додатків в середовищі *UMTS* можна говорити про дійсно безпровідний доступ до Інтернету. Забезпечувана технологією швидкість трансмісії перевершує не лише швидкість інших сучасних рішень безпровідної телефонії, але також і деяких кабельних технологій.

Використання технології високошвидкісної передачі даних - *HSPA*, системи передачі даних за допомогою *N* антен і їх прийому *M* антенами *MIMO*, типів модуляцій вищого порядку (*16QAM/64QAM*) в системі *UMTS* у безпровідних мобільних мережах дозволяють значно підвищити швидкість і надійність передачі даних.

Впровадження технології *HSPA+* в технологію *UMTS*, з урахуванням виділеного частотного ресурсу, значно скорочує витрати операторів і тому підвищити ефективність функціонування обчислювальних мереж [1,2].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В.* Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. – 592 с.

2. Беспроводные технологии передачи данных и беспроводные сети будущего. – [Электронный ресурс]. – Режим доступа: http://www.venture-biz.ru/informatsionnye-tekhnologii/193-besprovodnye-seti-budushego

УДК 004.428

А.С. Трусь
(КрНУ імені Михайла Остроградського, Україна)

ФУНКЦІОНАЛЬНІ ОСОБЛИВОСТІ MS SQL SERVER 2012

На сьогоднішній день використання баз даних (БД) та інформаційних систем стає невід'ємною частиною функціонування будь-яких організацій та підприємств. У зв'язку з цим велику актуальність набуває освоєння принципів побудови і ефективного застосування відповідних програмних продуктів та інформаційних технологій, основні ідеї котрих базуються на концепції баз даних (БД) і систем управління базами даних (СУБД). Одним із таких програмних продуктів є MS SQL Server 2012.

На сьогоднішній день мова SQL[1] набула дуже широкого розповсюдження і фактично стала стандартною мовою реляційних баз даних. Microsoft, Sybase та Ashton-Tate першочергово об'єдналися для створення і випуску на ринок першої версії програми, яка отримала назву SQL Server 1.0 для OS/2 (в 1989 році), котра фактично була еквівалентом Sybase SQL Server 3.0 для Unix. Microsoft SQL Server 4.2 був випущений в 1992. Офіційний реліз Microsoft SQL Server версії 4.21 для ОС Windows NT відбувся одночасно з релізом самої Windows NT (версії 3.1). Microsoft SQL Server 6.0 був першою версією SQL Server, створеної виключно для архітектури NT, а Microsoft SQL Server 7.0 - першим сервером баз даних зі справжнім користувацьким графічним інтерфейсом адміністрування, а також концепцією оперативної аналітичної обробки (OLAP), в основі якої лежить багатомірне представлення даних. Подальший розвиток мови сприяв випуску нових версій SQL Server: Microsoft SQL Server 2005[2] та Microsoft SQL Server 2008[3]. Були вдосконалені продуктивність, клієнтські інструменти інтегрованого середовища розробки, змінено інструментарій процесів керування сховищами даних, сервер звітів, сервер OLAP та інтелектуального аналізу даних тощо. В результаті тісної конкуренція та швидкого розвитку СУБД корпорація Microsoft в 2012 році випускає новий MS SQL Server 2012, який включає низку вдосконалень для роботи з критичними бізнес-застосунками і бізнес-аналітикою як в традиційних дата-центрах, так і в приватних, публічних і гібридних хмарних середовищах[3]. Серед нових можливостей SQL Server 2012 можна виділити: SQL Server AlwaysOn (рішення підтримки високого рівня доступності даних та аварійного відновлення), xVelocity (технологія збільшення продуктивності сховищ даних та програм бізнес-аналітики), нові рішення в області візуалізації PowerPivot і PowerView для створення звітів, семантична модель бізнес-аналітики та інструмент для адміністраторів баз даних SQL Server Data Tools.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *K. Henderson*. Guru's Guide to SQL Server Architecture and Internals, The 1/e / Ken Henderson. - Addison – Wesley. – 2005. – 1056p.
2. *Р. Виейра* - Программирование баз данных MS SQL Server 2005. Базовый курс / Роберт Виейра. - Вильямс. – 2007. - 1066 стр.
3. *R. Mistry, S. Misner*. Introducing Microsoft® SQL Server® 2012/ Ross Mistry and Stacia Misner. - Microsoft Press. – 2012. – 250p.

УДК 004.681

О.І. Труш
(Національний авіаційний університет, Україна)

ОСОБЛИВОСТІ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ В БРАУЗЕРАХ

Відмови у програмних складових інформаційних технологій проектування, визначають необхідність результативного процесу тестування на збалансованих вирішень щодо швидкості, вартості процесів тестування.

Існує ряд сучасних автоматизованих систем тестування, що характеризуються такими недоліками, як застосування конкретної мови програмування, складністю налаштування серверу та адміністрування відповідних баз даних.

Для забезпечення необхідного рівня надійності, якості програмного забезпечення визначаються в основному такі підходи: продукто-орієнтований і процесо-орієнтований.

В першому - акцент робиться на оцінку якості шляхом тестування готового програмного продукту. Цей підхід базується на припущенні, що чим більше знайдено і усунено дефектів в програмних складових при тестуванні, тим вище його якість.

При процесо-орієнтованому підході наголос робиться на застосуванні заходів щодо запобігання, своєчасного виявлення і усунення дефектів, починаючи з самих ранніх етапів життєвого циклу. Цей підхід покладений в основу концепції якості програмних складових за стадартами ISO/IEC і реалізується в серії міжнародних стандартів, проектів стандартів і в робочих матеріалах цих організацій.

В процесі виявлення помилок, проводятся так звані структурні перегляди проектних матеріалів і аудит вихідних кодів програм. Замовнику необхідно заявляти пред'явлення даних матеріалів або про не дуже глибокому контролі ходу такого процесу. Він зацікавлений в тому, щоб в організації розробника були поставлені процеси. У цьому випадку замовник може бути впевнений, що якість контролюється і забезпечується в процесі розробки. Саме на це спрямовані відома модель Capability Maturity Model (CMM) та відповідний стандарт ISO.

Для зменшення впливу недоліків при виконання проекту сучасних автоматизованих систем тестування доцільно використовувати програмний інструмент Selenium, призначений для тестування web-додатків з виконанням тестування в браузері за визначеною методикою. Вказаний програмний інструмент працює в браузерах: Internet Explorer, Mozilla, Firefox, Opera, та ін., і використовує серверні мови написання тестів на Java, NET, Perl, Python та Ruby.

Дана система тестування включає Selenium IDE, -Core, - Remote Control, і може бути призначена для тестування сумісності сайту для різних браузерів та тестування функціонування сайту.

Інструмент Selenium Remote Control являє собою сервер, написаний на Java, що приймає команди для браузера через HTTP протокол, формує тести для web - сайтів на будь-якій мові програмування, що реалізує гнучку інтеграцію Selenium з існуючим тестовим фреймворком. Для написання тестів Selenium надає драйвери на вказаних мовах. Він також реалізує тестування складних реалізує web - інтерфейсів базованих на AJAX в системі постійної інтеграції -Continuous Integration system.

УДК 004.056.5:004.415.3 (043.2)

О.В. Фролов; О.В. Матвійчук-Юдіна; Р.В. Зюбіна
(Національний авіаційний університет, Україна)

БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ НА БАЗІ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ

Вступ. Оцінка ризиків організації є основним джерелом визначення вимог до інформаційної безпеки. Через оцінки ризиків ідентифікуються загрози активам, оцінюється їхня уразливість й імовірність виникнення загроз, а також можливий руйнівний вплив при реалізації несанкціонованих дій. **Постановка задачі.** Під поняттям управління інформаційними ризиками будемо розуміти процес виявлення, аналізу та зменшення ризиків інформаційної безпеки, які можуть принести або приносять шкоду інформаційній системі. Завдання управління ризиками включає в себе створення набору заходів (засобів контролю), які дозволяють знизити рівень ризиків до допустимої величини.

Метою даної роботи є визначення актуальності питання управління ризиками безпеки інформаційного об'єкту та визначення основних етапів.

До переваг застосування системи управління ризиками можна віднести: ідентифікацію інформаційних активів та їх цінності; ідентифікацію загроз і вразливостей інформаційної безпеки; оцінка і аналіз ризиків; планування засобів і методів мінімізації інформаційних ризиків згідно міжнародних стандартів серії ISO; впровадження засобів контролю та моніторинг; аудит та контроль інформаційних ризиків. Оцінка ризиків здійснюється, яким передує набір підготовчих заходів, що включають в себе узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи. Під час виконання оцінки ризиків здійснюється розробка профілів загроз, які включають в себе інвентаризацію і оцінку цінності активів, ідентифікація відповідних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки. Також процес управління ризиків проводить оцінку та обробку ризиків інформаційної безпеки, що включає в себе визначення величини та ймовірності нанесення збитку в результаті здійснення загроз безпеки з використанням вразливостей, які були ідентифіковані на попередніх етапах, визначення стратегії захисту, а також вибір варіантів і прийняття рішень по обробці ризиків. Величина ризику визначається як усереднена величина річних втрат організації в результаті реалізації загроз безпеці. Виділимо чотири етапи процесу управління ризиками безпеки: *оцінка ризику* (виявлення та пріоритезация ризиків для бізнесу); *підтримка ухвалення рішень* (пошук та оцінка рішень для контролю на основі визначених раніше правил аналізу витрат); *реалізація контролю* (розгортання та використання рішень для контролю, що знижують ризик для організації); *оцінка ефективності програми* (аналіз ефективності процесу управління ризиками та перевірка того, чи забезпечують елементи контролю належний рівень безпеки).

Висновок. Тобто процес управління ризиками дозволяє отримати необхідну інформацію про структуру, властивості інформаційного об'єкту і наявні ризики та вибрати механізми по мінімізації.

УДК 004.415.3 (043.2)

А.В. Чунарьова; П.С. Гузєєв
(Національний авіаційний університет, Україна)

АНАЛІЗ КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ. Швидкий розвиток інформаційних технологій наприкінці двадцятого століття призвів до значних змін у суспільстві. На перший план виступає інформація та її значний вплив на всі аспекти суспільного життя. Тобто основною цінністю будь-якої ланки суспільства являються інформаційні ресурси. Відповідно постає питання щодо захисту інформації. Виникла потреба у створенні стійких систем обміну, зберігання та обробки інформаційних потоків. Тому необхідним є впровадження нових та вдосконалення старих, проте актуальних методів програмного та технічного захисту.

Одним з варіантів формування актуального і стійкого захисту інформаційних потоків є використання криптографічних методів захисту. З економічної та практичної точки зору вказані методи є доцільними для використання по відношенню до автоматизованих систем різного призначення та необхідного рівня захисту. Відповідно дуже важливим є вибір і групування алгоритмів значної стійкості, криптоаналіз яких потребував би недопустимої кількості наявних обчислювальних та інформаційних ресурсів і можливостей. При побудові криптографічних систем захисту інформації необхідно звертати увагу на середовище їх функціонування, можливість реалізації захищених каналів передачі інформації, доцільність використання певних алгоритмів шифрування, спроможність системи протистояти різним загрозам, можливість виникнення певних видів загроз. Гнучкість криптографічних методів дає можливість використовувати їх в різних сферах функціонування, що значно скорочує затрати на реалізацію загальної системи захисту.

Метою даної роботи є проведення досліджень існуючих алгоритмів та криптосистем. Це необхідно виконувати з метою підвищення практичності та стійкості систем захисту. Необхідним є формування основних вимог до криптосистем нового покоління, що в свою чергу дасть можливість охарактеризувати основні можливості системи захисту.

Основна ідея криптографічних методів полягає у можливості реалізації конфіденційності та цілісності шляхом використання шифротекстів. Також криптографія використовується для забезпечення наступних завдань: забезпечення достовірності, тобто адресант повинен ідентифікувати адресата, а зловмисник, відповідно, не повинен мати можливість видавати себе за адресата; забезпечення цілісності, тобто адресант в будь-який момент може виконати перевірку тексту на можливі модифікації; не заперечення авторства, тобто адресат не повинен мати можливість заперечити проведення операції щодо відправки інформації.

Висновок. Аналізуючи характеристики алгоритмів криптографічного шифрування можна зробити висновок, що в першу чергу при реалізації криптосистем треба орієнтуватися на середовище функціонування. Найперспективнішими в наш час є криптосистеми, що поєднують в собі елементи як симетричних, так і асиметричних алгоритмів шифрування.

УДК 004.056.5:004.415.3 (043.2)

А.В. Чунарьова; О.В. Матвійчук-Юдіна; О.І. Варченко
(Національний авіаційний університет, Україна)

АНАЛІЗ НАПРЯМІВ АУДИТУ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Вступ. На сьогоднішній день організацій, мають розгалужені інформаційно-комунікаційні системи та мережі (ІКСМ)і тому на перше місце виходить завдання управління, як і інформаційними потоками та безліччю різноманітних захисних механізмів. Складність мережної інфраструктури, різноманіття даних та програм призводять до того, що при реалізації системи інформаційної безпеки необхідне здійснення регулярного аудиту та постійного моніторингу безпеки інформаційних потоків та структури ІКСМ. Аудит є невід'ємною частиною забезпечення інформаційної безпеки корпоративної мережі з точки зору забезпечення цілісності, конфіденційності та доступності.

Метою даної роботи є аналіз напрямів аудиту сучасних інформаційно-комунікаційних систем та мереж

Під поняттям аудиту автоматизованих інформаційних систем будемо розуміти перевірку матеріально технічних ресурсів організації, зокрема ІКСМ, систем безпеки на предмет їх відповідності встановленим вимогам та стандартам. Основними завданнями аудиту є: оцінка поточного стану інформаційної безпеки; ідентифікація та ліквідація вразливостей; мінімізація збитків від потенційно реалізованих загроз; відповідність державним, національним та міжнародним стандартам. Виконання даних завдань неможливе без відображення поточного стану захищеності ІКСМ на існуючі критерії захищеності інформації від несанкціонованого доступу. Базовим нормативним документом є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Критерії надають базу для розробки та модернізації ІКСМ, у яких мають бути реалізовані функції захисту інформації та порівняльну шкалу для оцінки надійності діючих механізмів захисту інформації. Окрім функціональних критеріїв захищеності існують таки критерії гарантій, що дозволяють оцінити коректність реалізації систем захисту.

Наступним документом, що регламентує порядок проведення аудиту та визначення слабких місць ІКСМ є міжнародний стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій». Стандарт описує інфраструктуру, у якій користувачі описують вимоги, розробники описують характеристики з безпеки комп'ютерної системи, а експерти визначають, чи задовольняє комп'ютерна система критеріям забезпечення безпеки .

Важливу роль у роль у стандартизації критеріїв, яким повинна відповідати ІКСМ грає асоціація ISACA. Даною асоціацією створено стандарт COBIT «Контрольні об'єкти інформаційних та суміжних технологій». Стандарт вводить 5 основних об'єктів, що являються ресурсами інформаційних технологій: дані, додатки, технології, обладнання, люди. Та на відміну від державного нормативного документу НД ТЗІ 2.5-004-99, описуються такі критерії оцінки інформації: ефективність, продуктивність, конфіденційність, цілісність, надійність, придатність, узгодженість. Частина стандарту, що зосереджена на порядку проведення аудиту, орієнтована на аудиту ІТ – процесів. COBIT складається з високорівневих цілей контролю, що охоплюють всі параметри інформаційних систем, враховують життєвий цикл та специфічні задачі ІКСМ.

УДК 004.056.5:004.415.3 (043.2)

А.В. Чунарьова; О.В. Матвійчук-Юдіна; Р.В. Зюбіна
(Національний авіаційний університет, Україна)

СИСТЕМИ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Актуальність. На сьогодні розмежування доступу в інформаційно-комунікаційних системах та мережах (ІКСМ) полягає в розділенні і організації доступу до інформації користувачів відповідно до їх функціональних обов'язків і повноважень. Задача такого розмежування доступу до інформації: скорочення кількості користувачів, що не мають до неї відношення при виконанні своїх функцій. Розмежування доступу користувачів ІКСМ може здійснюватися за наступними параметрами: виглядом, характером, призначенням, ступенем важливості і секретності інформації; способами її обробки: обчислення, запис, внесення змін, виконання команди; умовним номером терміналу; часом обробки та ін.

Постановка задачі. При проектуванні ІКСМ на її базі проводяться: розробка і реалізація функціональних задач по розмежуванню і контролю доступу до апаратури та інформації, як в рамках інформаційної системи в цілому, так і до відокремлених інформаційних ресурсів; розробка апаратних засобів ідентифікації та автентифікації користувачів та ресурсів системи; розробка програмних засобів контролю і управління розмежування доступу; розробка окремої експлуатаційної документації на засоби ідентифікації, автентифікації, розмежування і контролю доступу.

Метою роботи є дослідження та аналіз сучасних шаблонів та механізмів автентифікації.

Автентифікація являє собою процедуру перевірки дійсності ідентифікаторів. У процесі ідентифікації та автентифікації користувач або програма (претендент) запитує доступ у системи (верифікатора). На даний час виділяють чотири відмінні шаблони систем автентифікації: локальна автентифікація, пряма автентифікація, непряма автентифікація, автономна автентифікація. На практиці така класифікація може дотримуватись не завжди. Наприклад, існують багаторівневі системи безпеки, які можуть використовувати не один, а два або навіть більше шаблони систем автентифікації. Ці шаблони в загальному діляться на дві категорії: призначені для окремих автономних комп'ютерів і для віддаленого доступу.

Висновки. Проведені дослідження показали, що для сучасних ІКСМ найоптимальнішим варіантом буде використання шаблону непрямої системи автентифікації. Роль автентифікаційного сервера, що приймає запити на автентифікацію від інших серверів повинен відігравати сервер бази даних. На сервері бази даних повинна підтримуватись єдина актуальна база особистих даних користувачів, що спрощує процес адміністрування. Комплекс засобів захисту ІКСМ для забезпечення надійного захисту повинен розміщуватися на сервері бази даних, але при цьому за рахунок відповідних клієнтських додатків охоплювати всі комп'ютери робочих груп, адміністраторів та керівництва, а також всі сервери, що містяться в автоматизованій системі.

УДК 004.415.3 (043.2)

А.В. Чунарьова; Д.М. Миколишин
(Національний авіаційний університет, Україна)

СУЧАСНІ АЛГОРИТМИ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ

Вступ. На сьогоднішній день розвиток інформаційних технологій привів до появи електронного документообігу. Проте використання електронного документообігу, пов'язане з збереженням документів від несанкціонованого копіювання, модифікації і підробки. Для вирішення проблеми захисту інформації від несанкціонованого доступу необхідне використання сучасних специфічних засобів і методів захисту. Одним з поширених методом такого захисту є електронний цифровий підпис. Під поняття електронного цифрового підпису (ЕЦП) будемо розуміти реквізит електронного документа, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису, що дає змогу ідентифікувати власника власника електронного документа. На даний час ЕЦП виконує такі функції контролю цілісності електронного документу та підтвердження його авторства.

Метою даної роботи являється аналіз сучасних алгоритмів формування та перевірки ЕЦП.

На сьогоднішній день асиметрична схема формування ЕЦП є найбільш поширена і використовується частіше, ніж симетрична схема. Це обумовлено тим фактом, що симетричні схеми для формування і розшифрування підпису використовують один і той самий ключ. Якщо зашифровану інформацію потрібно передавати, то в даному випадку потрібно і передавати ключ шифрування, саме це може створити проблему, адже якщо канал передачі не захищений, то ключ може бути перехоплений зловмисником. В асиметричних системах цей недолік відсутній, оскільки кожний учасник має пару ключів: відкритий та секретний, які зв'язані між собою. При цьому формування ЕЦП відбувається за допомогою секретного ключа відправника, а перевірка підпису – за допомогою відкритого ключа, тому необхідність передачі секретного ключа відсутня. У зв'язку з цим, асиметрична система має набагато більшу криптостійкість, тому саме їй надають перевагу під час створення ЕЦП. Загальновизнана схема ЕЦП, заснована на асиметричному алгоритмі охоплює три процеси: 1) генерація відкритого та закритого ключа; 2) формування підпису; 3) перевірка підпису. На сьогоднішній день існують такі алгоритми створення цифрового підпису: Схема RSA, Эль-Гамаля, DSA, ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002

В даний час більшість відомих алгоритмів ЕЦП засновано на складності рішення однієї з трьох завдань: дискретного логарифмування; факторизації; дискретного логарифмування на еліптичних кривих.

Висновок. Провівши аналіз асиметричних алгоритмів можна зробити , що найбільш оптимальною є схема створення ЕЦП RSA, яка виділяється своєю високою надійністю та простотою і найчастіше використовується в програмному забезпеченні для створення формування і перевірки ЕЦП. Якщо говорити в загальному про симетричні та асиметричні схеми, то перевагу, звичайно ж, надають асиметричним, так як саме вони забезпечують достатню криптостікійкість.

УДК 004.75

А.Л. Шеневидько
(Национальный авиационный университет, Украина)

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Во-первых, как следует понимать термин «облачные вычисления» (“cloud computing”)? Что в нем подразумевается под «облаком»? Правильно понимать «облако» как метафору удаленного вычислительного датацентра. Таким образом, программное обеспечение фактически предоставляется пользователю как сервис. Пользователю облачных вычислений не нужно заботиться ни об инфраструктуре, ни о фактическом программном обеспечении, «облако» успешно скрывает все технические и программные детали.

В первые идея была озвучена J.C.R. Licklider, в 1970 году. В эти годы он был ответственным за создание ARPANET (Advanced Research Projects Agency Network). Его идея заключалась в том, что каждый человек на земле будет подключен к сети, из которой он будет получать не только данные, но и программы. А, например, ученый John McCarthy высказал идею о том, что вычислительные мощности будут предоставляться пользователям как услуга (сервис). На этом развитие облачных технологий было приостановлено до 90-х годов, после чего ее развитию поспособствовал ряд факторов. Из определения и истории видно, что основой для создания и быстрого развития облачных вычислительных систем послужили крупные интернет сервисы, такие как Google, Amazon и др.

К достоинствам облачных вычислений можно добавить следующее: доступность, низкая, стоимость, гибкость, надежность, безопасность, большие вычислительные мощности. Но также есть и недостатки: постоянное соединение с сетью, программное обеспечение и его кастомизация, конфиденциальность, надежность, дороговизна оборудования. В настоящее время выделяют три категории «облаков»: **Публичное облако**, **Частное облако и Гибридное облако**. Так же облачные системы можно разделить по видам услуг, которые они предоставляют: все как услуга ,инфраструктура как услуг, платформа как услуга ,программное обеспечение как услуга, аппаратное обеспечение как рабочее место, данные как услуга , безопасность как сервис.

Облачные технологии MicrosoftOffice 365 для образовательных учреждений позволяет пользоваться всеми возможностями «облачных» служб, помогая экономить время и деньги, а также повышает работоспособность учащихся и сотрудников. Базовый функционал, включающий в себя облачные версии Exchange Online, Share Point Online и Office Web Apps, Skydrive, а также Lync Online с возможностью видеоконференций будет предоставляться бесплатно. Так же для образование был сделан специальный сервис Google Apps Education Edition – это Web-приложения на основе облачных вычислений, предоставляющие студентам и преподавателям учебных заведений инструменты, необходимые для эффективного общения и совместной работы.

Службы Google для образования, по мнению разработчиков, «содержат бесплатный набор инструментов, который позволит преподавателям и студентам более успешно и эффективно взаимодействовать, обучать и обучаться, всего лишь нужен интернет».

УДК 004.9

С.С. Шмигельський
(КрНУ ім. М.Остроградського, Україна)

ДОСЛІДЖЕННЯ І РОЗРОБКА ПРОГРАМНОГО МОДУЛЮ ЗАХИСТУ ВИХІДНИХ КОДІВ ВЕБ-ДОДАТКІВ

Сучасний етап розвитку суспільства характеризується інтенсивним розвитком інформатизації. Як наслідок, розвивається комп'ютерне піратство. Для протидії комп'ютерному піратству активно використовуються методи захисту програмного забезпечення від аналізу і несанкціонованої модифікації. Одним з таких методів є обфускація. Обфускація (від лат. Obfuscare - затінювати, затемнювати; і англ. Obfuscate - робити неочевидним, заплутаним, збивати з пантелику) або заплутування коду - приведення вихідного тексту або виконуваного коду програми до виду, який зберігає її функціональність, але ускладнює аналіз та розуміння алгоритмів роботи об'єкту обфускації [1].

В роботі досліджено існуючі методи, програми обфускації і деобфускації вихідних кодів [2, 3], а також розроблено методики захисту PHP–скриптів від аналізу та модифікацій на основі заплутування кодів та даних. Розвинена методологія заплутуючих перетворень стосовно програмного забезпечення, також програмних систем захисту інформації в блоках захисту логіки роботи. Розроблена класифікація існуючих методів заплутування кодів.

Розроблений програмний модуль здатний ускладнювати аналіз для мови програмування PHP. Ця програма користується лінгвістичним методом, у якому реалізовані заміни імен змінних, функцій, класів, видалення пробілів, переносів рядків. Також використовуються криптографічні методи на вибір користувача : base64 або CAST_256, які кодують програмний код, та додають декодер, що буде викликаний перед трансляцією.

У процесі виконання даної роботи були проаналізовані існуючі методи обфускації та деобфускації. Реалізована програма, яка має можливість обфускувати переданний програмний PHP–скрипт, а також частково відновити вихідний код за допомогою деобфускатора.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Чернов А. В.* «Интегрированная среда для исследования "обфускации" программ»: http://www.ict.nsc.ru/ws/Lyap2001/2350.

2. *Barak B., O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang.* On the (Im)possibility of Obfuscating Programs II LNCS 139. - 2001. -P. 1-18с.

3. *Stephen Drape, Irina Voiculescu*: Creating Transformations for Matrix Obfuscation. SAS 2009: 273-292 с.

УДК 004.056.5:004.415.3 (043.2)

О.К. Юдін, д.т.н.; О.І. Варченко, к.т.н.; Р.В. Зюбіна
(Національний авіаційний університет, Україна)

СИСТЕМИ ТА МЕТОДИ ВИЯВЛЕННЯ НСД В СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

Актуальність. Сучасні мережі передачі даних є основою розвитку інформаційного суспільства, а саме вони здійснюють зберігання, передачу й обробку інформації. Тому важливим атрибутом функціонування сучасних інформаційно-комунікаційних системах та мережах (ІКСМ) з умов забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів є здійснення процесів захисту інформації від несанкціонованого доступу (НСД). На сьогодні розгалужені інформаційні мережі функціонують під управлінням різних операційних систем, на перше місце виходить завдання управління всім різноманіттям захисних механізмів. Базовим підходом до вирішення цієї проблеми є використання **систем та методів виявлення НСД.** Застосування даних методів та систем унеможливить НСД та зловживання інформаційними ресурсами в сучасних ІКСМ.

Постановка задачі. Під поняття системи виявлення НСД будемо розуміти безліч різних програмних і апаратних засобів, що аналізують порядок використання інформаційних ресурсів, що захищають, і, у разі виявлення яких-небудь підозрілих або просто нетипових подій, здатні здійснювати певні самостійні дії з виявлення, ідентифікації і усунення причин, що їх викликали.

Метою даної роботи є проведення аналізу методів та систем виявлення вторгнень на основі протидії несанкціонованому доступу в сучасних ІКСМ.

Всі методи виявлення НСД можна розділити на два класи: методи виявлення аномалій і методи виявлення зловживань. Методи першого класу базуються на наявності готового опису нормальної поведінки спостережуваних об'єктів, і будь-яке відхилення від нормальної поведінки вважається порушенням. Методи виявлення НСД засновані на описі відомих порушень або атак: якщо спостережувана поведінка деякого об'єкту співпадає з описом відомої атаки, поведінка об'єкту вважається атакою. Існують різні підходи до класифікації систем виявлення вторгнень, але в практичній діяльності найчастіше застосовується така класифікація НСД, що враховує принципи практичної реалізації таких систем: виявлення атак на рівні мережі; виявлення атак на рівні системи (вузла). Існує і ще одна класифікація систем виявлення атак. Вона ділить системи по тому, коли аналізуються дані - **в реальному масштабі часу** або **після здійснення події**. Як правило, системи виявлення атак на рівні мережі працюють в реальному режимі часу, тоді як системи, що функціонують на рівні вузла, забезпечують автономний аналіз реєстраційних журналів операційної системи або додатків.

Висновок. Використання описаних видів методів та систем виявлення НСД дозволяє посилити політику безпеки і внести велику гнучкість до процесу експлуатації мережних ресурсів ІКСМ.

УДК 004.056.5:004.415.3 (043.2)

О.К. Юдін, д.т.н.; О.І. Варченко, к.т.н.; О.В. Фролов
(Національний авіаційний університет, Україна)

МЕТОДИ ОРГАНІЗАЦІЇ СУЧАСНИХ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Вступ. На сьогодні інформаційні ресурси корпоративних мереж потребують захисту від різноманітних за своєю сутністю зовнішніх та внутрішніх загроз, які можуть призвести до зниження цінності та якості інформаційних ресурсів або призвести до їх повної втрати. На даний час комплексний захист інформації являє собою сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази і спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації в сучасних інформаційно-комунікаійних системах та мережах (ІКСМ). Система інформаційної безпеки забезпечує цілісність, доступність і конфіденційність критично важливої інформації, а отже, життєздатність і ефективність в цілому самої інформаційної системи.

Метою даної роботи являється визначення пріоритетних напрямів та засобів захисту інформації від несанкціонованого доступу.

Комплексна система захисту інформації включає заходи та засоби, що реалізують способи, методи, механізми захисту інформації від:

1.витоку інформації технічними каналами (побічні електромагнітні випромінювання, акустоелектричних канали і т.д.);

2.несанкціонованих дій та несанкціонованого доступу до інформації (підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, застосування закладних пристроїв чи програм і т.д.);

3.спеціального впливу на інформацію (формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту).

Для кожної конкретної інформаційно-комунікаційної системи склад, структура та вимоги до системи захисту визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації (рис. 1.1).

З погляду методології в проблемі захисту інформації від несанкціонованого доступу необхідно виділити два напрями:

1.забезпечення і оцінювання захищеності інформації в ІКСМ, що функціонують;

*2.*реалізацію та оцінювання засобів захисту, що входять до складу компонентів, з яких будується інформаційно-комунікаційна система та мережа (програмних продуктів, засобів обчислювальної техніки і т. ін.), поза конкретним середовищем експлуатації.

Висновок. Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її оброблення в ІКСМ. Захист інформації має бути забезпечений на всіх стадіях життєвого циклу ІКСМ, на всіх технологічних етапах оброблення інформації і в усіх режимах функціонування. Життєвий цикл ІКСМ включає розроблення, впровадження, експлуатацію та виведення з експлуатації.

УДК 004.056.32

О.К. Юдін, д.т.н.; О.В. Фролов
(Національний авіаційний університет, Україна)

КОНЦЕПЦІЯ ОРГАНІЗАЦІЇ ІТ-ОСВІТИ В УКРАЇНІ

Великі корпорації та ІТ-компанії, по праву вважаються піонерами концепції «подвійної освіти»: обов'язкова базова підготовка і додаткова сертифікована освіта на прикладних курсах. Дана ідеологія дозволяє студентам отримати університетський диплом в рамках спеціальних освітніх ІТ-курсів. Взаємодія між університетом та ІТ-компаніями, спрямована на просування практичних дисциплін та спеціалізованих курсів для отримання повної вищої освіти є необхідною умовою для розвитку інформаційної безпеки.

Формування галузі інформаційної безпеки базується на вирішенні цілого комплексу взаємопов'язаних проблем, які можна умовно об'єднати в такі групи: концептуальні, нормативні та організаційні.

Безпека інформаційних технологій (БІТ) - найбільш прогресивна і швидко розвивається галузь, а в перспективі і контролюючий сектор світової індустрії послуг. Можливість зайняти на базі БІТ-технологій серйозні лідируючі позиції при невисоких початкових капіталовкладеннях, послужила основною причиною розвитку даного напрямку в багатьох країнах світу. Однією з необхідних умов і ключових факторів, які визначають успіх держави або безпосередньо компанії на ринку ІТ-послуг - наявність високо кваліфікованих кадрів.

На сучасному етапі розвитку суспільства та інтеграції інформаційного простору, велика кількість міжнародних університетів (спільно з компаніями ІТ) досягли значних успіхів на ниві вищої освіти в сфері інформаційної безпеки. Дана система навчання ефективно поєднує структуру вищих академічних установ та відповідність вимогам сучасним стандартам і ринку праці, які гарантують отримання якісної вищої освіти в області БІТ-технологій.

Переходячи до розгляду освітніх програмах університетів і компаній-партнерів, перш за все, слід відзначити їх головну відмінну рису - суворо практичну спрямованість на вирішення професійних завдань. Орієнтація на роботу з сучасними і широко поширеними програмами в умовах, максимально наближених до реальності, гарантує отримання знань і вмінь, які дійсно затребувані ринком, і дозволяють випускнику приступити до продуктивної роботи негайно після працевлаштування.

Крім того, додаткові курси підвищення кваліфікації в галузі ІТ і БІТ технологій, можуть і повинні стати базою для об'єднання існуючих елементів навчальних програм університету і прикладних задач практичної роботи.

Національні традиції, а також наявність в країні людських ресурсів, які володіють високим рівнем базових знань, створюють ідеальні умови для розвитку цілісної системи підготовки кадрів в області безпеки інформаційних технологій.Навчальних програм вузів традиційно орієнтовані на отримання фундаментальних знань (які, безумовно, є важливою і невід'ємною частиною підготовки фахівця), але не здатні компенсувати відсутність роботи з програмними продуктами та технологіями, які широко використовуються в сучасному бізнесі.

УДК 004.056.5 (043.2)

О.К. Юдін, д.т.н.; А.В. Чунарьова; О.В. Фролов
(Національний авіаційний університет, Україна)

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ СУЧАСНИХ ІКСМ

Актуальність. Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють формування, поширення й використання інформації, а також; системи регулювання суспільних відносин, що виникають при цьому.

На сьогодні інформаційна сфера є системоутворюючим чинником життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових безпеки держави.

На даний час приватна й ділова інформація має комерційну вартість і тому важливою є проблема її захисту від несанкціонованого доступу та атак. Нині спостерігається тенденція до підвищення кількості атак та несанкціонованого доступу, які захоплюють контроль над віддаленою інформаційною системою, копіюють та передають зловмисникам персональні дані, іншу конфіденційну або, навіть, секретну інформацію. Проблема комплексного захисту сучасних інформаційно-комунікаційних систем та мереж (ІКСМ) інформації стає ще актуальнішою, якщо мова йде про захист великої кількості оперативної інформації, що обробляється в сучасних комп'ютерних системах.

Постановка задачі. На сьогодні розпочато створення механізмів реалізації законів, підготовку законопроектів, що регламентують суспільні відносини в інформаційній сфері. Разом з тим, аналіз стану інформаційної безпеки України показує, що її рівень не повною мірою відповідає потребам суспільства і держави.

Метою роботи є аналіз існуючої нормативно-правової бази в галузі забезпечення інформаційної безпеки сучасних ІКСМ та побудови комплексної системи захисту інформації (КСЗІ).

Під поняттям нормативно-правового забезпечення слід розуміти сукупність правових норм, що визначають порядок створення, правовий статус і функціонування захищених ІКСМ, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів. Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації; статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані з інформаційною безпекою; правові положення окремих видів процесу керування та управління доступом в захищених ІКСМ; порядок створення й використання захищених ІКСМ; етапи побудови КСЗІ.

Висновки. Отже, в ході роботи було досліджено основні нормативно-правові документи з точки зору побудови КСЗІ в сучасних ІКСМ.

UDC 351.864:001.89

N.P. Kadet
(NAU, Ukraine);
M.V. Soroka
(Central Research and Development Institute of Armament and Military Engineering, Ukraine)

ANALYSIS OF RISKS AT REALIZATION OF INFORMATIVE PROJECTS

Development of information systems, which relates primarily to the introduction advanced technologies, requires more and more investment. Despite the fact that all projects begin with full confidence in their realization and almost all of them have well-developed business plan (program) and budget, however their completion, quite often, ,postponed indefinitely and expenditures frequently been exceeding planning targets.

Appearance of many factors which in advance are not taken into account, result in growth of risks of successful realization of project. Therefore the goal of this report is an analysis and estimation of project risks. Under a risk we understand an indefinite condition or event which can put possibility of successful realization of project under a threat, for example, cost, technical descriptions (quality) and terms of realization.

The analysis of risks includes authentication of possible risks and their evaluation. The purpose of authentication is an exposure of risks and forms of display. The evaluation of risks consists of measuring of actual level of danger of every separate risk and in determination of degree of its influence on a project. Risk estimation plugs determination of risk parameters – probabilities of offensive of unfavourable events, time, in influence and size of possible losses (losses) recognition, as a rule, to their prognosis on the certain period of time.

There are two factors in basis of risk: probability and vagueness. Risk factors are such events, which can come in the process of realization of concrete measure and influence on a cost, temporal and indexes from their planned values. Risk factors are subdivided into external and internal. Factors, that are conditioned by reasons that is unconnected directly with activity of enterprise, behave to external. Internal risk factors are factors appearance of that conditioned or it is descendant activity of enterprise. The processes of making decision in a management projects take place, as a rule, in the conditions of presence that or other measure of vagueness, conditioned such factors:

- by incomplete knowledge of all parameters, circumstances, situation, for the choice of optimum decision, and also by impossibility of adequate and exact account of all accessible information;
- by the presence of factor of chance, that realization of factors, which it is impossible to foresee and forecast even in probabilistic realization.

It should be noted that realization of project goes in the conditions of vagueness and risks these two categories interdependent.

Vagueness, in wide sense, it is inaccuracy of information about the terms of realization of project, including related to them by charges and results. Thus, an analysis of risk is the major stage of analysis of informative project. Within the framework of analysis the task of concordance decides two practically opposite aspirations-maximization of income and minimization of risks of project.

Thus, a problem of risk estimation at realization of informative projects is actual and leads to further research in this area, in-depth analysis of foreign experience.

УДК 681.3

A.V. Korochkin; O.V. Rusanova
(NTUU "KPI", Ukraine)

AN OVERVIEW OF THE GRID SCHEDULING ALGORITHMS

We consider the Grid Computing as a high performance computing environment that allows sharing of geographically distributed resources across multiple administrative domains and used to solve large scale computational demands. In the Grid environment, users can access the resources transparently without information where they are physically located. To achieve the promising potentials of computational Grids, job scheduling is an important issue to be considered [1,2].

We analyze Grid computing unique characteristics that make the design of scheduling algorithms more challenging such as: heterogeneity, autonomy, performance dynamism. We consider the main scheduling methods for Grid – centralized, decentralized and hierarchical and justify the advantages of last one [2, 3].

In this paper formed the initial data for Grid scheduling, such as application model (DAG task graph), Grid computing model (system graph) and optimization criteria. We propose the scheduling algorithms taxonomy for Grid computing. We concentrate our activity in static scheduling where we find Grid system node which guarantee minimal run time of a given application. The preferences of list scheduling for static approaches are defined [3].

An hierarchical Grid scheduling system model is considered and the main functions of Grid Scheduler and Local Resource Managers. The correct definition of applications run time is the main trouble in classic hierarchical Grid scheduling approach. That's why we propose improved hierarchical Grid scheduling method where application run time we determine in static. For this an effective list scheduling algorithm for homogeneous and heterogeneous nodes of Grid systems is proposed. The main steps of this algorithm are described.

Developed a software model for the implementation of our approach. Proposed list scheduling algorithm for homogeneous and heterogeneous Grid system nodes was compared with well known HEFT. We've got increase efficiency in the range of 10 up to 20%.

Advanced hierarchical scheduling method and develop algorithm can significantly improve the efficiency of Grid computing systems. Proposed program model can be used for software development of modern Grid systems.

REFERENCES

1. *K.Vivekanandan, D.Ramyachitra* A Study on Scheduling in Grid Environment/International Journal on Computer Science and Engineering, Vol.3 No.2,2011.940-950.

2. Technical Report No. 2006-504 Scheduling Algorithms for Grid Computing: State of the Art and Open Problems. *Fangpeng Dong and Selim G.* Akl. School of Computing,Queen's University Kingston, Ontario January 2006.

3. *Кулаков Ю.А., Русанова О.В., Шевело А.П.* Иерархический способ планирования для GRID.-Вісник НТУУ "КПІ". Сер. Інформатика, управління та обчислювальна техніка. - 2009. Випуск 51. - С.57 – 66.

UDC 656.7.052.001.76(043.2)

Voynov Ivan
(NAU, Ukraine)

ANYCAST IN DELAY TOLERANT NETWORKS

Anycast is a service that allows a node to send a message to at least one, preferably only one, of the members in a group. Anycast can be used to implement resource discovery mechanisms which are powerful building blocks for many distributed systems, including file sharing etc.

Delay Tolerant Networks (DTNs), as a class of useful but challenging networks, are receiving more and more attention.

The idea behind anycast is that a client send packets to any one of a few possible servers offering a particular service but does not really care any specific one.

In DTNs anycast means that a node wants to send a message to any one of a destination group and intermediate nodes help to deliver the message by leveraging their mobility when no contemporaneous path exists between the sender node and any node of the destination group.

Anycast in mobile ad hoc networks and in the Internet has been studied extensively in the past, due to the unpredictability of network connectivity and delay, and limited storage capacity, anycast in DTNs is a quite unique and challenging problem. It requires both re-definition of anycast semantics and new routing algorithms.

Moreover, in unicast in DTNs, the destination of a message is determined when it is generated, while in anycast, the destination can be any one of a group of nodes and during routing, both the path to a group member and the destination can change dynamically according to current mobile device movement situation.

In this paper, I'll also define three semantics models of anycast in DTNs, namely CM (Current Membership), TIM (Temporal Interval Membership) and TPM (Temporal Point Membership Model), which unambiguously define the intended receivers of a message in the anycast routing. Based on the model, I'm also propose a novel routing metric named EMDDA (Expected Multi-Destination Delay for Anycast) which utilizes the uncontrolled random moving characteristic of mobile devices.

REFERENCES

1. *D. Katabi and J. Wroclawski*. A Framework for Scalable Global IPAnycast (GIA). In Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Stockholm, Sweden, 2000.
2. *S. Jain, K. Fall, and R. Patra*. Routing in a Delay Tolerant Network. In Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pages 145–158, Portland, OR, USA, 2004.

Наукове видання

ЗБІРНИК ТЕЗ

VI Міжнародної
науково-технічної конференції

«КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2013)

11-13 червня 2013 року

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

Підп. до друку 06.06.13. 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 – 58, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002

ДЛЯ НОТАТОК