

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

**ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
ХІІ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІ**

**«КОМП'ЮТЕРНІ СИСТЕМИ
ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»
(CSNT-2019)**

28–30 березня 2019 року

Київ 2019

Збірник тез доповідей XII Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2019), м. Київ, 28–30 березня 2019 р., Національний авіаційний університет. – К.: НАУ, 2019. – 134 с.

Рецензенти:

О.А.Чемерис – д.т.н., с.н.с., заступник директора з наукової роботи Інституту проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України;

В.Є.Мухін – д.т.н., професор, професор кафедри математичних методів системного аналізу Науково-технічного університету України «Київський політехнічний інститут ім. І.Сікорського»;

О.Д.Азаров – д.т.н., професор, декан факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету.

Збірник тез доповідей укладено за матеріалами XII міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2019). У доповідях розглянуті наукові, технічні та технологічні проблеми побудови, проектування сучасних комп'ютерних систем, засоби і методи моделювання комп'ютерних мереж, проблеми захисту ресурсів в інформаційних системах, технології підготовки авіаційних фахівців.

Редакційна колегія:

І.А.Жуков – д.т.н. (головний редактор)

Н.В.Журавель – (відповідальний секретар)

О.В.Азаренко – д.т.н.

В.П.Гамаюн – д.т.н.

В.І.Дровозовов – к.т.н.

В.В.Козловський – д.т.н.

В.М.Опанасенко – д.т.н.

М.К.Печурін – д.т.н.

О.В.Толстікова – к.т.н.

Рекомендовано до друку вченою радою Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету (протокол № 2 від 18 березня 2019 р.).

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

© Національний авіаційний університет, 2019

ЗМІСТ

Андрєєв В.І., Андрєєв О.В. МЕТОД ОПТИМАЛЬНОЇ ЕКСТРАПОЛЯЦІЇ ВИПАДКОВИХ НЕСТАЦІОНАРНИХ СИГНАЛІВ НА ФОНІ ЗАВАД.....	10
Антонов В.К. ВЕКТОРНИЙ ПРОСТІР КОНТИНУАЛЬНОЇ РОЗМІРНОСТІ.....	12
Балакин С.В. МЕТОД ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ В КОМПЬЮТЕРНОЙ СЕТИ.....	14
Бахмач А.В. СИСТЕМИ ЗАХИСТУ В ОПЕРАЦІЙНИХ СИСТЕМАХ MICROSOFT WINDOWS 7 / 8 / 10.....	16
Безверщенко Є.І., Гузій М.М., Проценко М.М. ТЕХНОЛОГІЇ ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	18
Бейсембаев А.А., Ербосынова А.С., Павленко П.Н., Власенко Ю.В. МЕТОД ОПРЕДЕЛЕНИЯ ПРОСТРАНСТВЕННЫХ ПОЛОЖЕНИЙ МАНИПУЛЯЦИОННОГО РОБОТА.....	20
Боровик В.М., Малюк І.А. МОДЕЛІ ПРОЕКТУВАННЯ У КЛІЄНТ-СЕРВЕРНИХ МЕРЕЖАХ ІЗ ЧЕРГАМИ ТА ПРІОРИТЕТАМИ.....	22
Васильєв В.М. КОМП'ЮТЕРНА ОБРОБКА ДАНИХ В МЕРЕЖЕВІЙ БАГАТОПОЗИЦІЙНІЙ СИСТЕМІ СПОСТЕРЕЖЕННЯ.....	25
Винничук С.Д., Місько В.М. МЕТОД МНОЖИНОГО КВАДРАТИЧНОГО k-РЕШЕТА З ВИКОРИСТАННЯМ СИГНАЛЬНИХ ОСТАЧ ПРИ ПРОСПЮВАННІ ПРОБНИХ ЗНАЧЕНЬ.....	27

Водоп'янов С.В., Ушаков К.С., Пастухов О.А. ОСОБЛИВОСТІ ПОБУДОВИ СУЧАСНОЇ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ АЕРОВУЗЛА.....	29
Гамаюн В.П. ТЕХНОЛОГИЯ ОБРАБОТКИ ПСЕВДО УПОРЯДОЧЕННИХ МАССИВОВ.....	31
Гамаюн В.П. АДАПТИРОВАННЫЕ СТРУКТУРЫ ДАННЫХ ДЛЯ ВЫСОКОРОИЗВОДИТЕЛЬНОЙ ОБРАБОТКИ.....	33
Гончар С.Ф. ПІДХІД ДО АНАЛІЗУ РИЗИКУ НА ОСНОВІ ТЕОРІЇ КОМПЛЕКСНИХ ЧИСЕЛ.....	35
Гришко Н.С. ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ВІДДАЛЕНОГО ДОСТУПУ.....	37
Grinenko O.O. ANALYSIS OF SOFTWARE ECOSYSTEMS USING PETRI NETS.....	39
Давиденко А.М., Висоцька О.О. ВИЗНАЧЕННЯ ФУНКЦІЇ МОНІТОРИНГУ СТАНУ САНКЦІОНОВАНИХ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ ЗА ДОПОМОГОЮ АНАЛІЗУ ЇХ КЛАВІАТУРНОГО ПОЧЕРКУ.....	41
Даниліна Г.В., Коваль Д.С. ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ	43
Демчик В.В., Корочкін О.В., Русанова О.В., Тизунь В.Ю. ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБЧИСЛЕНЬ В ГЕТЕРОГЕННИХ КОМП'ЮТЕРНИХ СИСТЕМАХ.....	45
Дрововозов В.І., Бут С.В., Голего Н.М. МОЖЛИВОСТІ НАДАВАНІ КВАНТОВИМИ ОБЧИСЛЕННЯМИ.....	47

Дрововозов В.І., Голованьов Є.О., Журавель Н.В.	
МЕТОДИКА РОЗРОБКИ ВЕБ-ДОДАТКУ ДЛЯ RSS-АГРЕГАЦІЇ.....	49
Zhukov I.A., Kravets I.M.	
SWISS KNIFE OF EMBEDDED SYSTEMS.....	51
Zhukov I.A., Pechurin N.K., Kondratova L.P.	
METHOD FOR THE AVIATION SECTOR OBJECTS SAFETY ENSURING RESOURCES DISTRIBUTION BASED ON THE MACROECONOMIC INDICATOR	53
Заріцький О.В., Павленко П.М., Захарчук Т.М.	
КОМП'ЮТЕРНА СИСТЕМА АНАЛІТИЧНОЇ ОЦІНКИ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ТА ЇЇ ОПЛАТИ.....	55
Іскренко Ю.Ю.	
СХЕМА МНОЖИНОГО ДОСТУПУ В ШИРОКОСМУГОВІЙ БЕЗДРОТОВІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ LTE.....	58
Кадет Н.П.	
ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЛЬОТНУ ПІДГОТОВКУ В АВІАЦІЇ ПОВІТРЯНИХ СИЛ.....	60
Кірхар Н.В.	
МОДУЛЬНЕ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	61
Коваленко Д.І., Калитюк А.В.	
ОРГАНІЗАЦІЯ ПЕРЕДАЧІ ДАНИХ МІЖ КЛІЄНТАМИ МЕРЕЖІ НАВІГАЦІЙНИХ ПРИСТРОЇВ G2S.....	64
Ковалев Н.А.	
ОРГАНИЗАЦИЯ ВЫЧИСЛЕНИЙ ПОД УПРАВЛЕНИЕМ ПОТОКА ДАННЫХ.....	66

Коврижкін О.Г., Рибасова Н.О. МОДУЛЬ АНАЛІЗУ ДОСТОВІРНОСТІ СУПУТНИКОВИХ СИГНАЛІВ НА ОСНОВІ ІМІТАЦІЙНОЇ МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ.....	68
Коцюр А.Б., Пряхін Д.В. ПРИНЦИПИ ФУНКЦІОНУВАННЯ ПРОТОКОЛІВ IP Security.....	70
Kudrenko S.A., Pushkin Yu.A. BUG TRACKING SYSTEM FOR IT PROJECT.....	72
Курченко О.А., Брже夫ська З.М., Гребенніков А.Б. МЕТОДИ ТЕСТУВАННЯ ТА ПІДТВЕРДЖЕННЯ ВІЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ.....	74
Лазаренко С.В., Войтенко С.Д., Німченко Т.В. АНАЛІЗ МЕТОДІВ ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА.....	76
Лапач М.В. ДЕФЕКТИ КОДУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	78
Лукашенко В.В. МЕТОД ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ.....	80
Мазенко Д.В., Журавель С.В. ОСОБЛИВОСТІ ЗАХИСТУ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ.....	82
Мартінова О.П., Журавель Н.В. ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ МЕТОДОМ БАГАТОКРИТЕРІАЛЬНОЇ МАРШРУТИЗАЦІЇ.....	84
Мельничук О.В., Пастухов О.А., Фатькова О.О. МОНІТОРИНГ ЗНОСУ ТА ПРОГНОЗУВАННЯ ВІДМОВ МОДУЛІВ КОСМІЧНИХ АПАРАТІВ ЗА ДОПОМОГОЮ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ ТА ОПЕРАЦІЙНОЇ СИСТЕМИ РЕАЛЬНОГО ЧАСУ	86

Надточій В.І.	
ПРОГНОЗУВАННЯ РОЗГАЛУЖЕНЬ КОНВЕЄРНОГО ПРОЦЕСОРА.....	88
Павленко П.М., Темніков А.В., Балушок К.Б.	
СИСТЕМА УПРАВЛІННЯ ТЕХНІЧНОЮ ПІДГОТОВКОЮ МАШИНОБУДІВНОГО ПІДПРИЄМСТВА.....	90
Пащенко Н.В., Мокійчук В.М., Самойліченко О.В.	
ОЦІНЮВАННЯ РИЗИКІВ ЛАБОРАТОРНИХ КОМП'ЮТЕРНИХ СИСТЕМ ІЗ ЗАСТОСУВАННЯМ МЕТОДУ FMEA.....	92
Поперешняк С.В.	
СУМІСНІ РОЗПОДІЛИ ДЕЯКИХ СТАТИСТИК ВИПАДКОВИХ БІТОВИХ ВЕКТОРІВ.....	94
Protsenko M.M., Guzii M.M.	
SD-WAN TECHNOLOGY PROSPECTS.....	96
Ракицький В.А.	
ВИКОРИСТАННЯ МЕРЕЖЕВОГО RTSP - ПРОТОКОЛУ В СИСТЕМАХ, ЩО ПРАЦЮЮТЬ З МУЛЬТИМЕДІА ДАНИМИ.....	98
Рахманов А.Т., Хамдамов Р.Х., Керимов К.Ф., Камалов Ш.К.	
АЛГОРИТМ АВТОМАТИЧЕСКОГО ОБНАРУЖЕНИЯ УЯЗВИМОСТИ ВИДА SQL ИНЪЕКЦИИ.....	100
Rusanova O.V., Korochkin A.V., Shevelo O.P.	
CLASSIFICATION OF SCHEDULING PROBLEMS FOR MODERN PARALLEL COMPUTER SYSTEMS.....	102
Сімченко С.В., Таратонova О.С.	
ДЮДНІ ПРИЙМАЧІ З НАНОТЕКСТУРОВАНИМ ПОКРИТТЯМ ДЛЯ ОПТОВОЛОКОННИХ ЛІНІЙ ЗВ'ЯЗКУ.....	104

Sinko Yu.	
THE USE OF CLOUD COMPUTING IN HIGHER EDUCATION INSTITUTIONS.....	106
Терентьева И.Е., Уланский В.В., Мачалин И.А.	
ИССЛЕДОВАНИЕ УРОВНЯ ДОСТУПНОСТИ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ МЕТОДА МОНТЕ-КАРЛО.....	108
Ткаченко В.В., Комаров М.Ю.	
ОСНОВНІ ПІДХОДИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	110
Толстікова О.В., Бут С.В., Дехтяренко А.Т.	
ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСІ РОЗРОБКИ ПРИКЛАДНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	112
Fomina N.B.	
NEURAL NETWORKS AND UNIVERSITY EDUCATIONAL PROCESS FORECASTING.....	114
Хамдамов Р.Х., Рахманов Х.Э.	
ДИСТАНЦИОННЫЙ МОНИТОРИНГ ЗЕМЕЛЬ СЕЛЬСКОХОЗЯЙСТВЕННОГО НАЗНАЧЕНИЯ ПО МУЛЬТИСПЕКТРАЛЬНЫМ СПУТНИКОВЫМ СНИМКАМ SENTINEL 2.....	116
Хамдамов Р.Х., Керимов К.Ф.	
МЕТОДЫ БЛОКИРОВАНИЯ УЯЗВИМОСТЕЙ ВИДА XSS НА ОСНОВЕ СЕРВИС- ОРИЕНТИРОВАННОЙ АРХИТЕКТУРЫ.....	119
Хамдамов Р.Х., Рахманов Х.Э., Сакиев Т.Р.	
РАСПОЗНАВАНИЕ ДЫМА И ОГНЯ МЕТОДОМ КОНТУРНОГО АНАЛИЗА ПО ДАННЫМ ВИДЕОИЗОБРАЖЕНИЯ.....	121
Ходаков Д.В., Горіна В.В.	
МОДЕЛЬ ІЄРАРХІЇ ПРОЦЕСІВ ТЕСТУВАННЯ.....	125

Чемерис О.А., Сушко С.В.

МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ
ОПТИМІЗАЦІЇ РОБОТИ МІКРОПРОЦЕСОРНИХ
СИСТЕМ.....127

Чуба І.В.

АЛГОРИТМ БАГАТОКРИТЕРІАЛЬНОГО
ВИБОРУ МАРШРУТІВ У ГЕТЕРОГЕННІЙ
МЕРЕЖІ.....130

МЕТОД ОПТИМАЛЬНОЇ ЕКСТРАПОЛЯЦІЇ ВИПАДКОВИХ НЕСТАЦІОНАРНИХ СИГНАЛІВ НА ФОНІ ЗАВАД

Вирішення задач екстраполяції випадкових сигналів (ВНС), до яких відноситься і трафік комп'ютерних мереж, займають важливе місце як в теорії випадкових процесів, так і в практичному використанні цієї теорії в різних галузях науки та техніки.

Недостатньо вивченими залишаються задачі екстраполяції випадкових нестационарних сигналів на фоні стаціонарних та нестационарних завад.

Для вирішення цієї задачі було запропоновано метод двопараметричної оптимальної екстраполяції ВНС на фоні завад.

Математичну модель ВНС можна представити у вигляді:

$$Y(t) = a_0 + a_1 t_i^g,$$

де a_0 – початкова точка процесу, a_1 – швидкість процесу, γ – коефіцієнт нелінійності процесу, t_i – моменти часу процесу.

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

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

Двопараметричний метод оптимальної екстраполяції, який по двом значенням попередніх спостережень за ВНС – Y_1 і Y_2 , та апіорній інформації про параметри цього сигналу дозволяє отримати оцінку Y_3^* майбутнього значення Y_3 момент часу t_{n+1} шляхом оптимального вибору параметру оптимізації α по відповідному критерію оптимізації при мінімальній похибці спостережень e :

$$e = Y_3 - Y_3^*.$$

В основу методу, поставлено задачу визначення оптимальних вагових коефіцієнтів α_{1opt} , α_{2opt} за критерієм мінімуму дисперсії $\min D_{\epsilon}(\alpha_{1opt}, \alpha_{2opt})$ похибки оптимального екстрапольованого значення випадкового нестационарного сигналу на фоні завад.

Для виконання екстраполяції необхідно мати набір апіорної ймовірностної інформації про ВНС. Це наступний набір для точок спостереження Y_1 , Y_2 : – математичні сподівання – m_{Y1} , m_{Y2} ;

дисперсії – D_{Y_1} , D_{Y_2} (або їх середньоквадратичні відхилення σ_Y^2 , $\sigma_{Y_2}^2$); кореляційна функція – $K_Y(t_1, t_2)$. Крім того, треба визначити інтервали спостереження ΔT та екстраполяції τ , а також величину потужності завади σ_ξ^2 . Далі треба довизначити відсутні параметри для точки ВНС t_3 , для якої треба здійснити екстраполяцію: математичне сподівання m_{Y_3} , дисперсію D_{Y_3} , середньоквадратичне відхилення $\sigma_{Y_3}^2$, та відповідні кореляційні функції $K_Y(t_1, t_3)$, $K_Y(t_2, t_3)$.

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

$$Y_3^* = a_1 Y_1 + a_2 Y_2 ,$$

де α_1 , α_2 – параметри двопараметричної оптимізації, що позначаються як α_{1opt} та α_{2opt} . Ці параметри визначаються наступним чином:

$$a_{1opt} = \frac{b_1 a_{22} - b_2 a_{12}}{a_{11} a_{22} - a_{21} a_{12}} ,$$

$$a_{2opt} = \frac{a_{11} b_2 - b_1 a_{21}}{a_{11} a_{22} - a_{21} a_{12}} ,$$

де

$$a_{11} = m_{Y_1}^2 + D_{Y_1} , \quad a_{12} = m_{Y_1} m_{Y_2} + k(t_1, t_2) ,$$

$$b_1 = m_{Y_1} m_{Y_3} + k(t_1, t_3) , \quad a_{21} = m_{Y_1} m_{Y_2} + k(t_1, t_2) ,$$

$$a_{22} = m_{Y_2}^2 + D_{Y_2} , \quad b_2 = m_{Y_2} m_{Y_3} + k(t_2, t_3) .$$

В роботі запропонована методика довизначення необхідних для екстраполяції параметрів, та був проведений експеримент методом статистичного імітаційного моделювання, аналіз результатів якого показує працездатність і ефективність запропонованого методу екстраполяції навіть при низькому відношенню середньоквадратичних значень сигнал / шум, ілюструють новизну, корисність та ефективність методу оптимальної екстраполяції випадкового нестационарного процесу на фоні завад.

ВЕКТОРНИЙ ПРОСТІР КОНТИНУАЛЬНОЇ РОЗМІРНОСТІ

Ідея є продовженням уявлень про простір (евклідовий, Мінковського, Гільберта). Введемо вісь неперервного номера y координати $q(y)$. $y \geq 0; \in R$ пробігає значення від 0 (час) до ∞ (протяжність – починаючи з 1). Розмірність координат із дробовими y визначимо інтерполяцією по цілим y . За побудовою дійсний принцип відповідності для дискретної розмірності, де заміною сум на інтеграли одержуємо:

$$|Q| = \left| \sqrt{\int_0^\infty q^2(y) dy} \right|; \quad \langle Q_1, Q_2 \rangle = \int_0^\infty q_1(y) q_2(y) dy; \quad \text{div} A(y, Q) = \int_0^\infty \frac{\partial A(y, Q)}{\partial q(y)} dy;$$

$ds^2 = \int_0^\infty \int_0^\infty g(i, j) dy(i) dy(j)$ - норму континуального вектора; скалярний

добуток; дивергенцію векторного поля; метрику. Функція g утворюється просторовими градієнтами хвильової функції, при $g=0$ пустий простір не має протяжності і часу. Принцип невизначеності Гейзенберга доповнимо множником номера $\Delta y \cdot \Delta p \cdot \Delta x \geq h$. Побудуємо континуальне рівняння Шредінгера для хвильової функції

$$\begin{aligned} \int_0^\infty a(y) \frac{\partial^{b(y)} \Psi(y, q(y))}{\partial q(y)^{b(j)}} dy + \frac{\partial^2 \Psi(y, q(y))}{\partial y^2} = 0 \\ \frac{\partial^{b(y)}}{\partial q(y)^{b(y)}} \Psi(y, q(y)) = \frac{1}{24} (b^4(y) - 10b^3(y) + 35b^2(y) - 50b(y) + 24) \Psi(y, q(y)) - \\ - \frac{1}{6} (b^4(y) - 9b^3(y) + 26b^2(y) - 24b(y)) \frac{\partial}{\partial q(y)} + \Psi(y, q(y)) \\ + \frac{1}{4} (b^4(y) - 8b^3(y) + 19b^2(y) - 12b(y)) \frac{\partial^2}{\partial q(y)^2} \Psi(y, q(y)) - \\ - \frac{1}{6} (b^4(y) - 7b^3(y) + 14b^2(y) - 8b(y)) \frac{\partial^3}{\partial q(y)^3} \Psi(y, q(y)) + \\ + \frac{1}{24} (b^4(y) - 6b^3(y) + 11b^2(y) - 6b(y)) \frac{\partial^4}{\partial q(y)^4} \Psi(y, q(y)). \end{aligned}$$

Функції $a(y)$ (вагових коефіцієнтів) і $b(y)$ (порядку диференціювання

уздовж y) визначаються із принципу відповідності дискретній розмірності, умови осциляції хвильової функції уздовж y ; дробові похідні інтерполяцією. Функція $a(y)$ містить масу частинки – хвилі. Всі фізичні величини є вимірюваннями руху матерії. Матерія без руху не існує. Маса є виміром руху уздовж розмірності;

оператор її оцінки $\hat{m} = \int_y h_1(y, q_y) \left(\frac{\partial \Psi(y, q(y))}{\partial y} + \frac{\partial \Psi(y, q(y))}{\partial q} \cdot \frac{dq(y)}{dy} \right)^2 dy$;

де функція h_1 задовольняє перетворенням Лоренца. Ознаки підтвердження квантово-хвильової природи інерції-маси-енергії є в експериментах на адронному колайдері: «зникнення» протонів в каналі прискорення; матеріалізація струй, (які не є значимими); осциляції (міжрозмірності) сонячних нейтрино. Когерентна осциляція частинок уздовж розмірності цілеспрямовано впливає на інерцію і вагу макротіл. Можливо створення генератора когерентних міжрозмірностних коливань. Міжрозмірностною осциляцією пояснюється темна матерія і гравітація. Встановлюється зв'язок між квантовою механікою і гравітацією. Цікавою є задача розвитку-еволюції матерії, простору, його розмірності. За «початок» приймемо стан простору із нескінченно малою розмірністю близькою до нуля. Інакше матерія і простір виникали би «із нічого», аби («ненульовий початок», «Великий вибух») було би «контргіпотетичне» питання про походження початку.

Введемо континуальні мережі – у континуальному просторі станів їх вірогідності змінюються з інтенсивністю потоків як у моделі Колмогорова, і діють обміни нижчого рівня між обмінами вищого рівня – подібно до фракталів. Тобто є потоки з нецілим номером, і їх множина має потужність континуума. Це дозволяє суттєво розширити можливість створення математичних моделей фізичних, технічних, біологічних (онкологія), економічних, соціальних процесів.

МЕТОД ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ В КОМПЬЮТЕРНОЙ СЕТИ

Технический прогресс обусловил ситуацию, когда большинство информации не только на предприятиях, но и у рядовых пользователей сохраняется и обрабатывается на удаленных вычислительных станциях. Для более удобной работы пользователей, оперативного обмена, гибкой обработки и хранения информации в инфраструктуру предприятий и проживания граждан встраиваются компьютерные сети, которые в настоящее время стали неотъемлемой частью различных сфер деятельности и отдыха человека. Как следствие, возникает актуальная проблема защиты таких компьютерных сетей, что в свою очередь предполагает разработку соответствующих алгоритмов, методов и средств обнаружения несанкционированной деятельности в сетях.

Разработка новых алгоритмов, методов, программных и аппаратных средств не только выявления несанкционированных действий в сетях, но и повышения эффективности выявления таких действий является актуальной задачей сегодняшнего дня [1].

Рассмотрены и проанализированы основные методы, а также обоснованно введены дополнительные элементы в предложенные модели для ускорения работы и повышения общей производительности. Описан подход к процессу обучения и распознавания аномалий в компьютерной сети.

Предложен метод выявления аномального поведения, который основан на диагностике вторжений в компьютерные сети и не требует постоянного обновления сигнатур. Для моделирования были выбраны и применены операторы теории Демпстера-Шейфера для формирования соответствующего решения о наличии или отсутствии несанкционированных действий в сети. Это обусловило выделение тех признаков несанкционированных действий, которые определенным образом характеризуют действия злоумышленника или определенную атаку. На основе анализа математических моделей диагностики и алгоритмов выявления изменений определены параметры процесса диагностирования, в том числе алгоритмы контроля временных фрагментов и

формирования данных для определения симптомов и сигнатур вторжений. Приведена и обоснована необходимость объединения нескольких симптомов для получения точного диагноза [2].

Решение задачи выявления аномальной активности (которая не обязательно является вторжением злоумышленника) состоит из следующих шагов:

1. Создание дерева диагностики и формирование массивов с состояниями нормального функционирования системы.
2. Сравниваются данные состояний в сетке диагностирования на выявление отклонений от нормального состояния активности системы в сторону отклонений (аномалий).
3. При обнаружении сигнатур, которые соответствуют отклонением, дерево диагностирования оповещает о нарушениях.
4. При обнаружении сигнатур, которые соответствуют состояниям нормального функционирования системы, дерево диагностирования не препятствует работе системы.

Выполнение данных шагов позволит выявлять и обрабатывать аномальную активность пользователя и системы.

Теоретическая ценность полученных результатов заключается в разработке новых и улучшении существующих методов анализа аномальной активности в сетях. В частности, выбраны инструменты для моделирования и внедрения предложенных методов с целью повышения эффективности выявления аномальных действий в компьютерных сетях. Выполнено исследование эффективности данного метода и доказана его корректность в сравнении с существующими решениями.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Balakin S.V., Zhukov I.A. Detection of computer attacks using outliner method / I.A. Zhukov., S.V. Balakin. – Young Scientist, 2016. – 91-93 pp.
2. Балакин С.В. Организация пресечения вторжений в компьютерные сети алгоритмами выявления изменений. Проблеми інформатизації та управління: зб. наук. праць. – К.: НАУ, 2017. – № 3(59). – С. 65-69.

**СИСТЕМИ ЗАХИСТУ В ОПЕРАЦІЙНИХ СИСТЕМАХ
MICROSOFT WINDOWS 7 / 8 / 10**

Користувачі все частіше приділяють увагу захищеності інформації або даних, що знаходяться на комп'ютері, тому, обираючи операційну систему, прагнемо, аби всі дані були надійно захищені.

Одним із основних критеріїв при виборі операційної системи є її захищеність. Інформація, що зберігається на комп'ютері, є інтелектуальною власністю користувача, а тому потребує захисту, як і будь-яка інша власність.

Розглянуто системи захисту в операційних системах Microsoft Windows 7/8/10 та результати досліджень цих систем, а також можливості протидії, що базуються на вже існуючих стандартах Common Weakness Enumeration, Open Web Application Security Project та National Vulnerability Database.

З виходом нових операційних систем та їх оновленням, ризик натрапити на найпопулярніші вразливості поступово зменшується.

Компанія Microsoft – лідер на ринку операційних систем, у своїх останніх трьох системах пропонує користувачу цілий ряд гнучких механізмів безпеки, які націлені захистити операційну систему від несанкціонованого викрадення інформації та протидіяти основним вразливостям операційної системи.

Слід розуміти, що у кожній операційній системі є важливі файли, що потребують захисту, а захист бібліотек та фреймворків є пріоритетним. Тому належний їх захист є запорукою безпечного програмного забезпечення.

З виходом операційної системи Windows 7 були розширені можливості шифрування диску BitLocker, додавши програму BitLocker To Go, яка дозволяє шифрувати знімні носії.

Розглянуто технології DEP, ASLR та SEHOP, служба UAC, технологія обернено – орієнтованого програмування, технологія DirectAccess, технології шифрування (BitLocker та EFS), механізм довірених сертифікатів SSL.

Для деяких вразливостей не зазначено механізм, який може запобігти проблемі – це означає, що у Microsoft немає відповідного

механізму для захисту або дана вразливість не здійснюється програмним шляхом.

Підвищення ролі криптографічних методів захисту інформації є дуже потужним етапом захисту операційної системи, так як їх злам є, майже, технічно неможливим. Розробники нових операційних системах Windows все більше і більше уваги приділяють методам захисту від несанкціонованого доступу до інформації.

Завдяки загальному переліку вразливостей операційних систем можна визначити на яких ієрархічних рівнях зосереджується найбільша кількість помилок.

Основна кількість помилок зосереджена у вихідному коді програми, тому, на дану ділянку націлені основні системи захисту.

Методологія дослідження систем захисту операційних систем базується на загальному переліку вразливостей, які були представлені Національним інститутом стандартів і технологій (NIST).

Велика кількість вразливостей націлена на веб-додатки, проте компанія Microsoft з кожним роком активно впроваджує нові системи захисту від такого виду вразливостей.

За результатами аналізу стандарту Common Weakness Enumeration запропонована відповідність вразливостям до поданих механізмів безпеки, які повністю або частково допомагають запобігти тим чи іншим вразливостям.

Компанія Microsoft випускає оновлення для своїх операційних систем, тим самим підвищуючи рівень захисту даних. Завдяки останньому оновленню Windows 10, CreatorsUpdate, операційна система отримала кардинальні зміни.

Незважаючи на те, що абсолютно надійного захисту для операційної системи просто не існує, можна констатувати, що проаналізовані операційні системи Microsoft Windows 8 / 10 стали надійнішими, аніж їхні попередники.

¹ Є. І. Безвершенко,² М. М. Гузій, к.т.н.,² М. М. Проценко, к.т.н.,¹ Ужгородський Національний університет, Ужгород² Національний авіаційний університет, Київ

ТЕХНОЛОГІЇ ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Еволюція систем мережної безпеки відбувається за двома паралельними напрямками - централізованого управління загрозами (Unified Threat Management, UTM) та розвитку комплексних систем безпеки: міжмережеві екрани (NGFW), системи попередження вторгнень (IPS), антивіруси, антиспам, Web-фільтри, захист від витоків інформації (DLP). На рис.1 наведена ілюстрація динаміка ринку систем мережної безпеки.

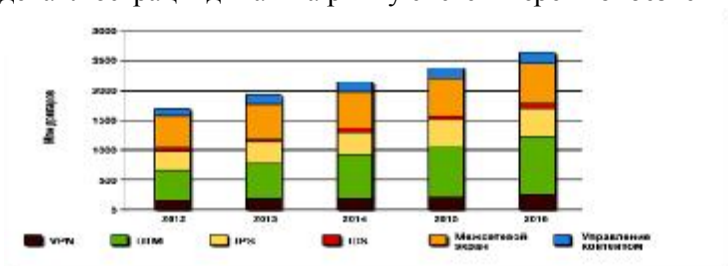


Рис.1. Динаміка ринку систем мережної безпеки

Схема взаємодії засобів безпеки UTM наведена на рис.2.

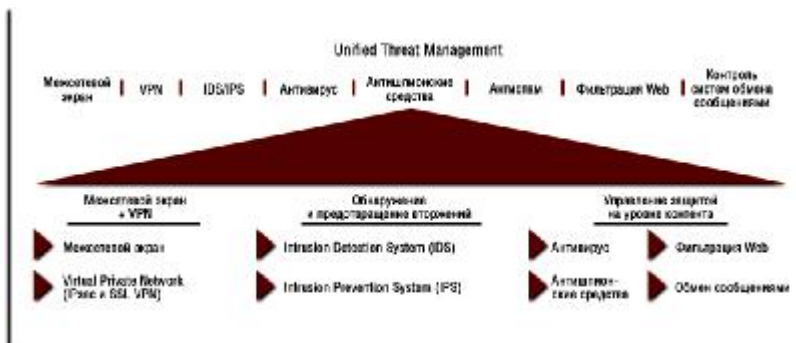


Рис.2. Взаємодія засобів безпеки UTM

Інтегровані засоби UTM реалізують наступні функції мережної безпеки: міжмережевий екран, запобігання несанкціонованого доступу до мережі, антивірусний шлюз, антиспамовий шлюз, IPSec-VPN, фільтрація контенту, розкриття SSL/TLS-трафіка, балансування навантаження, запобігання витоку даних.

На рис.3 представлено квадрант Гартнера для компаній на ринку UTM. Лідером рішень (правий верхній квадрат) в плані функціоналу і реалізації технології централізованого управління вразливостями є компанія Fortinet (офіційний дистриб'ютор в Україні - компанія ERC).

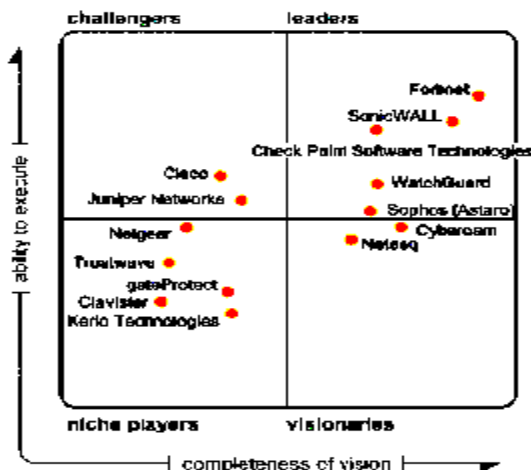


Рис. 3. Квадрант Гартнера для компаній на ринку UTM

Аналіз переваг та недоліків систем UTM показав доцільність їх використання в якості систем захисту інформації в компаніях рівня SMB і недостатній функціонал систем UTM для захисту великих корпоративних мереж.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Електронний ресурс. <https://www.osp.ru/lan/2013/06/13036284/>.
2. Електронний ресурс. <https://vido.com.ua/article/4334/biezopasnost-po-sistiemie-all-inclusive-ili-iedinaia-sistiemia-upravleniia-zashchitoi-ot-ughroz-utm-ot-kompanii-fortinet/>

¹А. А. Бейсембаев, к.т.н.,¹А. С. Ербосынова²П. Н. Павленко, д.т.н.,²Ю. В. Власенко, н.с.¹НАО КазННТУ им. К.И. Сатпаева, Казахстан²Национальный авиационный университет, г. Киев, Украина

МЕТОД ОПРЕДЕЛЕНИЯ ПРОСТРАНСТВЕННЫХ ПОЛОЖЕНИЙ МАНИПУЛЯЦИОННОГО РОБОТА

Проектирование системы управления манипуляционным роботом (МР) в пространстве координат OXYZ предусматривает решение обратной задачи кинематики. Кинематическую систему МР можно представить в виде последовательно соединенных звеньев, имеющих геометрические размеры, которые можно задать векторами $\vec{a}_i$, $i=1,2,\dots,n$, где n – число звеньев МР.

В общем случае вектор значений обобщенных координат $Q^j (q_1^j, q_2^j, \dots, q_n^j)^T$, определяет длину и ориентацию векторов $\vec{a}_j$ и задаёт точку позиционирования схвата МР $A_j(x_j, y_j, z_j)$.

Тогда постановку задачи можно представить в виде минимизации некоторого критерия качества, например, энергетических затрат, вида:

$$J(Q) = \sum_{j=1}^{m-1} \sum_{i=1}^n c_i |q_i^j - q_i^{j+1}| \rightarrow \min, \quad (1)$$

при ограничении, в виде логического выражения, описывающего рабочее пространство МР [2]:

$$\forall A_j(x_j, y_j, z_j), j = \overline{1, m}: (D_1)^j L_1^j (D_2)^j L_2^j \dots L_{n-1}^j (D_n) = 1, \quad (2)$$

где $[D_i] \in [D]_i(x, y, z) \leq 0$; m – число точек, аппроксимирующих траекторию; c_i – коэффициент, характеризующий динамические показатели привода i -ой степени; L – знаки логических операций [2].

Таким образом, метод определения пространственных положений МР можно представить в виде последовательных этапов информационных преобразований следующим образом:

Этап 1. Ввод исходных значений: координат точек траектории движения схвата $A_j(x_j, y_j, z_j)$, $j=1,2,\dots,m$, логические выражения $L_1, L_2, \dots, L_{n-2}$, описывающие рабочее пространство МР, $\Delta q_1, \Delta q_2, \dots, \Delta q_n$ величины шагов поиска решения, начальное положение конфигурации МР $Q^0(q_1^0, q_2^0, \dots, q_n^0)^T$, начальное положение схвата в точке $A_0(x_0, y_0, z_0)$.

Этап 2. Если выполняется условие $\forall A_j(x_j, y_j, z_j), j = \overline{1, m}: L_1 = 1$, то перейти к этапу 3, в противном случае делается вывод, что задача неразрешима.

Этап 3. Присвоить начальные значения $j=1; i=1$.

Этап 4. При заданном значении q_i^j определяем вид логического выражения L_i^{j-1} .

Этап 5. Если координаты точки $A_j(x_j, y_j, z_j)$ не удовлетворяют логическому условию $L_i^{j-1} = 1$, то определить знак согласно выражению $S_j = \begin{cases} \text{Sign}(|\bar{a}_j| - |\bar{a}_{j-1}|), \text{ для линейной оси} \\ \text{Sign}(\text{Arg} \bar{a}_j - \text{Arg} \bar{a}_{j-1}), \text{ для угловой оси} \end{cases}$ и перейти к этапу 6, в противном случае перейти к этапу 7.

Этап 6. $q_i^j = q_i^{j-1} + S_j \cdot \Delta q_i$, перейти к этапу 5.

Этап 7. Увеличить значение $i=i+1$.

Этап 8. Если $i \leq n-2$, то перейти к этапу 4, в противном случае присвоить $j=j+1$ и перейти к этапу 9.

Этап 9. Определить аналитически значения обобщенных координат q_{n-1}^j, q_n^j .

Этап 10. Если $j \leq m$, то присвоить $i=1$ и перейти к этапу 4.

Этап 11. Вывод значений матрицы $Q(q_i^j)$.

Определение пространственных положений звеньев МР осуществлено в виде задачи условной оптимизации, с критерием вида (1), при ограничениях вида (2). При этом рабочее пространство МР описано в виде логических выражений, с использованием R – функции. Для практической реализации метода планируется использование инструментальных средств системы моделирования цифрового производства Dassault Systèmes DELMIA (Франция).

МОДЕЛІ ПРОЕКТУВАННЯ У КЛІЄНТ-СЕРВЕРНИХ МЕРЕЖАХ ІЗ ЧЕРГАМИ ТА ПРІОРИТЕТАМИ

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

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

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

Розглядається ситуація управління запитами, які очікують своєї обробки. Фізична інтерпретація черги має інформаційний характер і може пояснюватися по-різному. У нашому випадку деталі цього механізму не мають принципового значення. Як зазначалося на початку, протоколи обробки запитів постійно ускладнюються, а загальна тенденція – пошук оптимальних методів контролю роботи

системи з урахуванням усіх можливих критеріїв. Наша задача - дати приклад рішення вибору запиту для обробки на сервері при альтернативних ситуаціях вибору.

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

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

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

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

При наданні інформації “прибор вільний” може з’явитися ситуація, коли у черзі знаходяться заяви більше одного типу. Для вирішення таких конфліктних ситуацій використовується пріоритетний параметр, який визначає можливість вибору заяви s-

го типу для обслуговування на приборі. Звичайно, що якась заява обов'язково буде вибрана.

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

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

Для вирішення цієї проблеми використовується стандартний прийом заміни існуючих нелінійних складові, що дозволить у подальшому використати методи лінійного програмування.

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

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

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

КОМП'ЮТЕРНА ОБРОБКА ДАНИХ В МЕРЕЖЕВІЙ БАГАТОПОЗИЦІЙНІЙ СИСТЕМІ СПОСТЕРЕЖЕННЯ

Для усунення недоліків радіолокаційних систем спостереження останнім часом застосовуються багатопозиційні системи спостереження, які використовують метод мультилатерації.

Мультилатерація (MLAT) – знаходження місця розташування об'єкта, засноване на вимірах різниць часу приходу сигналу (TDOA - Time Difference of Arrival) від об'єкта (транспондера) до трьох або більше наземних станцій, координати розташування яких відомі.

Значення різниці часу фіксації сигналу на двох станціях визначає геометричне місце точок, де може знаходитися об'єкт – це гіперболоїд, у фокусах якого знаходяться станції. При перетинанні відповідного числа гіперболоїдів можна точно визначити місцеположення джерела сигналу. При розв'язанні завдання на площині знаходиться точка перетину гіпербол.

Мережева організація багатопозиційної системи спостереження MLAT забезпечує синхронізацію за часом, цифрову обробку сигналів, передачу даних в стандартному протоколі. Координати місцеположення літака обчислюється у центральному процесорі MLAT за різницею часу прибуття сигналу до встановлених наземних станцій в результаті розв'язання системи нелінійних рівнянь, які встановлюють зв'язок невідомих координат x, y, z положення об'єкта, відомих координат x_j, y_j, z_j наземних станцій ($j=1, \dots, n$) і різниць часу приходу τ_{jo} сигналу транспондера на j -у станцію і базову станцію с координатами x_o, y_o, z_o .

Мультилатерація забезпечує більш високу точність в порівнянні з радіолокаційними системами, які використовуються для керування повітряним рухом.

Для системи керування повітряним рухом використання даних системи багатопозиційного спостереження слід розглядати не тільки для більш точного визначення місцезнаходження літака, але і для його автоматичного супроводження.

Метою даної роботи є синтез алгоритму траєкторної оцінки для автосупроводження літаків за даними багатопозиційної системи спостереження MLAT в автоматизованій системі керування

повітряним рухом. Синтез проводиться на базі лінійного оптимального фільтра Калмана з попередньою оцінкою координат положення об'єкта x_m, y_m, z_m за методом найменших квадратів. Застосування фільтра Калмана дозволяє не тільки підвищити точність оцінки координат об'єкту, але і відновити значення складових швидкості його руху V_x, V_y, V_z , що необхідно для реалізації функції автосупроводження.

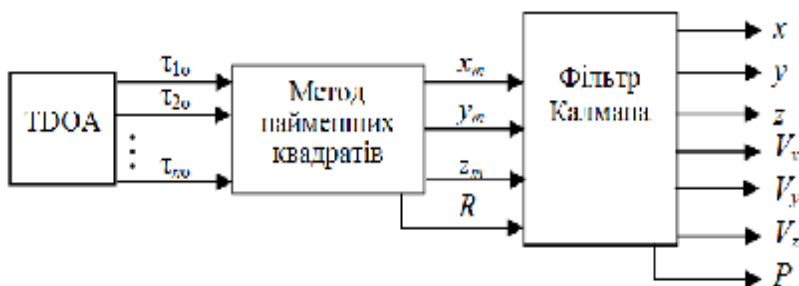
Для синтезу алгоритму траєкторної оцінки і траєкторного супроводу літаків визначається нелінійний функціональний зв'язок між оцінюваними траєкторними параметрами і різницями часу, що фіксуються системою MLAT, з урахуванням випадкових похибок у фіксації часу приходу сигналу.

Використовуючи метод статистичної лінеаризації виводиться математична модель вимірювань, що задовольняє умовам використання фільтра Калмана. При цьому визначаються всі необхідні статистичні характеристики для складових елементів фільтра у вигляді матриці коваріацій похибок вимірів R лінеаризованого фільтра.

Математична модель, що описує рух літака, визначається також у формі, що задовольняє постановці фільтра Калмана.

Виводяться вирази для розрахунку апіорних статистичних характеристик похибок оцінок траєкторних параметрів у вигляді матриці коваріацій похибок оцінок P в рівняннях фільтра Калмана.

Результати проведеного комп'ютерного моделювання показують можливість істотно підвищити точність визначення місцеположення літака при застосуванні синтезованого алгоритму оцінки і супроводження у порівнянні з визначенням положення різницево-далекомірним методом без використання оптимальної фільтрації.



МЕТОД МНОЖИНОГО КВАДРАТИЧНОГО k-РЕШЕТА З ВИКОРИСТАННЯМ СИГНАЛЬНИХ ОСТАЧ ПРИ ПРОСІЮВАННІ ПРОБНИХ ЗНАЧЕНЬ

На сьогоднішній день криптоалгоритм RSA використовується у web серверах, браузерів, електронній пошті та є ключовою технологією у системах електронних платежів. Найбільш поширена атака на цей криптоалгоритм заснована на факторизації ключа N , що є добутком двох простих чисел. Серед методів факторизації метод квадратичного решета (QS) займає друге місце у списку найшвидших алгоритмів, поступаючись тільки методу решета числового поля. Відносна простота алгоритму сприяла виникненню багатьох його модифікацій, серед яких методи множинного квадратичного решета (MPQS) та метод квадратичного k -решета (MQkS) [1].

В методі QS найбільш затратною за часом є процедура пошуку В-гладких чисел, в ході якої шукають ті з пробних X , що для остач $y(X)$ достатньо близькими будуть значення $\log(y(X))$ та $\sum_{j=1}^{pfa} s_j \log p_j$, де p_j – прості числа (елементи факторної бази). Оскільки при цьому можливі значення $s_j > 1$, то необхідно визначати значення X , при яких $y(X) \bmod(p^{s_j}) = 0$, що у випадку частоті зміни поліномів $y_{a,b}(X) = (aX + b)^2 - N = a^2X^2 + 2abX + b^2 - N$, чи $y_k(X) = X^2 - kN$ призводить до відчутного зростання обчислювальних затрат.

Для просіювання пробних значень X пропонується скористатися їх відсіюванням на основі порівняння сигнальних остач $y^*(X)$ з остачами $y_k(X) = X^2 - kN$ ($k \geq 1$), де сигнальні остачі – це добуток перших степенів елементів ФБ, що є множниками $y_k(X)$.

Серед пробних значень відсіюють ті, для яких $\log(y_k(X)) < h \cdot \log(y^*(X))$, де дійсне число $h \in [0, 1]$ – це параметр, який можна вибрати.

За рахунок його вибору можна скоротити час розрахунку майже вдвічі. Необхідно відмітити, що при використанні розміру ФБ, рівного L^a , та радіусу просіювання, рівного L^b , які визначені згідно [2], для чисел N порядку 2^{1024} число елементів матриці перевищить $9 * 10^{20}$, а кількість пробних X може перевищити $27 * 10^{30}$. На даний час такий обсяг пам'яті недоступний для сучасних обчислювальних систем. В найближчому майбутньому проблематичним також є виконання за прийнятний час числа операцій, що перевищує $27 * 10^{30}$. Тому є потреба в зниженні як кількості елементів ФБ (для методу MQkS ЗФБ), так і інтервалу просіювання. В методі MQkS число елементів ЗФБ визначається на основі вибору параметру pla , а розмір інтервалу просіювання – параметра plb . Проте зменшення розміру ФБ призводить до збільшення часу пошуку В-гладких. Тому одночасне зменшення fa та fb практично неможливе.

Для методу QS та його модифікацій обчислювальна складність оцінюється величиною $O(\exp(C\sqrt{\ln N \ln \ln N}))$, де $C \geq 1$. На основі проведених чисельних експериментів встановлено, що при $pla \leq 0.94$ та $pla > 0.9$ для аналізованої множини чисел, коефіцієнт C в формулі оцінки обчислювальної складності методу MQkS виявлявся меншим за одиницю. Проте не можна стверджувати, що такий факт матиме місце для довільних N . В той же час мона стверджувати що за рахунок використання ідеї діагоналізації матриці «на ходу», що пропонується в роботі [3] принципово можливе розкладання чисел N порядку 2^{1024} .

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Винничук С.Д., Місько В.М. Метод множинного k-решета цілочисельної факторизації // Електронне моделювання. 2018, Т.40, № 5. с. 3-26. <https://doi.org/10.15407/emodel.40.05.003>
2. Eric Landquist The Quadratic Sieve Factoring Algorithm // MATH 488: Cryptographic Algorithms December 14, 2001 p. 1—11.
3. Vynnychuck S., Misko V. Acceleration analysis of the quadratic sieve method based on the online matrix solving. // Mathematics and cybernetics – applied aspects., 2018. DOI: 10.15587/1729-4061.2018.133603

**С. В. Водоп'янов,
К. С. Ушаков,
О. А. Пастухов**

Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ПОБУДОВИ СУЧАСНОЇ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ АЕРОВУЗЛА

Рішення проблеми удосконалення авіаційної комунікаційної інфраструктури є найважливішою задачею. Шляхом цього рішення є інтеграція існуючих, а особливо майбутніх засобів організації повітряного руху (ОрПР) у так звану "систему систем", яка базується на безшовній організації авіаційних мереж та стиковці мережних сегментів. Система систем авіаційної комунікаційної інфраструктури базується на безшовному об'єднанні сегментів не тільки наземного та бортового розташування, але й супутникових сегментів, зокрема, так званих персональних супутникових сервісів.

Основним автономним елементом авіатранспортної інфраструктури є аеровузол – близько розташовані аеродроми, організація і виконання польотів з яких вимагають спеціального узгодження і координування. Для реалізації безшовної технології при побудові інтегрованої мережі аеровузла, перш за все, необхідно визначитися з комутаційними пристроями – їх принципами побудови, мережними протоколами та специфікою обробки даних. Наприклад, при застосуванні супутникових сегментів у складі інформаційно-обчислювальної мережі необхідно враховувати затримки доставки даних. Для супутників, що знаходяться на високих геостаціонарних орбітах, тільки затримки на розповсюдження сигналу від користувача до супутника й назад складають близько 250 мілісекунд. Тому, в інтегрованих комутаційних вузлах, побудованих на базі маршрутизаторів, комутаторів звичайних (*Switch*) і програмних (*Softswitch*), систем передавання даних через *IP*-мережі (*IP Multimedia Subsystem – IMS*) набори протоколів доставки даних мають бути доповнені протоколами тривалого зберігання та гарантованої доставки даних (по типу протоколів мереж з толерантністю до затримок – *Delay-Tolerant Networks – DTN*). Крім того, необхідно забезпечувати взаємодію між успадкованими мережами *ATN* на основі еталонної

моделі *OSI* та майбутніми мережами *ATN/IPS* на основі стандарту *IPv6*.

Пропонована модель архітектури інтегрованої мережі аеровузла, яка надана на рис. 1.

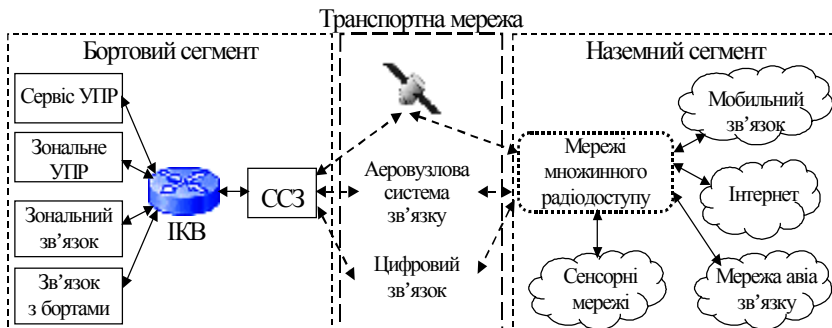


Рис. 1. Мережна архітектура інтегрованої мережі аеровузла.
 CC3 – складена система зв'язку; ІКВ – інтегрований комутаційний вузол

Окрім складених комунікаційних мереж, які об'єднують різні сегменти, до складу інтегрованої мережі аеровузла входить безліч сервісних мереж, які використовуються для забезпечення обміну інформацією, безпосередньо не пов'язаною з організацією повітряного руху. Це мережі авіакомпаній, аеропортів, що входять до складу аеровузла, спеціалізовані мережі для контролю стану аеродрому – льотного поля, службових приміщень, ангарів, диспетчерських веж тощо. Прикладами таких мереж служать мережі транкінгового та мобільного зв'язку, сенсорні мережі для збору інформації про температуру та вологість злітно-посадочних смуг, рульових доріжок та ін.

На основі використання сучасних технічних засобів реалізується концепція гнучкої організаційної структури повітряного простору, що дозволяє оперативно змінювати межі секторів УПР залежно від повітряної обстановки, що складається. Здійснюється оптимізація повітряного простору, завдяки чому забезпечується заданий рівень безпеки повітряного руху, метод обслуговування повітряного руху "від перону до перону" і використання технології зональної навігації.

ТЕХНОЛОГИЯ ОБРАБОТКИ ПСЕВДОУПОРЯДОЧЕННЫХ МАССИВОВ

Для каждой системы счисления, применяемой в компьютерной среде определена технология обработки данных, соответствующая арифметико-логическому базису [1]. Реализация арифметико – поисковых (АП) операций включает обработку–сортировку массивов разрядно-логарифмических (RL) кодов. Априорное ранжирование при формировании таких массивов является дополнительным резервом сокращения временных затрат из-за позиционно-непозиционных свойств RL кодов [1].

Предложена технология обработки RL кодов в базовых операциях умножения, сложения-вычитания. Массив частичных произведений, массивы слагаемых формируются с учетом априорной сортировки операндов.

При умножении рабочий массив (массив частичных произведений) разделяется на 4 составляющие части. Если каждый сомножитель A и B разделяется по правилу

$$A = \max RLA \div 1/2QRLA \text{ и } (1/2 Q+1)RLA \div \min RLA \leftrightarrow \{1\}\{2\},$$

$$B = \max RLB \div 1/2QRLB \text{ и } (1/2 Q+1)RLB \div \min RLB \leftrightarrow \{3\}\{4\},$$

то при умножении $A*B$ получаются следующие массивы:

$$M\{1-3\} = (\max RLA \div 1/2QRLA) * (\max RLB \div 1/2QRLB)$$

$$M\{1-4\} = (\max RLA \div 1/2QRLA) * ((1/2 Q+1)RLB \div \min RLB)$$

$$M\{2-3\} = ((1/2 Q+1)RLA \div \min RLA) * (\max RLB \div 1/2QRLB)$$

$$M\{2-4\} = ((1/2 Q+1)RLA \div \min RLA) * ((1/2 Q+1)RLB \div \min RLB).$$

Располагая в памяти массивы $M\{1-3\}$, $M\{1-4\}$, $M\{2-3\}$, $M\{2-4\}$ по величине входящих в них кодов, определим общую структуру $M\{1-3\}$ $M\{1-4,2-3\}$ $M\{2-4\}$ рабочих массивов, где $M\{1-4,2-3\}$ объединённый массив, так как $M\{1-4\}$ и $M\{2-3\}$ состоят из близких по величине кодов.

Параллельную сортировку выполняют в каждом массиве, затем в объединённом массиве реализуется общая сортировка, формирующая конечный результат. Моделирование показывает, что общее время сортировки около $1.5 N$, где N – общее

количество элементов в рабочих регистрах (для умножения $N=QA*QB$) .Предложен метод взаимокорреляции рабочих массивов, который состоит из перестановки некоторого количества максимальных и минимальных кодов в этих (рабочих) массивах. В рассматриваемом умножении из массива $M\{1-3\}$ два минимальных значения RL кодов включаются в массив $M\{1-4, 2-3\}$, два RL кода из массива $M\{2-4\}$ в массив $M\{1-4, 2-3\}$. В массив $M\{2-4\}$ включаются два минимальных кода $M\{1-4, 2-3\}$. Далее в $M\{1-3\}$ включаются 2 максимальных RL кода $M\{1-4, 2-3\}$. Общая схема обмена следующая

$$M\{1-3\} \leftrightarrow M\{1-4,2-3\} \leftrightarrow M\{2-4\}.$$

Далее выполняется отдельно сортировка (параллельно) в каждом рабочем массиве. Полученные результаты объединяются в один массив и после общей сортировки формируется окончательный результата. Применение такой технологии сокращает время сортировки до N тактов, что уменьшает общее время умножения разрядно-логарифмических кодов на 1-2 порядка. Такой результат является внедрением свойств разрядно-логарифмических кодов и базовой позиционной двоичной системы: $N=\log_2 p^1$ определяет и вес и позицию ненулевого разряда одновременно [1].

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Гамаюн В.П. Разрядно-логарифмическая арифметика. Методы и алгоритмы. – К.: Книжное из-во НАУ, 2007. - 272 с.

АДАПТИРОВАННЫЕ СТРУКТУРЫ ДАННЫХ ДЛЯ ВЫСОКОРОИЗВОДИТЕЛЬНОЙ ОБРАБОТКИ

Разработки теории, методов, способов адаптированных структур данных является одним из исчисления в остаточных классах, системы счисления с недвоичным основанием – неполный перечень реализованных проектов. Каждое исследование выполняется с конкретной целью, чаще всего адаптированные структуры исследуются для решения проблемы повышения производительности. Предлагаются результаты ненулевых разрядов счисления в технологиях компьютерной обработки [1].

Главной особенностью разрядно-логарифмической (РЛ) системы счисления является тот факт, что основной код ненулевого разряда $N = \log_2 p^i$ определяет и вес и позицию ненулевого разряда одновременно и составляет новое решение в направлении перспективных технологий и организации вычислительного процесса - обработке больших разрядных полей «малыми» операционными средствами [1].

Операция сдвига в РЛ системе реализуется способом сложения каждого кода операнда на константу сдвига (при сдвиге влево) и вычитания из каждого кода константы сдвига (при сдвиге вправо). Структурная реализации сдвига не применяется и, соответственно, уменьшаются аппаратные затраты.

Решается проблема представления нуля – как нулевого значения показателя значащих единиц в формате структуры операнда. При этом интерпретация нуля на всех компьютерных средствах одинакова.

Реализуются новые способы анализа данных при выполнении всех базовых операций:

- выравнивание мантисс путем сравнения минимальных и максимальных кодов;
- автоматизированный подбор пробных цифр при делении, что отличается от всех алгоритмов двоичного деления;
- уникальный алгоритм извлечения корня любой степени;
- сокращение структуры операционных автоматов-вследствие небольшой размерности кодов значащих разрядов.

Несмотря на отличие интерпретации двоичного разряда и кода значащего разряда РЛ системы соблюдаются правила и положения ассоциативной, ассоциативной ортогональной обработки.

Эффективным является аппарат пороговой обработки: любой код доступен для преобразования и анализа средствами работы с РЛ массивами.

При разрядно-логарифмическом представлении упорядоченность (ранжирование) набора кодов может быть нарушена без потери количественной меры числовой характеристики [1]. Если двоичное число A может быть представлено упорядоченным набором

$$A \leftarrow A^{PL} = \{ N_1 N_2 N_3 N_4 \dots N_i \dots N_Q \} ,$$

где N_i – код ненулевого разряда и $N_i > N_{i+1}$, то без потери количественной меры числа A возможно такое число представить неупорядоченным набором $\therefore A \leftarrow A^{PL} =$

$= \{ N_9 N_{21} N_1 N_2 N_{12} N_3 N_4 \dots N_i \dots N_Q N_{17} \}$ и, следовательно, такая система счисления имеет свойства как позиционных так и непозиционных систем счисления.

Такой результат является внедрением свойств разрядно-логарифмических кодов и базовой позиционной двоичной системы.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Гамаюн В.П. Разрядно-логарифмическая арифметика. Методы и алгоритмы.- К.: Книжное из-во НАУ, 2007. - 272 с.

ПІДХІД ДО АНАЛІЗУ РИЗИКУ НА ОСНОВІ ТЕОРІЇ КОМПЛЕКСНИХ ЧИСЕЛ

Проблема оцінки ризику тісно пов'язана з чіткістю формулювання поняття ризику, розумінням та інтерпретації його складових, а у випадку множини ризиків – здійсненням над ними операцій [1].

Цілком природно використовувати гроші як універсальної характеристики можливих результатів будь-яких втрат. Але у своїй теорії про вимірювання ризику Д. Бернуллі зазначає, що підхід, при якому «ціна ризику» обчислюється в грошах, далеко не досконалий. Ризик, сприймається кожним по-своєму, і оцінюватися однаково не може. Оцінка корисності благ залежить від людини, що знаходиться в ризикованій ситуації. Таким чином, знання збитків і ймовірності не завжди достатньо для визначення цінності результату, оскільки корисність в кожному окремому випадку може залежати від суб'єкта, що робить оцінку. Кожен суб'єкт має свою систему цінностей і реагує на ризик відповідно до цієї системи.

При побудові моделей раціонального вибору в умовах ризику намагаються зробити їх універсальними, не залежними від суб'єкта прийняття рішень – об'єктивними. Відсутність суб'єкта в моделях прийняття рішень призводить до суперечностей, що найбільш яскраво демонструє теорія Бернуллі. Кожен суб'єкт має свою систему цілей, цінностей і оцінок, і його поведінка в умовах ризику визначається саме цією системою, а не однаковими для всіх логіко-методологічними стандартами. В результаті суб'єкт вибирає ту альтернативу, яка найповніше відповідає його цілям, оцінкам і системі цінностей. Тут можна казати про суб'єктивний ризик.

Таким чином, прийняття рішень у сфері управління ризиками в значній мірі залежить від сприйняття ризику, його усвідомлення.

Тому, коректна кількісна оцінка повного ризику повинна поєднувати в собі не тільки складову об'єктивного ризику, а й складову суб'єктивного ризику.

В залежності від можливого результату ризику поділяють на додатні та від'ємні. Додатний ризик означає можливість отримання

збитку, тобто це ризик, що може призвести до погіршення ситуації. Від'ємний ризик – це ризик, що відображає ймовірність отримання прибутку. Таким чином, ризики характеризуються конкретним значенням, і можуть набувати як додатних так і від'ємних значень.

У той же час, ризик може зменшуватися або збільшуватися, змінюючи напрям, зберігаючи при цьому знак. Тому, ризики, як об'єктивні, так і суб'єктивні, характеризуються напрямком та значенням і їх можна подати у вигляді векторів.

Для визначення результуючого повного ризику необхідно додати об'єктивний і суб'єктивний ризики. Але алгебраїчно додавати ці два ризики неможна через їх відмінність по своєму характеру. У цьому випадку, результуючий повний ризик можна знаходити шляхом векторного додавання об'єктивного і суб'єктивного векторів з отриманням вектору повного ризику. Оскільки вектор являється представленням комплексного числа на декартовій площині, то результуючий повний ризик можливо представити у вигляді комплексного числа, рис.1. Об'єктивний і суб'єктивний ризики будуть являти собою дійсну і уявну частини результуючого повного ризику:

$$R = r + im,$$

де r - об'єктивний ризик, m - суб'єктивний ризик, $i = \sqrt{-1}$.

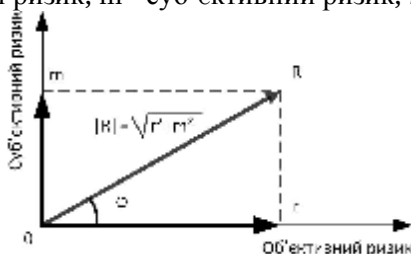


Рис. 1. Графічне представлення комплексного ризику.

Запропонований підхід до аналізу ризиків дозволить враховувати суб'єктивну складову ризику, а також відкрити можливість здійснення операцій над ризиками.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Мохор В.В. Идея построения алгебры рисков на основе теории комплексных чисел / Мохор В.В., Гончар С.Ф. // Електронне моделювання. – 2018. – Т.40. – №4. – С. 107-111.

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ВІДДАЛЕНОГО ДОСТУПУ

Віддалений доступ - це комплекс апаратно-програмних засобів, що забезпечують дистанційне використання ресурсів окремого комп'ютера або цілої обчислювальної мережі. Віддалений доступ дуже широке поняття, яке включає різні типи і варіанти взаємодії комп'ютерів, мереж і додатків. Почати сеанс віддаленого доступу можна, подавши відповідну команду і вказавши ім'я машини, з якою хочуть працювати. Сеанс забезпечується спільною роботою програмного забезпечення віддаленого комп'ютера і комп'ютера користувача. Вони встановлюють TCP-зв'язок і спілкуються через TCP- і UDP-пакети. Для користування службою telnet необхідно мати доступ в Інтернет класу не нижче dial-up.

Існує безліч реалізацій програм віддаленого адміністрування. Всі реалізації відрізняються інтерфейсами і використовуваними протоколами. Інтерфейс може бути візуальний або консольний. Одними з найбільш популярних і поширених програм є, наприклад, компонент Windows Remote Desktop Services з клієнтом Remote Desktop Connection, Radmin, DameWare, PuTTY, VNC, UltraVNC, TightVNC, Apple Remote Desktop, Hamachi, TeamViewer, Remote Office Manager, Ammyy Admin та ін.[1].

Також останнім часом стали дуже популярні віртуальні приватні мережі (VPN). Переваги технології VPN в тому, що організація віддаленого доступу створюється на базі загальнодоступної мережі Інтернет, що набагато дешевше і краще.

Недолік технології VPN в тому, що протокол безпеки складно налаштувати, і це може призвести до помилок в процесі установки, що спричинять проблеми з безпекою. Також якщо VPN-сервіс налаштований неправильно, може статися витік DNS і IP-адрес, якими можуть скористатися в злочинних цілях хакери. Проте, незважаючи на все це технологія VPN має перспективи на подальший розвиток.

Зокрема в перспективі вирішення наступних проблем:

1. Вироблення і затвердження єдиного стандарту побудови подібних мереж. Швидше за все, основою цього стандарту буде,

вже зарекомендований протокол IPSec. Цілком можливо, що буде використовуватися протокол IPv6, роботи над яким активно тривають. Даний протокол має всі можливості взаємодії з VPN, які тільки можуть побажати мережеві розробники, зокрема, управління смугою пропускання, визначення приналежності IPv6-пакетів до конкретного потоку (наприклад, вищий пріоритет будуть отримувати пакети мультимедійних даних для передачі в реальному часі).

2. Підвищення продуктивності VPN-продуктів і створення зручних засобів управління VPN. Розвиток засобів побудови VPN буде йти в напрямку VPN на базі маршрутизаторів, так як дане рішення поєднує в собі досить високу продуктивність, інтеграцію VPN і маршрутизації в одному пристрої. Однак будуть розвиватися і недорогі рішення для невеликих організацій.

3. Покращення захисту інформації. VPN включає в себе шифрування підтвердження справжності та контроль доступу. Читати всі отримані дані може лише власник ключа до шифру. Найбільш часто використовуваними в VPN-рішеннях алгоритмами кодування в наш час є DES, Triple DES і різні реалізації AES. Підтвердження справжності включає в себе перевірку цілісності даних та ідентифікацію осіб та об'єктів, задіяних у VPN. Перша гарантує, що дані дійшли до адресата саме в тому вигляді, в якому були послані. Найпопулярніші алгоритми перевірки цілісності даних на сьогодні MD5 і SHA1 [2].

У міру свого розвитку VPN перетворюються в системи взаємопов'язаних мереж, які будуть з'єднувати мобільних користувачів, торгових партнерів та постачальників з критично важливими корпоративними додатками, що працюють в протоколі IP. VPN стануть фундаментом для нових комерційних операцій і послуг, які будуть стимулювати ринок і допомагати модернізувати виробництво.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Петренко З. Захищена віртуальна приватна мережу: сучасний погляд право на захист конфіденційних даних / Світ Internet. – М.: №2, 2001.

2. Салливан До. Прогрес технології VPN.PCWEEK/RE. – М.: №2, 1999.

ANALYSIS OF SOFTWARE ECOSYSTEMS USING PETRI NETS

The concept of "software ecosystem" is widely used by companies and researchers of the software. According to [1] researches of software ecosystems are represented by several definitions depends on their goal, aims, actors etc. That's why throughout this thesis we will consider a few definitions of software ecosystems. So, software ecosystem is a set of actors functioning as a unit and interacting with a shared market for software and services, together with the relationships among them. These relationships are frequently underpinned by a common technological platform or market and operate through the exchange of information, resources and artifacts. The transaction between two software vendors is centered around software components and software services. In this thesis a definition of software components is used: software component a bundle of software functions accessible through a single interface or carrying a single name which is or can be used as an element in other software packages but of which the core functionality is developed separate from these packages. A software service is a software component accessible via communications outside the users native environment. User can be both human and non-human. Native environment changes depending on the user. If the user is human, the native environment is most probably his or her own computer. If the user is a software package, the native environment consists of the compiled or interpreted code.

Corporation "Microsoft" defines software ecosystem as a set of interactions and mutual influences of organizations (public, educational and commercial) and individuals, which work with software.

Also some authors describe software ecosystems and the typical elements of ecosystems and their context, namely: software and its role in IT; users of software; software creating processes; management of the establishment and maintenance of software; supply and support of software; communication network of state agencies; software economy.

According to [2] we study the software ecosystems by creating their models. To describe software ecosystems can be used the following tools: i *, UML, Petri nets. Petri nets is the most common nowadays

formalism that describes the structure and interaction of parallel systems and processes [3].

According to [4] software ecosystems metrics can be the following:

- Productivity. This criterion shows the statistical analysis of nationwide product development and software services for a certain period.
- Diversity. This criterion shows the ranking of IT companies according to the following criteria: "software revenue", "income system integration" and "income from software services."
- Flexibility. This criteria determines which of the fastest growing sectors in IT market.
- Productivity. This criterion determines the impact of investments in the IT industry.
- Sustainability (Vitality). This criterion defines total income in all sectors of the IT market.
- Maturity. This criterion determines a qualitative characteristics of software ecosystems development.

According Petri nets theory these metrics can be analysed using the following structural properties of Petri nets:

- structural survivability
- controllability
- structural limitations
- conservatism and partial conservatism
- repeatability and partial repetition
- contradiction and partial contradiction.

REFERENCES

1. Грінєнко О.О. Екосистеми програмного забезпечення / О.О. Грінєнко // Вісник НТУ. – К.: НТУ – 2012. – Вип. 26. – С. 508 – 512.
2. Sidorov N.A., Grinenko O.O. Software Ecosystem Modeling / N.A. Sidorov, O.O. Grinenko // Інженерія програмного забезпечення. – 2013. – № 2. – С. 38 – 48.
3. Советов Б.Я., Яковлев С.А. Моделирование систем. – М.: Высшая школа, 2001. – 344 с.
4. Grinenko O.O. Metrics of software ecosystems. // Збірник тез «Інженерія програмного забезпечення – 2016». – Міжнародна науково-технічна конференція аспірантів і студентів «Інженерія програмного забезпечення – 2016». – 6-9 червня 2016. – С. 24.

ВИЗНАЧЕННЯ ФУНКЦІЇ МОНІТОРИНГУ СТАНУ САНКЦІОНОВАНИХ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ ЗА ДОПОМОГОЮ АНАЛІЗУ ЇХ КЛАВІАТУРНОГО ПОЧЕРКУ

Майже у всіх областях діяльності людини використовуються комп'ютерні системи, а більшість інформації, що обробляється, зберігається в базах даних. Тому досить важливим є коректність вводу цієї інформації. Це відноситься і до друкарки, яка набирає текст книги, і до оператора, який вводить будь-яку інформацію до бази даних. Коректність вводу інформації напряму залежить від уважності людини, яка цю інформацію вводить до комп'ютерної системи. В зв'язку з цим актуальною задачею сьогодення є розробка системи моніторингу роботи за комп'ютером відповідних співробітників.

В даній роботі, для створення системи аналізу динаміки роботи користувачів комп'ютерних систем за їх клавіатурним почерком [1], була розроблена наступна функція моніторингу R :

$$R = \begin{cases} 1, \text{ якщо } (Usx \in Usl) \wedge (Usx = Usl_d) \wedge (Och \leq p * Och_{sr_t}); \\ 0, \text{ якщо } (Usx \in Usb) \vee ((Usx \in Usl) \wedge ((Usx \neq Usl_d) \vee (Och \geq p * Och_{sr_t}))); \end{cases}$$

де $Usx \in Us$ – користувач комп'ютерної системи, який проходить процедуру моніторингу; $Us = \{Us_1, Us_2, \dots, Us_p, \dots, Us_m\}$; $p = \overline{1, m}$; Us – множина людей, котрі можуть спробувати отримати доступ до системи, яка захищається і відповідно проходити процедуру моніторингу; m – кількість членів множини Us ; $Usl = \{Usl_1, Usl_2, \dots, Usl_b, \dots, Usl_d, \dots, Usl_l\}$; $t = \overline{1, l}$; Usl – множина легальних користувачів даної системи ($Usl \subset Us$); l – кількість легальних користувачів даної системи; Usl_d – легальний користувач, за котрого видає себе людина, моніторинг дій якої виконується ($(Usl_d \in Us) \wedge (Usl_d \in Usl)$); Usb – порушник, тобто людина, яка не зареєстрована в даній системі, але отримала до неї

доступ $((Usb \in Us) \wedge (Usb \notin UsI))$. Зразок клавіатурного почерку користувача має вигляд: $O = \{v_1, v_2, v_i, \dots, v_s, Och\}$; $i = \overline{1, s}$; де s – кількість символів у слові, динаміка вводу яких аналізується; v_i – часовий інтервал між натисканням i -1-го та i -го символів слова; Och – кількість помилок, тобто кількість неправильно введених символів, під час вводу слова; Och_{sr_t} – середнє арифметичне значення кількості помилок t -го користувача; p – коефіцієнт припустимого відхилення значення кількості помилок.

Робота розробленої системи моніторингу, як і будь-якої біометричної системи розпізнавання, складається з двох етапів: накопичення бази даних навчальних зразків клавіатурного почерку всіх користувачів системи; розпізнавання образів, на основі накопичених раніше зразків. Накопичення зразків почерку є сенс продовжувати і під час етапу розпізнавання. Для розпізнавання в базі даних необхідна наявність хоча б декількох сотень навчальних зразків почерку для кожного співробітника. Для реалізації даного методу розпізнавання образів був обраний один з найбільш ефективних механізмів вирішення даної задачі – нейронні мережі.

На основі результатів проведених експериментів, можна зробити висновки, що імовірність правильної роботи даної системи моніторингу залежить від наступних параметрів [1]: кількість параметрів, що аналізуються; якість обраних для аналізу параметрів; кількість накопичених зразків почерку для кожного користувача; амплітуда відсотка помилок у користувачів; наявність в системі функції видалення з бази даних, навчальних зразків з грубими помилками, використовуючи для цього ефективний алгоритм [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Висоцька О.О. Моніторинг роботи користувачів комп'ютерних систем за допомогою технологій розпізнавання за клавіатурним почерком // Моделювання та інформаційні технології. Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. – 2018. – Вип. 84. – С. 119-125.

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Віртуальні приватні мережі (VPN) являють собою технологію, що дозволяє забезпечувати захист передачі інформації за допомогою її криптографічного перетворення.

Засоби організації віртуальних приватних мереж – це програмні рішення або програмно-апаратні пристрої, які дають можливість організовувати єдиний захищений інформаційний простір, що використовує, зокрема, незахищені канали зв'язку (наприклад, Інтернет).

Основні функції засобів організації віртуальних приватних мереж:

- організація криптографічного захисту інформаційної взаємодії між підрозділами інформаційної системи підприємства;
- забезпечення криптографічного захисту інформаційної взаємодії вилучених користувачів з інформаційною системою підприємства;
- ідентифікація й аутентифікація користувачів при доступі до ресурсів інформаційної системи підприємства.

Всі продукти для створення VPN можна умовно розділити на дві категорії – програмні й апаратні. Програмне рішення для VPN, як правило, готовий додаток, що встановлюється на підключеному до мережі комп'ютері зі стандартною операційною системою. З міркувань захисту й продуктивності для установки VPN-додатків найкраще виділяти окремі машини, які повинні встановлюватися на всіх кінцях з'єднань.

Для розгортання програмні рішення звичайно складніше, ніж апаратні. Створення подібної системи передбачає конфігурування сервера для розпізнавання даного комп'ютера і його операційної системи, VPN-пакета, мережних плат для кожного з'єднання й спеціальних плат для прискорення операцій шифрування. Така робота складна навіть для досвідчених фахівців. З іншого боку, вартість програмних рішень відносно нижче(залежно від розміру мережі можна придбати VPN-пакет).

Апаратні VPN-рішення містять у собі все, що необхідно для з'єднання – комп'ютер, приватну (як правило) операційну систему й спеціальне програмне забезпечення. Ряд компаній пропонують цілий спектр рішень, які можуть масштабуватися залежно від кількості одночасних VPN-з'єднань, з якими планується працювати, і очікуваного обсягу трафіка. Розгортати апаратні рішення значно простіше, і на їхній запуск потрібно всього кілька годин. Ще однією серйозною перевагою апаратних VPN-рішень є більше висока продуктивність. У них використовуються спеціальні друковані плати й операційні системи, оптимізовані під дане завдання й звільнені від необхідності підтримувати інші функції. До мінусів апаратних рішень ставиться їхня висока вартість.

Вибір рішення залежить від розміру мережі й обсягу трафіка. Необхідно пам'ятати, що шифрування вимагає істотних обчислювальних ресурсів і може перевантажувати комп'ютер, коли кілька VPN-з'єднань одночасно беруть участь у передачі даних.

Переваги технології VPN настільки переконливі, що багато компаній починають будувати свою стратегію з урахуванням використання Інтернету як головний засіб передачі інформації, навіть уразливої.

При правильному виборі VPN:

- підприємство одержує захищені канали зв'язку за ціною доступу в Інтернет, що в кілька разів дешевше виділених ліній;
- при установці VPN не потрібно змінювати топологію мереж, переписувати додатки, навчати користувачів – все це забезпечує значну економію;
- забезпечується масштабування, оскільки VPN не створює проблем росту й зберігає зроблені інвестиції;
- незалежність від криптографії й можливість використовувати модулі криптографії будь-яких виробників відповідно до національних стандартів тієї або іншої країни;
- відкриті інтерфейси дозволяють інтегрувати вашу мережу з іншими програмними продуктами й бізнес-додатками.

Подальший розвиток мережі Інтернет буде супроводжуватися збільшенням числа користувачів і перенесенням туди все більшої кількості послуг для них. Виходячи з цього, ринок VPN збереже тенденцію зростання в найближчій перспективі, поки йому на зміну не прийде нова технологія організації безпечних з'єднань.

**В. В. Демчик,
О. В. Корочкін, к.т.н.,
О. В. Русанова, к.т.н.,
В. Ю. Тизунь,**

*Національний технічний університет України
“КПІ ім. І. Сікорського”, Київ*

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБЧИСЛЕНЬ В ГЕТЕРОГЕННИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

В даній роботі досліджуються питання підвищення ефективності високонавантажених обчислень в неоднорідних комп'ютерних системах за рахунок застосування в них концепції комбінованого паралелізму [1].

Використання графічних процесорів (GPU) дозволяє розвантажити центральні процесори в системах за рахунок зняття з останніх ролі управління графічним інтерфейсом користувача. Графічний процесор являє собою набір великої кількості малих, простих та порівняно дешевих процесорних елементів, що власне кажучи являє собою окрему паралельну комп'ютерну систему зі спільною пам'яттю [2]. З часом розвиток цього типу процесорів призвів до надлишкових потужностей в них. GPU були активні лише в моменти значних оброблень графічних операцій, а решту часу простоювали. Це призвело до винайдення шейдерних блоків, доступних для програмування, та, відповідно, техніки використання графічних процесорів для обчислень загального призначення (GPGPU - *англ. General-purpose computing on graphics processing units*, неспеціалізовані обчислення на графічних процесорах) [2].

Інтерес як наукового світу, так і бізнесу до даної технології виражається в збільшенні кількості наукових праць що стосуються даної теми та появою цілого ряду програмних реалізацій GPGPU. Спершу вони були націлені лише на невеликий ряд найновіших GPU компанії Nvidia, проте з появою мови програмування OpenCL (*англ. Open Computing Language*, відкрита мова обчислень) з'явилася можливість програмувати загальні обчислення і для більшості звичайних GPU.

Описані вище особливості GPU дозволяють досягти значного приросту швидкодії при виконанні великої кількості однакових

елементарних обчислень, тобто при реалізації обчислень в рамках дрібнозернистого паралелізму. З іншого боку, відповідно до таксономії Флінна GPU можна віднести до SIMD систем, і виходячи з чого можна зробити висновок що «вузьким місцем» гетерогенної системи яка містить і CPU і GPU є інтерфейс їх взаємодії, по якому центральних процесором відправляються чергові набори даних для обчислень на GPU та отримуються результати. З появою інтерфейсу PCI 2.1 з'явилася можливість одночасного обміну даними між CPU та GPU з декількох потоків CPU. А отже, стає можливою реалізація обчислень в рамках комбінованого паралелізму, який в попередніх дослідженнях продемонстрував свою ефективність [1].

В ході роботи було розроблено нейронну мережу для розпізнавання великих об'ємів тексту (оскільки даний тип програм потребує значної кількості складних обчислень, які можна звести до великого набору елементарних обчислень), в якій закладено можливість регуляції відсотку обчислень, який припадає на GPU (від 100% - всі обчислення ведуться на GPU, а CPU відповідає лише за загальний менеджмент, до 0% - контрольний варіант, всі обчислення ведуться на CPU). Було проведено тестування на ряді реальних неоднорідних комп'ютерних систем з різноманітними комбінаціями CPU та GPU. Також було проведено тестування без застосування паралельної відправки даних на GPU.

Результати тестування показали можливість скорочення часу виконання паралельних програм в гетерогенних комп'ютерних системах за рахунок застосування комбінованого паралелізму.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Демчик В.В. Комбінований паралелізм як засіб підвищення ефективності паралельних обчислень / В.В.Демчик, О.В.Корочкін, О.В.Русанова. – Тези XI Міжнародної науково-технічної конференції "Комп'ютерні системи і мережні технології". – К.: НАУ, 2018. - С. 21-22.

2. Hyesoon Kim, Richard Vuduc, Sara Baghsorkhi. Performance Analysis and Tuning for General Purpose Graphics Processing Units (GPGPU). — Morgan & Claypool Publishers, 2012. — 96 p.

МОЖЛИВОСТІ НАДАВАНІ КВАНТОВИМИ ОБЧИСЛЕННЯМИ

Задача пошуку альтернативних варіантів обчислень, що можуть надати новий інструментарій для вирішення раніше не вирішуваних проблем, пов'язаних із фізичними обмеженнями, завжди була, є і буде актуальною.

Фундаментальна одиниця інформації у квантовому комп'ютері (квантовий біт або кубіт), не двійкова, а скоріше четверична за своєю природою. Ця властивість кубіта виникає як прямий наслідок його підпорядкованості законам квантової механіки, які радикально відрізняються від законів класичної фізики. Кубіт може існувати не тільки в стані, відповідному логічним 0 або 1, як класичний біт, але також у станах, відповідних суперпозиції цих класичних станів, тобто кубіт може існувати як нуль, як одиниця, і як 0 і 1 одночасно. При цьому можна вказати певний чисельний коефіцієнт, що представляє ймовірність опинитися в кожному стані.

У звичайному комп'ютері щоб отримати потрібний результат біти послідовно обробляються елементами що базуються на Булевій логіці. Аналогічно квантовий комп'ютер обробляє кубіти, виконуючи послідовність операцій квантовими логічними елементами, кожний з яких представляє собою унітарне перетворення, що діє на одиничний кубіт або пару кубітів. Послідовно виконуючи ці перетворення, квантовий комп'ютер може виконати складне унітарне перетворення над усім набором кубітів впорядкованих у певному початковому стані. Після цього можна зробити вимірювання над кубітами, яке і дасть кінцевий результат обчислень. Ця схожість обчислень між квантовим і класичним комп'ютером дозволяє вважати, що, принаймні, в теорії, класичний комп'ютер може в точності відтворювати роботу квантового комп'ютера. Симуляція квантового комп'ютера на класичному комп'ютері обчислювально складна проблема, тому що кореляції між квантовими бітами якісно відрізняється від

кореляцій між класичними бітами, як було вперше показано Джоном Беллом.

Квантові комп'ютери особливо добре імітують природу і її процеси.

Квантові обчислення також можуть революціонізувати матеріалознавство або передачу інформації. Завдяки заплутаності, кубіти, які фізично розділені на великі відстані, потенційно можуть створити канал для передачі інформації, який науково доведено більш безпечним, ніж наші поточні канали, що робить криптографічне застосування квантових комп'ютерів більш доцільним. Потужною можливістю криптографії на квантових комп'ютерах є створення та розподіл ключів – базису шифрування. Квантовий розподіл ключів (КРК) вирішує основну проблему симетричного шифрування – генерацію двох ідентичних реплік ключа для двох віддалених користувачів таким способом, що третя репліка ключа не може існувати в природі, оскільки це неможливо через закони квантової механіки. Для передачі секретного повідомлення на практиці завжди застосовується комбінація КРК, симетричного шифрування та інших примітивів класичної криптографії. Переваги КРК перед асиметричними технологіями розподілу ключів полягають в його безумовній захищеності, тобто за відсутності припущення про обчислювальні ресурси зломисника. Крім того, безпека асиметричного шифрування має серйозну загрозу з боку квантових комп'ютерів, які з використанням алгоритму Шора можуть зламати такий шифр.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Mavroeidis Vetal. The impact of quantum computing on present cryptography / Int. J. of Adv. Comp. Sci. and Appl. – Vol.9(3). – 2018.
2. Wang J., et al. Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units / Optics Express. – 2016. – Vol.24(8). – pp.8302-8309

МЕТОДИКА РОЗРОБКИ ВЕБ-ДОДАТКУ ДЛЯ RSS-АГРЕГАЦІЇ

Широке використання сайтів різного призначення у сучасному світі дає можливість доступу до необхідної інформації великої кількості користувачів, однак потрібно звернути увагу, що контент сайтів часто змінюється. Ручна перевірка кожного сайту щодо наявності нового контенту може бути дуже тривалою, втомливою та незручною. Використання RSS – Really Simple Syndication («Справді Просте Розповсюдження») – набагато кращий спосіб сповіщення про новий чи змінений контент. RSS – це формат даних, який дозволяє відобразити та розповсюдити інформацію у зручний та ефективний спосіб. RSS може забезпечити доступність інформації та фільтрування важливого матеріалу серед величезної кількості ресурсів наявних в Інтернеті.

Підхід до рішення проблеми. З точки зору підходу до реалізації RSS-агрегаторів зараз існують два типи. Перший тип представляє собою додатки, які інсталиються на персональний комп'ютер, смартфон чи планшет. Найбільш відомі приклади таких агрегаторів : NetNewsWire, Flipboard, Prismatic та Zite. Перевагою таких рішень є можливість перегляду збережених даних у разі відсутності доступу до мережі Інтернет. Недолік – неможливість доступу до даних з пристроїв, де не встановлено додаток. Інший тип – агрегатори, що представляють собою веб-додатки, доступні для використання з будь-якого браузеру з будь-якого пристрою. Найбільш відомі додатки : Google News, Drudge Report, City FALCON, Huffington Post, Fark, Zero Hedge, Newslookup, Newsvine та інші. Запропонований підхід базується на другому типі – RSS-агрегаторі, що базується на веб-додатках.

Розглянуто підхід до методики побудови веб-додатку для RSS-агрегації з використанням сучасних технологій для веб-розробки. Показано відмінності між традиційними та одно-сторінковими додатками, описано проблему збереження даних на стороні клієнта та вирішення цієї проблеми за рахунок використання

технології локального сховища, що пропонується стандартом HTML5.

З розвитком технологій в галузі веб-розробки стало можливим зберігати досить значні об'єми інформації локально на пристрої користувача. Мова розмітки HTML5 вводить новий програмний інтерфейс користувача – Local Storage, тобто локальне сховище, зі значно більшим об'ємом місця, доступного для збереження даних (мінімум 5 Мб), ніж при використанні куків (4Кб). Більшість сучасних RSS-агрегаторів, що працюють через браузер, представляють собою традиційні веб-додатки, на яких для перегляду інформації потрібно робити переходи на інші сторінки. У разі зникнення Інтернет-зв'язку подальше користування веб-сайтом неможливе. Рішенням такої проблеми є побудова додатку у вигляді SPA – single-pageapplication, тобто одно-сторінкового додатку. У такому додатку ніколи не відбувається переходу на інші сторінки, а завантаження нових даних відбувається за допомогою таких технологій, як AJAX або веб-сокети. Більше того, одно-сторінкові додатки можна відкривати з локальних файлів та користуватися без доступу до Інтернету.

Отже, одно-сторінковий додаток зменшує час пересилання даних, навантаження на сервер та дозволяє адекватно відреагувати на ситуацію зникнення Інтернет-зв'язку. Для побудови додатку доцільно використати набір програмного забезпечення MEAN, який орієнтований на розробку одно-сторінкових додатків та містить наступні компоненти: MongoDB в якості бази даних, Express.js в якості сервера, Angular.js у якості фреймворка для клієнтської частини, тобто інтерфейсу користувача, та Node.js – JavaScript платформа для серверної розробки. У таких додатках вкрай важливо використовувати описаний раніше програмний інтерфейс Local Storage, введений у HTML5.

RSS-агрегація зручний та потужний спосіб організації необхідних новин в одному місці. Для такої цілі як найкраще підходить одно-сторінковий веб-додаток, забезпечуючи надійний, зручний та швидкий доступ з браузера користувача. Для написання клієнтської та серверної частин запропоновано використовувати одну мову програмування – JavaScript та відповідно набір програмного забезпечення MEAN. Проблему збереження даних вирішує технологія Local Storage.

I. A. Zhukov, Dr Sc Eng,
I. M. Kravets, Ph D
National Aviation University, Kiev

SWISS KHIFE OF EMBEDDED SYSTEMS

Different micro-controllers normally have different developing tools. For instance Arduino rely on Arduino IDE. Few more advanced users set up different graphical interfaces like Eclipse for better project management. Sometimes it may be hard to keep up with different micro-controllers and tools.

The embedded hardware is almost always accessible via so-called developer boards. These consist of a micro-controller (MCU) with integrated or additional external memory on the board, input/output pins for the connection of sensors or actuators, and an interface for connection to and communication with the PC – usually USB. This supplies the board directly with power (5V via USB), and – depending on the board – reduces it to a lower voltage, e.g. 3.3V. The micro-controller can be addressed via a serial interface because of an interface chip, e.g. from FTDI or SiliconLabs.

Where are the major differences? On the one hand, the MCUs used can have a big impact. They range from 8-bit MCUs such as the Arduino Uno to 16-bit MCUs such as an MSP430 from Texas Instruments, to 32-bit MCUs such as the ARM Cortex M series. This is coupled with a clock frequency that can range from the single-digit MHz range up to several hundred MHz. An increase in speed and computing power of the MCU allows faster or more powerful applications (e.g. modern encryption), but also requires more power.

In order to be able to program for these MCUs or boards, firmware (i.e. software that is embedded in the chip) is required. At this point, there are basically a lot of choices for developers. While “small” MCUs are programmed in C or C++, additional script languages are available for the more powerful 32-bit variants, e.g. Embedded Lua or subsets of Python (MicroPython) and Javascript (Espruino).

After the choice of a board or a development framework has been made, the question arises as to how the whole thing is specifically programmed and equipped. Usually we need the following parts if we want to develop in C or C++:

- A crosscompiler capable of translating C/C++ code for the processor of the target hardware. In the open source area this is often the GCC, in a variant for the target. For example: arm-none-eabi-gcc for ARM Cortex processors/MCUs or xtensa-lx106-elf-gcc for the ESP series of Espressif.

- The compiler includes additional tools such as linkers, preprocessors, archivers and others that work together to create an executable binary for the target hardware.

- In most cases, a flashing tool is needed to get the firmware binary on the board – often via USB, in combination with a serial port, or via a programmer. Sometimes the USB interfaces of the boards allow us to access the board like a drive and copy the binary (or script for boards that support script languages) directly into a file system.

All these tools are easy to download and manually install. However, this means a lot of effort and is quite error-prone if, for example, versions of different tools do not work well together.

PlatformIO (<https://platformio.org>) takes a different approach. It is a cross-platform, multiple framework, professional tool for embedded systems engineers and for software developers who write applications for embedded products.

PlatformIO applies the latest scalable and flexible software technology to the embedded market – an area traditionally served by complex software tools that experienced hardware engineers have learned over time (often painfully so). Instead, with PlatformIO, users can be hobbyists or professionals. They can import the classic Arduino “Blink” sketch or develop a sophisticated low-level embedded C program for a commercial Internet of Things (IoT) product. Example code for any supported framework can be compiled and uploaded to a target platform in minutes.

If we remember our own C/C++ projects and the tedious work with makefiles, include and library paths, we can breathe a sigh of relief here. Thanks to SCons, source files are automatically found within our own project and linked to the sources of the embedded frameworks. PlatformIO also integrates library management so that external libraries (e.g. for certain sensors, displays or network protocols) can be easily found and installed.

¹ **I. A. Zhukov**, Dr Sc Eng,

¹ **N. K. Pechurin**, Dr Sc Eng,

² **L. P. Kondratova**, Ph D

¹National Aviation University, Kyiv, Ukraine,

²National Technical University of Ukraine “Igor Sikorsky Kiev Polytechnic Institute”, Kyiv, Ukraine

METHOD FOR THE AVIATION SECTOR OBJECTS SAFETY ENSURING RESOURCES DISTRIBUTION BASED ON THE MACROECONOMIC INDICATOR

Both the elements from D.I.Mendeleev’s table, connected in the molecules of fuel for an aircraft, or the conductors in an aircraft computer cheap (low level abstraction), and the interconnecting aviation industry-devices or the aviation transport- devices (high level abstraction) represents the aviation sector objects, which had to be safed because of fact, that it generates (potential) dangerous for the aviation sector as for the integer system. And every object must take its own part of safety ensuring resources. The value of resource, which according to optimal distribution program, had to be directed on certain object safety, is depended on power of dangerous from certain object; the parameter that may be chosen and allows us to estimate the share of total resources, is the information load coming from the final (terminal) subscribers (devices), which are dangerous information generators on the operated devices, and on those in the production process.

Estimating the total information capacity (performance) of software and hardware - primary sources, for the network, information is quite a difficult task: it reminded the authors of the difficulties of the early 70s - 80s of the twentieth century in evaluating a similar indicator for a computer network of computer centers of collective using, academic network, networks of the control by air traffic, which were designed under the supervision of academicians V.M. Glushkov, E.A. Yakubaytis. The primary information, directly from intelligent sensors, microprocessors, to computer networks and systems, in particular, to the air traffic control a system, that is the object of the attack and, accordingly, the subject of the protection.

The intensity of the information flow from the i -th thing depends on the degree of its orderliness. Assuming that the intensity of the

information flow from a thing of each type is known, and also making an assumption about the additive nature of the function: intensity of the total endangered primary information flow from each i -th thing flow intensity, we have the opportunity to go now to the problem of estimation (detection) of the distribution of the things flow intensities $X(t)$ - sources of the primary information for the protection. The classical approach to aviation safety is based on three subjects of vulnerability detection: air traffic control, aircraft, airport. The peculiarity of the approach professed in the report is that it takes into account the generation of “dangerous” information by devices (things) placed in the aircraft being operated and its infrastructure, as well as devices that are in production, in particular, by computer engineering devices, in the initial stages of production, and requiring adequate security.

To solve the above problem, it is proposed to use macroeconomic indicator *GDP*, more precisely - its sectoral components. This indicator shows the quantity of items that can potentially by intelligent sensors and actuators generate a traffic load on the system (including computer) of the safety in the aviation sector.

The method of estimating the primary information for the protection and subsequent calculation of distribution program is based on building a dynamic algebraic (one-product flow) model taking into account the interrelation of the parameters. As a base construction, it is proposed to use V.V.Leontyev’s model of the interbranch balance

$$(E - A(t)) \cdot X(t) - G(t) = 0,$$

where $A(t)$ is a technological matrix that exists at the moment t ; $G(t)$ represents *GDP*.

Proposed model takes into account the relationship between objects in the production process of the things, and the corresponding method allows to calculate an adequate schema of flow intensities of the objects primary information – generators of dangers in aviation sector.

Thus, by using well known macroeconomic indicator *GDP* (or similar), we can to programming the effective distribution of limited resources to ensure the object safety, in particular, when the devices software and hardware aviation sector computer network of things will be manufactured.

КОМП'ЮТЕРНА СИСТЕМА АНАЛІТИЧНОЇ ОЦІНКИ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ТА ЇЇ ОПЛАТИ

Промислово розвинуті країни світу замість тарифної системи оплати і оцінки будь якої праці ефективно використовують інформаційні системи аналітичної її оцінки. В даний час декілька американських компаній монополізували ринок впровадження цих систем та надання відповідних послуг. Разом з тим, практично всі пострадянські країни до даного часу використовують морально застарілу систему тарифної оцінки праці та нарахування її оплати. Колектив авторів створив вітчизняний аналог – інтелектуальну систему аналітичної оцінки професійної діяльності та її оплати. Система базується на існуючих базових нормативних документах, розробленому теоретичному та методологічному базису, використовує можливості теорії і практики штучного інтелекту. І на відміну від існуючих систем враховує значно більшу кількість факторів та можливостей міжнародної інформаційної інтеграції та можливостей сучасних цифрових технологій. Коротко розглянемо основні (базові для розуміння) елементи даної розробки.

Складність праці – об'єктивна характеристика, що відображає зміст процесу праці і проявляється у вимогах до кваліфікації до робітника. Аналітичне оцінювання професійної діяльності передбачає виділення характеристик верхнього рівня структурних елементів (сутностей) моделі, які, у свою чергу, поєднують характеристики окремих операції за певними ознаками: освітньо-кваліфікаційний рівень, методи, засоби виконання операцій тощо, тобто розширюють і поєднують елементи моделей. Запропонований метод виділення структурних елементів професійної діяльності та поєднання їх за чітко визначеною ознакою в групі дозволяє отримати структурну модель професійної діяльності більш детального рівня, у якій основний акцент робиться на характеристиках сутностей та зв'язок між ними як елементами складної системи.

Авторами запропоновано використовувати теорію нечітких множин та описати фактори лінгвістичними змінними. На відміну від існуючої методики, яка потребує постійного оновлення баз даних інструментів, обладнання тощо, авторами визначено поле знань, розроблено алгоритми та правила роботи експертної системи для оцінювання складності робіт робітників з використанням лише характеристик факторів верхнього рівня, описаних лінгвістичними змінними.

В межах дослідження було визначено поле знань (область або множина) – модель знань про предметну галузь, тобто здійснено перехід від структурованих знань до їх формалізації. Продукційна модель знань N_p (продукцій) подана кортежем:

$$N_p = (S_{p_d}; R_{a_p}; A^r \rightarrow A^s; R_{b_p}),$$

де S_{p_d} – опис класу d ситуацій для p - моделі, $p = \{1 \dots p\}$, $d = \{1 \dots d\}$;

R_{a_p} – умова, за якою p продукція активується;

$A^r \rightarrow A^s$ – ядро продукції;

R_{b_p} – умова (дія), яку необхідно виконати після реалізації ядра:

$$P_t = \bigwedge_{r=1, r} A^r \rightarrow \bigwedge_{s=1, s} A^s. \quad (1)$$

де P_t – позначення t -ї продукції;

t – кількість продукцій у продукційній моделі;

A^r – змінний предикат (факт) від r змінних, який має назву посилки;

A^s – змінний предикат (факт) від s змінних, який має назву заключення, або термінальний предикат.

У дослідженні розроблено базові функціональні елементи експертної системи аналізу операцій як одного з модулів ІТ аналітичного оцінювання та визначено поле знань – модель знань про предметну галузь, тобто перехід від структурованих знань до їх формалізації.

Узагальнену синтаксичну структуру поля знань подано виразом:

$$F_k = (A, M, E),$$

де $A = \{A_b, A_f\}$ – структура вхідних даних, які підлягають інтерпретації в системі; $M = (S_k, S_f)$ – модель інтерпретації даних, де S_k – концептуальна структура предметної галузі; S_f – функціональна структура, яка моделює схему міркувань під час інтерпретації; $E = \{E_o, E_a\}$ – структура вихідних даних.

Функціональну модель системи аналітичного оцінювання операцій професійної діяльності зображено на рисунку.

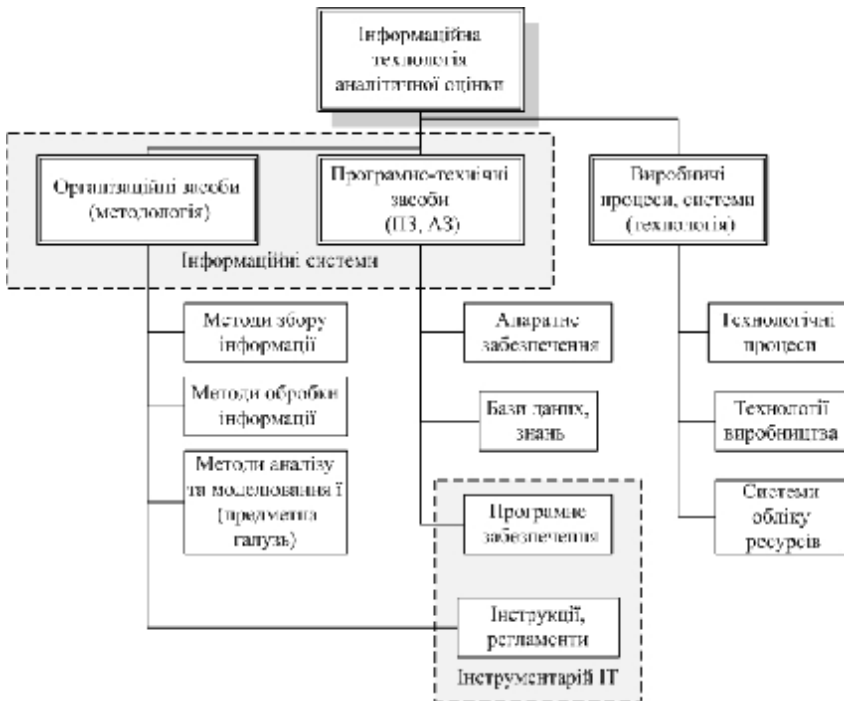


Рис. 1. Склад системи аналітичної оцінки

СХЕМА МНОЖИНОГО ДОСТУПУ В ШИРОКОСМУГОВІЙ БЕЗДРОТОВІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ LTE

Актуальним питанням є оптимальна настройка і моделювання роботи антен, використовуваних в якості провідника для випромінювання або уловлювання електромагнітної енергії з простору в бездротових широкосмугових регіональних мережах *WiMAX*. При двостороннього зв'язку одна і та ж антена використовується як для прийому, так і для передачі сигналу. Збільшення кількості антен і правильне розосередження їх у просторі здатне збільшити пропускну здатність, радіус дії системи і зменшити загасання сигналу. Моделювання та порівняння різних конфігурацій розташування і налаштувань антен здатне істотно підвищити ефективність функціонування мережі і знизити вартість на проектування і впровадження.

Сучасні архітектури інтернету не забезпечують повної гарантії якості. До теперішнього моменту часу запропоновано безліч адаптивних методів, які дозволяють зробити додатки реального часу більш толерантними до варіацій затримок і втрат пакетів. Незважаючи на це, проблема якісної передачі мультимедійного трафіку в мережах *TCP / IP* залишається вирішеною не до кінця [1].

В основу технології *WIMAX* покладена стільникова топологія передачі інформації, де кожна базова станція (БС) стільники повинна забезпечувати в рамках стільники передачу мультимедійного трафіку (ММТ) з заданою якістю обслуговування *QoS*. Однією з головних особливостей в процесі функціонування мережі є управління під час виникнення різних конфліктів ситуацій. До конфлікту ситуацій можна віднести найбільш поширені: перевантаження мережі в цілому, що найчастіше характерно для передачі мультимедійного трафіку в реальному часі, перевантаження її окремих компонентів або сегментів, вихід з ладу окремих компонентів мережі, порушення нормального процесу функціонування мережі. Наслідки таких ситуацій полягають в повну або часткову відмову функціонування компонент мережі, зниженні її продуктивності в цілому і окремих

компонент, порушення зв'язності мережі, в погіршенні якості обслуговування деякої частини абонентів і в спотворенні або знищенні інформації, що надається їм.

При плануванні і моделюванні роботи приймально-передавального обладнання мобільного бездротового широкосмугового комп'ютерної мережі *Wimax* на основі множинного доступу (*MIMO*) необхідно особливу увагу приділяти такими етапами:

- формування діаграми спрямованості (ДН) антени зі зворотним зв'язком, при формуванні якої радіочастотні електричні імпульси передавача за допомогою антени перетворюються в електромагнітну енергію, яка випромінюється за певним принципом в навколишній простір [1]. Для поліпшення якості, зони покриття, пропускної спроможності системи та зменшення ймовірності порушення зв'язку система використовує багатоелементні антени на основі множинного доступу;

- просторове - часове кодування (без зворотного зв'язку) - техніка передачі рознесеного радіо прийому, підтримує просторове рознесення і зменшує кордону замирання сигналу [2];

- просторове мультиплексування, без зворотного зв'язку забезпечує переваги високої швидкості передачі даних і пропускної здатності. Порівнюючи з системами обладнаними одиничними антенами, приймач обладнаний багатоелементними антенами може розділити різні потоки інформації і функціонувати з високої пропускної здатності. Особливо ефективно можливо використовувати дане властивість при передачі мультимедійної інформації, яка складається з двох основних потоків - аудіо і відео.

ВИКОРИСТАНІ ДЖЕРЕЛА

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 // Математические машины и системы. – № 6. – 2001. – С.56-69.

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЛЬОТНУ ПІДГОТОВКУ В АВІАЦІЇ ПОВІТРЯНИХ СИЛ

Досвід участі авіації повітряних сил в антитерористичній операції на сході України надав певний поштовх використанню сучасних інформаційних технологій в системі льотної підготовки. Суттєво було збільшено використання у польотах, у тому числі на бойове застосування додаткових GPS пристроїв.

Для обчислювання навігаційних задач та бойових (спеціальних) завдань стали використовуватися електронні планшети зі спеціальним програмним забезпеченням.

При цьому були проведені позитивні випробування передачі тактичної обстановки на електронний планшет, який знаходиться на борту літака (вертольоту). Поступово впроваджується у практику використання льотним складом тактичних тренажерів для відпрацювання питань тактичної взаємодії із взаємодіючими групами, а також протидії віртуальному противнику у різних умовах обстановки.

Водночас, слід зауважити, що розробка спеціального програмного забезпечення для електронних планшетів та тактичних тренажерів вітчизняними волонтерами та фахівцями провідних установ здійснюється у ініціативному порядку без належної державної підтримки.

При цьому, використання електронних планшетів у польоті потребує нормативного урегулювання.

Аналіз високотехнологічної продукції вітчизняних розробників та виробників показує, що вона здатна забезпечити вирішення широкого кола завдань:

- проведення навігаційних та тактичних розрахунків;
- підтримку прийняття рішення;
- безпаперову підготовку;
- контроль (самоконтроль) готовності авіаційного персоналу до польотів;
- аналіз якості виконання польотного (бойового) завдання.

Всі без винятку завдання є актуальними, але зупинимось на ключовому - підтримка прийняття рішення. Адже при збільшенні об'єму інформації, яка проходить через осіб бойової обслуги, до деякої межі, зменшується якість її обробки, збільшується час. Погіршується ефективність рішень, які приймаються. Виникає протиріччя між збільшенням кількості потрібної інформації та часом на ухвалення оптимального рішення.

Запропонований метод розподілу задач розпізнає функціональний стан оператора, та в залежності від його стану проводить перерозподіл завдань між особами бойової обслуги. Розглядається варіант формалізації процесу розпізнавання ситуацій з їх подальшим структуруванням. Завдання, які вирішує система підтримки прийняття рішень (СППР), структуруються за ознакою автоматизації на автоматичні, полу автоматичні та ті, що вирішуються лише оператором. В перспективних СППР повинно бути закладено “адаптивне управління” в основі якого лежить поняття функціонального стану оператора та його спроможності приймати адекватні кваліфіковані рішення.

З метою упорядкування питань впровадження інноваційних технологій в систему льотної підготовки авіації повітряних сил доцільно проведення досліджень з подальшою розробкою відповідного комплексу заходів (“дорожньої карти”, програми).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Олексів І. Б. Метод прийняття управлінських рішень на засадах компромісного розв'язання / І. Б. Олексів // Актуальні проблеми економіки.— 2004. — №12(42). — С. 142—149.
2. Ситник В. Ф. Системи підтримки прийняття рішень: Навч. посіб. / В.Ф. Ситник. — К.: КНЕУ, 2009. — 614 с.
3. Системи підтримки прийняття рішень:] Навч. посіб. Для самост. вивч. дисц. / [укл.: С.М. Братушка, С.М. Новак, С.О. Хайлук] — Суми: ДВНЗ “УАБС НБУ”, 2010. — 265 с.
4. Дюк В.А. Data Mining – интеллектуальный анализ данных [Электронный ресурс] / В.А. Дюк. – Режим доступа: <http://www.olap.ru/basic/dm2.asp>.

МОДУЛЬНЕ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тести – не єдиний інструмент для забезпечення якості коду. У наш час також є інструменти статичної типізації та утиліти для перевірки коду (linters). Вони виконують статичний аналіз коду для пошуку невідповідностей обраному стилю коду, неправильного використання мови, помилок в контракті даних і багато іншого [1].

Vue Test Utils – офіційна бібліотека для модульного тестування Vue-компонентів. Шаблон webpack vue-cli йде в комплекті з Karma або Jest, як з добре підтримуваними програмами запуску тестів.

Контрактом даних називають формат даних, який буде використовуватися деякою частиною додатка, наприклад функцією [3]. Зазвичай під цим розуміється в якому вигляді будуть представлені дані, наприклад, тип вхідних і вихідних даних.

Статична типізація в мовах програмування, робить код більш безпечним на основі кожного контракту. Такі інструменти, як TypeScript або Flow, дозволяють визначати змінні, параметри і типи значень, що повертаються. Вони гарантують, що класи, функції та методи мають певну структуру, а інша частина коду завдяки цьому, виконується. Багато компаній, які використовують статичну типізацію, відразу ж припускаються до кількох помилок.

Наприклад, порівняємо типізовану і не типізовану версію функції sum:

```
// Не типізована функція
function sum(a, b)
{   return a + b;
}
// Типізована функція
function sum(a: number, b: number) : number
{   return a + b;
}
```

Версія функції без вказівки типів не заважає викликати її з невеликими вхідними даними, в результаті повертаючи конкатенацію рядків. Наприклад, виклик sum ('1', '2') повертає '12'. Однак, якщо використати статичну типізацію, отримуємо помилку,

таку як `Argument of type "1" is not assignable to parameter of type 'number'`, і ця помилка типізації запобігає під час компіляції зробити виклик функції, який поверне невірний результат, оскільки ми очікуємо складання чисел, а не конкатенацію рядків.

Вищенаведений тест досить простий, але на практиці у Vue-компонентів інші призначення, які можливо перевірити, наприклад: виклики до API, здійснення або відправка мутацій або дій зі сховищем Vuex, тестування взаємодії.

Хоча є кілька розбіжностей з приводу кількості типів тестів та їх імен, найбільш поширеними є тести компонентів і API. Це всього лише особливі типи інтеграційних тестів. Зокрема, тести компонентів – це тести, які пишуться на стороні фронтенда при тестуванні програми.

Найлегше створювати і обслуговувати модульні тести, тому що, вони тестують певну функціональність ізольовано, тому більшість тестових наборів - це модульні тести.

Модульні тести найбільш корисні під час розробки, або щоб допомогти розробнику подумати як саме спроектувати компонент, або відредагувати існуючий компонент. Вони запускаються кожен раз при зміні коду.

Vue Test Utils і величезна екосистема JavaScript забезпечують безліч інструментів для того щоб забезпечити майже 100% покриття тестами. Однак модульні тести є лише частиною піраміди тестування. Є й інші типи тестів, включаючи тести e2e (end-to-end) і тести знімками (snapshot). Модульні тести - це найменші і найпростіші тести.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Блэк Р. Ключевые процессы тестирования. Пер. с англ. - М.: ЛОРИ. 2006. — 214 с.
2. Криспин Л., Грегори Дж. Гибкое тестирование: практическое руководство для тестировщиков ПО и гибких команд. : Пер. с англ. — М. : ООО “И.Д. Вильямс”, 2010. — 464 с. : ил. — Парал. тит. англ..
3. Канер Сэм и др. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-решений: Пер. с англ. / Сэм Канер, Джек Фолк, Енг Кек Нгуен. – К.: «ДиаСофт», 2001. – 544 с.

**ОРГАНІЗАЦІЯ ПЕРЕДАЧІ ДАНИХ МІЖ КЛІЄНТАМИ
МЕРЕЖІ НАВІГАЦІЙНИХ ПРИСТРОЇВ G²S**

Організація швидкого і захищеного доступу мобільних пристроїв до серверів додатків / сервісів / ресурсів мережі Інтернет неможлива без створення бездротової мережі. Прикладом побудови такої мережі слугує проект G²S (Go to the sound – іди на звук).

G²S - система навігації інвалідів зору використовуючи озвучення об'єктів інфраструктури. Ідея комплексу полягає в пошуку включених маяків через мобільний додаток. Основна проблема полягає в передачі даних між маяком і мобільним додатком. Маяк оснащений мікроконтролером ESP32 з вбудованим Wi-Fi модулем: 802.11b/g/n/e/i, до 150 Mbps с HT40 та Bluetooth: v4.2 BR/EDR і BLE. Через мобільний додаток користувач має можливість обрати маяк. При наближенні до маяка на відстань 50-70 м подається звуковий та/або вибросигнал про доступність обраного маяка для керування. Передача даних здійснюється вбудованим Wi-Fi модулем TCP/IP протоколами. IP – фундаментальний протокол з комплекту TCP/IP – він передає IP-дейтаграми та виконує функцію маршрутизації, тобто визначає маршрут за яким буде прямувати IP-дейтаграма. TCP – протокол вищого рівня, який дозволяє прикладним програмам, запущених на різних комп'ютерах мережі, обмінюватись потоками даних. TCP ділить потоки даних на TCP-сегменти й передає їх за допомогою IP. Визначається Wi-Fi точка мобільний додаток отримує ID маяка. Маяк у свою чергу отримує IP телефону.

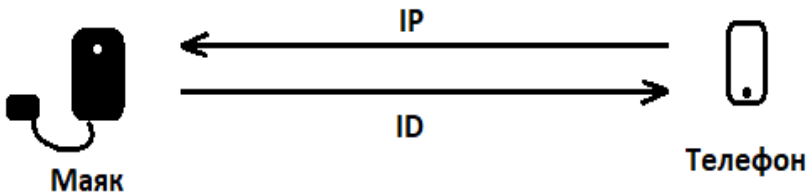


Рис.1. Передача адрес від телефону до маяка й навпаки

Формуючи протоколи TCP передає пакети даних на IP, який було визначено раніше. IP не гарантує, що TCP-сегменти будуть отримані в тій же послідовності в якій були відправлені, тому TCP виконує повторний збір TCP-сегментів на іншому кінці маршруту.

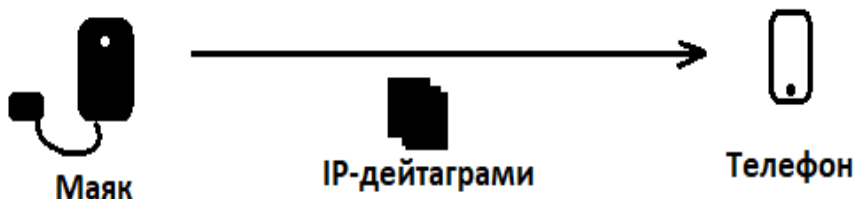


Рис.2. Передавача IP-дейтаграм від маяка на телефон

TCP забезпечує перевірку на наявність помилок та обмін перевіряючими повідомленнями, щоб дані досягли свого місця без спотворень. Маяком надсилаються контрольні суми для перевірки цілісності даних, телефон у свою чергу відправляє підтвердження про прийняття даних без помилок.

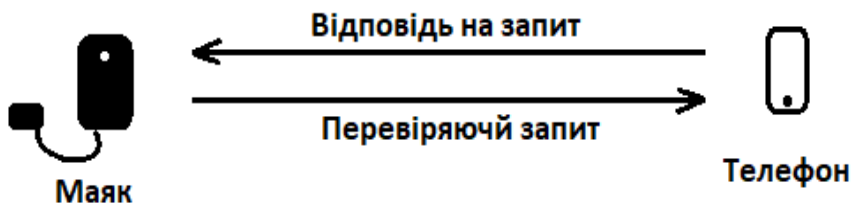


Рис.3. Відправка перевірочних запитів та підтверджуючих повідомлень

Таким чином в мережі навігаційних пристроїв G2S за допомогою Wi-Fi зв'язку та TCP/IP протоколів забезпечується швидка та безпечна передача даних.

ОРГАНИЗАЦИЯ ВЫЧИСЛЕНИЙ ПОД УПРАВЛЕНИЕМ ПОТОКА ДАННЫХ

Одним из подходов к ускорению решения задач является организация вычислений под управлением потока данных, реализуемых в потоковых вычислительных системах (ПВС) [1]. Известно множество моделей ПВС, однако многие присущие им ограничения так и не были преодолены [1]. Одна из причин кроется в идеализации чисто потоковой реализации вычислений.

Предлагается модель организации вычислений под управлением потока данных (рис.1), в которой предусмотрено их некоторое предварительное планирование.

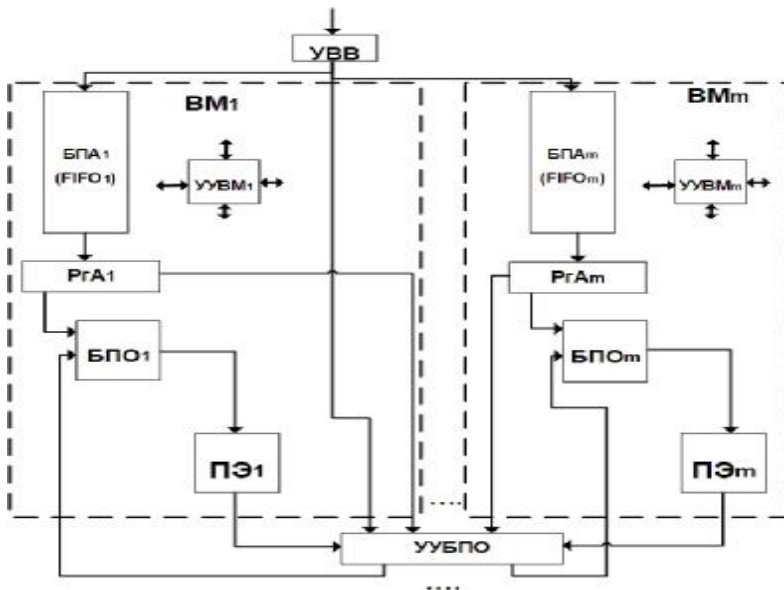


Рис.1 Структура ПВС: УВВ – устройство ввода-вывода; ВМ – вычислительный модуль; УУВМ – устройство управления ВМ; БПА и БПО – блоки памяти акторов и операндов соответственно; РгА – регистр акторов; ПЭ – процессорный элемент; УУБПО – устройство управления записью в БПО

Транслятор системы получает ярусно-параллельную форму графа потока вычислений задачи. Планировщик исходя из числа m ВМ формирует столько же очередей акторов и связанных с ними групп операндов. Каждая очередь посредством УВВ вводится в БПА (реализованный как FIFO), а группы операндов посредством УВВ и УУБПО в БПО (реализованный как 2-портовое ОЗУ) соответствующего ВМ. На этапе функционирования ПВС в каждом ВМ после выполнения предыдущей команды с выхода БПА в РГА поступает очередной актор. При этом их очередь в БПА продвигается. По адресам в полях актора считываются операнды. Если все они присутствуют в БПО, то формируется готовая к выполнению команда, передаваемая на вход ПЭ. Очередной результат посредством УУБПО по адресу в поле текущего актора (находится в РГА) записывается в соответствующий БПО этого или другого ВМ, и выполнение текущей команды завершается. Затем с головы очереди в БПА считывается новый актор, и цикл выполнения команды повторяется вновь. Координация описанных действий в пределах ВМ осуществляется УУВМ. Совмещение во времени функционирования всех ВМ обеспечивает высокий уровень параллелизма вычислений.

Предложенная модель ПВС обладает следующими преимуществами:

- не использует ассоциативную память и громоздкие коммутационные сети (наибольший объем пересылки данных приходится на считывание операндов и акторов, которые во всех ВМ выполняются параллельно и независимо);
- простая программная реализация транслятора и планировщика, который можно настраивать на использование известных дисциплин предварительного формирования очередей команд [2] для повышения производительности ПВС;
- эффективная реализация на базе ПЛИС с учетом масштабируемости и отказоустойчивости.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Барский А.Б. Вычислительная система, управляемая потоком данных / А.Б. Барский, В.В. Шилов // Приложение к журналу "Информационные технологии". – 2000. - №8. - 24 с.
2. Симоненко В.П. Организация вычислительных процессов в ЭВМ / В.П. Симоненко. – К.: «Век+», 1997. – 304 с.

МОДУЛЬ АНАЛІЗУ ДОСТОВІРНОСТІ СУПУТНИКОВИХ СИГНАЛІВ НА ОСНОВІ ІМІТАЦІЙНОЇ МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ

В [1] розглянуто підхід до побудови правил логічного висновку з використанням теорії нечітких множин. В [2], на основі запропонованих логічних правил, розроблені методи створення підсистем (модулів) штучного інтелекту, засновані на використанні нечіткого структурного графа.

Метод дозволяє створювати моделі синтезу рішень на основі формалізації «бачення світу завдання» людиною - досвідченим експертом (групою експертів). В результаті розроблені способи створення модуля, що імітує роботу оператора з аналізу поточної ситуації і вироблення командних сигналів.

Використання безпілотного літального апарату (БПЛА), в області, що інтенсивно розвивається, після періоду їх роботи в інформаційно-допоміжних цілях (фото-відео розвідка, коригувальники, ретранслятори і т.п.), з'являється явна тенденція до використання «ударних» БПЛА, здатних нести зброю і завдавати шкоди противнику. Відповідно до цієї тенденції різко зросла кількість розробок, спрямованих на протидію саме цього, відносно нового, виду зброї.

Методами боротьби з БПЛА противника, головним чином, залишаються застосування засобів ППО і засобів радіоелектронної боротьби (РЕБ). Традиційні існуючі засоби ППО, по відношенню до БПЛА, на жаль, не виправдано дорогі, тому що розраховувалися, в основному, на боротьбу з вельми не дешевими бойовими ЛА і ракетами тактичного рівня. На цьому тлі, перспективними і реально затребуваними стають «інтелектуальні» засоби РЕБ.

Основні методи їх застосування:

- «засліплення» систем навігації із застосуванням потужного поміхо-шумового придушення радіосигналів заданого спектра;
- спотворення навігаційних сигналів (перш за все, імітація роботи помилкових псевдосупутників, що ведуть до дезорієнтації бортових систем навігації і деградації систем управління);

- розшифровка і декодування системи команд управління від «санкціонованих» операторів і заміна їх помилковими сигналами більшої потужності - «перехоплення управління на себе».

У свою чергу, системи навігації та управління БПЛА, в основному, використовують три методи (частіше, їх комплексування):

- навігація по сигналам від зовнішніх джерел (радіомаяки, супутники, ретранслятори і т.п.);
- автономна навігація з використанням інерційних систем;
- використання керуючих сигналів від зовнішнього оператора.

Основна проблема автономних (захищених) інерційних систем - «далі летимо - більша помилка». Тому і використовують незалежні від часу польоту «зовнішні» джерела що, на жаль, піддаються ризику компрометації.

Авторами запропонований підхід до створення модуля, як елемента системи управління БПЛА, призначеного для розпізнавання факту придушення (найпростіший випадок), а також несанкціонованої дискредитації сигналів навігації і/або управління. Модуль дозволить розпізнати факт появи хибних сигналів, дасть вказівки системі ігнорувати/компенсувати фіктивні дії і використовувати «довірчі» режими роботи, що дозволить виконати маневр - «повернення на вихідний/заданий кінцевий пункт маршруту» або навіть завершити виконання завдання в автономному режимі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Коврижкін О.Г. Формирование компромиссных правил нечеткого вывода // Техн. кібернетика – 1992. – № 5. – С. 50-55.

2. Коврижкін О.Г. Аксиоматика имитационной модели принятия решений // Материалы международной конференции: Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта (isdmcI'2009) – 2009 г., Евпатория, Украина, Т. 1. – С. 181.

ПРИНЦИПИ ФУНКЦІОНУВАННЯ ПРОТОКОЛІВ IP Security

У наш час велика кількість мереж з'єднана між собою за допомогою Інтернет. Тому очевидно, що для безпечної роботи такої великої системи необхідно приймати деякі міри захисту. Проблема безпеки мереж залишається невирішеною і на сьогоднішній день, оскільки у більшості компаній не вирішені питання забезпечення безпеки, у результаті чого вони несуть фінансові збитки.

Окрім крадіжки інформації, загрозу можуть представляти атаки типу «відмова в обслуговуванні» та крадіжки послуг.

Також у наш час на ряду з мережевою безпекою значно зросла потреба в управлінні трафіком, як у локальних мережах організацій, так і у глобальній мережі Інтернет. Це пов'язано зі значним розвитком за останнє десятиліття специфічного контенту, який передереться через мережі. До цього контенту можна віднести графічну інформацію, голосові а також відео конференції, потокове відео та аудіо та інше. Ця інформація надзвичайно перевантажує мережеві лінії.

IP Security – це комплект протоколів, що стосуються питань шифрування, аутентифікації і забезпечення захисту при транспортуванні IP-пакетів.

Застосування всього комплексу механізмів IPSec дозволяє забезпечити перевірку цілісності переданих даних, їх конфіденційність (шифрування переданих даних з метою їх захисту від несанкціонованого перегляду), захист від повторень і справжність.

Гарантії цілісності і конфіденційності даних в специфікації IPSec забезпечуються за рахунок використання механізмів аутентифікації і шифрування відповідно. Специфікація IPSec передбачає можливість підтримки сторонами інформаційного обміну різних протоколів і параметрів аутентифікації і шифрування пакетів даних, а також різних схем розподілу ключів.

На відміну від SSL (Secure Socket Layer), який працює на четвертому (транспортному) рівні і тісніше пов'язаний з більш

високими рівнями моделі OSI, IPSec покликаний забезпечити низькорівневий захист.

Крім того, протокол можна використовувати для створення міжмережевого екрану. Сенс міжмережевого екрану полягає в тому, що він контролює і фільтрує пакети, що проходять через нього, відповідно до заданих правил. Встановлюється набір правил, і екран переглядає всі пакети які проходять через нього. Якщо передані пакети потрапляють під дію цих правил, міжмережевий екран обробляє їх відповідним чином. Налаштувавши політику безпеки відповідним чином, можна, наприклад, заборонити інтернет-трафік. Для цього достатньо заборонити відсилання пакетів, в які вкладаються повідомлення протоколів HTTP та HTTPS.

IPsec можна застосовувати і для захисту серверів. Для цього відкидаються всі пакети, окрім пакетів, необхідних для коректного виконання функцій сервера.

IPSec – є найпопулярнішим стандартом для створення корпоративних VPN-мереж і підтримується більшістю виробників мережевого устаткування і розробників операційних систем.

Для зв'язку між мережами IPSec зазвичай застосовується в тунельному режимі з протоколом ESP.

По суті, між двома шлюзами організовується захищений IP-тунель. Разом з IPSec часто використовуються і інші протоколи тунелювання, які забезпечують передачу поверх IPSec багатоадресних розсилок (multicast), протоколів маршрутизації, інкапсуляцію протоколів другого рівня.

На масштабованість IPSec впливає швидке зростання числа тунелів при збільшенні числа вузлів в мережі.

На безпеку IPSec впливає безліч чинників, і, навіть, VPN- шлюзи з досить якісною реалізацією протоколу IPSec можуть бути зламані із-за неправильних налаштувань на етапі впровадження або експлуатації.

Основні чинники, які необхідно враховувати при виборі і впровадженні рішень IPSec VPN, це:

- управління ключами;
- надійність використовуваної криптографії;
- безпечна реалізація протоколів в VPN- продуктах;
- захищеність VPN- мережі від атак.

BUG TRACKING SYSTEM FOR IT PROJECT

A project is a temporary endeavor, or discipline, undertaken to create a unique product, service, or result. It leads the project from concept development to project completion. IT project management is a sub-discipline of project management in which information technology projects are planned, monitored and controlled. In other words, a project is a sequence of tasks bounded by time, resources and required results; has a defined outcome and deliverables; has a deadline; and has a budget limiting number of people, supplies and capital. It can any type of project that deal with IT infrastructure, information systems, or compute technologies. This can include, but is not limited to: developing mobile apps, programming large-scale software system, updating a web-page, creating an online shopping site, developing an entire web infrastructure, employing IT security measures.

Project characteristics include:

- Accomplishment with shared resources often only available on part-time basis
- Cross-functional team work may be required
- Uncertainty and potential change during execution
- Changes to the way the business operates
- Specific deadlines, time and resource constraints.

When the organization assumes the launch of a new project, it is always about having something “final” as a goal. To develop software products is not a project. The project is, for example, “the creation and implementation of the information system X by December 1 of the next year”.

The reason for the transition from general (functional) management to project management is more often due to reliability instead of a relative abstract perspective to predictable results.

The bug tracking system (the bug tracking system) is an application program designed to help software developers (programmers, testers, etc.) record and monitor errors (bugs) found in programs, as well as monitor the process of eliminating these bugs.

BTS helps programmers keep track of bugs. When the programmer noticed an error or a bug, the maximum amount of available information of a bug has to be collected. It is necessary to be extremely accurate in the observations. This is especially essential for bug reports from users.

BTS allows storing bug information in the following form:

- defect number (identifier);
- short description of the defect;
- who reported the defect;
- date and time when the defect was discovered;
- the version of the product in which the defect is found;
- the severity of the defect and the priority of the solution;
- a description of the steps to identify the defect (reproducing unintended program behavior);
- expected result and actual result;
- who is responsible for eliminating the defect;
- current state (status) of the defect;
- version of the product in which the defect is fixed.

It should be noted that error tracking systems can be useful not only for programmers. Bug reports can be used by project managers. In fact, such reports give an indication of the performance of programmers when working to improve software performance. When processing reports, it is necessary to consider the priority of errors and the complexity of their elimination. The manager must understand that some errors can be difficult to fix, due to the system architecture. It makes no sense to demand the speedy elimination of errors in the system modules: unreasoned actions to eliminate one error can generate hundreds of other errors.

REFERENCES

1. Gauri M. Puranik, Design of Bug Tracking System/ International Journal of Innovative Research in Science, Engineering and Technology [Web resource]. – Access mode - <http://www.ijirset.com/upload/2014/july>
2. <http://www.bug-track.com> [Web resource]. – Access mode - <http://www.bug-track.com>

МЕТОДИ ТЕСТУВАННЯ ТА ПІДТВЕРДЖЕННЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою - комплексність.

Існують десятки технічних методів тестування безпеки, які можна умовно згрупувати за такими категоріями [1]:

1. Методи дослідження.
2. Методи аналізу цілі.
3. Методи підтвердження наявності вразливостей.

Розглянемо більш детально методи підтвердження наявності вразливостей. Мета застосування цих методів полягає в тому, щоб довести, що існує проблема вразливості системи, а також для демонстрації впливу на інформаційну безпеку, в разі експлуатації вразливості. Методи підтвердження наявності вразливостей включають найбільші ризики, оскільки ці методи мають більший потенціал впливу на цільову систему або мережу, ніж інші методи.

До методів підтвердження наявності вразливостей відноситься:

1. Підбір паролів. Коли користувач вводить пароль, генерується хеш введеного пароля і порівнюється зі збереженим хешем фактичного пароля користувача. Якщо хеші збігаються, то користувач проходить аутентифікацію.

Підбір паролів це процес відновлення фактичних паролів з їх хеш-значень, що зберігаються в комп'ютерній системі або передаються по мережі. Можлива також атака за словником, тобто використання для генерації не випадкових значень а типових значень слабких паролів. Інший спосіб злому відомий як гібридна

атака, ґрунтується на словниковому методі, додаючи числові і символічні знаки до слів зі словника. Ще один метод підбору паролів називається методом грубої сили. Підбір паролів може також бути виконаний за допомогою райдужних таблиць, це таблиці з попередньо обчисленими хешами паролів. [2].

2. Тест на проникнення. Тест на проникнення це техніка, в якій аудитори безпеки імітують реальні атаки, щоб визначити методи для обходу функцій безпеки програми, системи або мережі. Вона часто включає в себе запуск реальних атак на реальні системи і дані, з використанням інструментів і методів, які зазвичай використовуються зловмисниками. Системи можуть бути пошкоджені або іншим чином виведені з ладу в процесі тестування на проникнення. Тестування на проникнення часто включає в себе нетехнічні методи атаки.

Висновки:

1. Існуючі методи дослідження інформаційної безпеки підприємства умовно розділені на 3 категорії: методи дослідження, аналізу цілі та підтвердження наявності вразливостей.

2. Методи підтвердження наявності вразливостей застосовуються для виявлення вразливості системи, а також для демонстрації впливу на інформаційну безпеку підприємства.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Аверченков В.И. Аудит информационной безопасности, учебное пособие// ФЛИНТА 2011.

2. FreeBSD Handbook [Електронний ресурс]// Режим доступу: <https://www.freebsd.org/doc/handbook/>

¹С. В. Лазаренко, д.т.н.,

¹С. Д. Войтенко, к.т.н.

²Т. В. Німченко, к.т.н.

¹Національний авіаційний університет

²Київський національний університет ім. Тараса Шевченка

АНАЛІЗ МЕТОДІВ ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Існують десятки технічних методів тестування безпеки, які можуть бути використані для оцінки рівня інформаційної безпеки. Їх можна умовно згрупувати за такими категоріями [1]:

- *Методи дослідження.*
- *Методи аналізу цілі.*
- *Методи підтвердження наявності вразливостей.*

Тестування інформаційної безпеки підприємства складається з 4 фаз. Кожна фаза реалізується із застосуванням зазначених методів і відбувається в такому порядку:

- фаза планування;
- фаза дослідження;
- фаза атаки;
- звіт.

На етапі планування, визначаються правила аудиту, документально встановлюється мета аудиту та підтвердження обізнаності керівництва про майбутнє тестування. Етап планування встановлює основу для успішного тесту на проникнення. Фактичного тестування в цій фазі не відбувається.

Фаза дослідження складається з двох частин. Перша частина є початком фактичного тестування, і охоплює збір інформації та сканування.

Друга частина фази є фактичним аналізом вразливостей, який включає визначення сервісів, додатків і операційних систем сканованих хостів, пошук по базах вразливостей (процес, який відбувається автоматично для сканерів вразливостей) і ручне тестування експертом аудитором. Експерти можуть використовувати свої власні бази для виявлення вразливостей вручну.

Далі слідує фаза атаки. Вона складається з таких кроків:

- отримання доступу до системи;
- підвищення власних привілеїв;
- дослідження системи всередині;
- встановлення додаткових утиліт для полегшення

повторного доступу.

Якщо атака пройшла успішно, вразливість документується і розробляються рекомендації для її усунення. У багатьох випадках, експлуатовані вразливості не надають максимальний рівень потенційного доступу для зловмисника. Замість цього вони можуть надати аудиторам додаткові інформацію про цільову мережу і її потенційні вразливості, або викликати зміну стану безпеки цілі. Деякі вразливості дозволяють аудиторам підвищувати свої привілеї в системі або мережі, та отримувати доступ до додаткових ресурсів. Якщо це стається, потребує проведення додаткового аналізу і тестування, щоб визначити справжній рівень ризику для мережі, та типи інформації, що може бути скомпрометована.

Фаза звітності відбувається одночасно з іншими трьома фазами випробувань на проникнення. У фазах дослідження та атаки, зазвичай записуються для подальшого зберігання журнали подій і формуються періодичні звіти для системних адміністраторів і менеджменту. По завершенні тестування, звіт, як правило, розробляється для опису виявлених вразливостей, оцінки ризику, а також подальшими рекомендаціями, щодо пом'якшення ризику.

Таким чином, питання аудиту інформаційної безпеки описані у значній кількості літератури, однак досі не існує єдиного стандарту та методології для технічного аудиту інформаційної безпеки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Аверченков В.И. Аудит информационной безопасности, учебное пособие // ФЛИНТА. - 2011.

ДЕФЕКТИ КОДУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Традиційно у інженерії програмного забезпечення кількісною характеристикою якості програмного коду є метрика, як певна чисельна величина, яка дозволяє отримати значення деякої властивості ПЗ. Метрики є поширеним і достатньо надійним механізмом оцінки внутрішньої будови програм.

Якість ПЗ – ступінь, в якій ПЗ володіє необхідною комбінацією властивостей [2].

Якість ПЗ – це сукупність характеристик ПЗ, що відносяться до його здатності задовольняти встановлені та передбачувані потреби [3].

Дефект ПЗ – це недолік ПП, що є причиною його неочікуваного виконання [1, 3]. З точки зору користувача, дефект - це те, що не відповідає його очікуванням до програмного забезпечення. Дефект якості програмного коду – недолік програмного продукту, який відображає невідповідність характеристик ПЗ встановленим і передбачуваним потребам [1, 3].

Поняття якості програмного коду є складовою якості ПП. Якість коду може визначатись різними критеріями. Деякі з них мають значення тільки з точки зору людини. Наприклад, форматування тексту програми – неважливо для комп'ютера, але може мати велике значення для супроводу. Багато з існуючих стандартів кодування, що визначають специфічні для мови програмування угоди та задають низку правил, мають на меті полегшити супровід ПЗ в майбутньому. Також існують інші критерії, що визначають якість написання коду, наприклад, такі, як структурованість – ступінь логічного розділення коду на блоки [3].

Метрика – це кількісний масштаб і метод, який може використовуватися для вимірювання [5]. Введення і використання метрик необхідно для поліпшення контролю над процесом розробки, зокрема над процесом тестування [6].

Якість ПЗ може бути описана великою кількістю різнорідних характеристик. Поняття якості програми – багатопланове та може бути виражено адекватно тільки деякою структурованою системою характеристик або атрибутів. Така система характеристик

називається моделлю якості, в якій метрики використовуються для кількісного описання та вимірювання якості.

Вибір метрик варто зробити, ґрунтуючись на методі Альбрехта, а також на методології СММІ (Capability Maturity Model Integration), як найбільш часто використовувані при оцінці якості.

До основних метрик дефектів коду ПЗ можна віднести:

- Метрика Альбрехта;
- Метрика альтернативної щільності помилок (Alternative defect density);
- Метрика щільності помилок для коду автора (Defect density) (для програміста);
- Універсальна метрика якості коду в ході процесу перегляду коду (code review).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. International Standard ISO 8402:1994 Quality management and quality assurance [Електронний ресурс] – 1994. – Режим доступу: http://www.iso.org/iso/catalogue_detail.htm?cs number=20115
2. 1061-1998 IEEE Standart for Software Quality Metrics Methodology [Електронний ресурс] – 1998. – Режим доступу: <http://standards.ieee.org/findstds/standard/1061-1998.html>
3. Marc McDonald; Robert Musson; Ross Smith The Practical Guide to Defect Prevention – Microsoft Press, 2007. – 480p.
4. Тестирование и качество ПО [Електронний ресурс] Качество программного обеспечения / The Institute of Electrical and Electronics Engineers – 2004. – Режим доступу: http://software-testing.ru/files/se/3-10-software_engineering_quality.pdf
5. International Standard ISO/IEC 14598-1 Information technology — Software product evaluation [Електронний ресурс] – 1999. - Режим доступу: http://www.iso.org/iso/catalogue_detail.htm?cs number=24902
6. Program Verification Systems, Метрики кода програмного забезпечення [Електронний ресурс] – 2009. - Режим доступу: <http://www.viva64.com/ru/a/0045/>

В. В. Лукашенко, к.т.н.

Національний авіаційний університет, Київ

МЕТОД ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

При проектуванні та експлуатації комп'ютерних мереж актуальною задачею є вирішення проблеми надання якісних послуг з розподіленою обробкою інформації, яка в значній мірі визначається розвиненістю механізму управління мережею.

Важливою проблемою є розробка інтелектуального методу управління комп'ютерними мережами, що дозволяє достатньо швидко і адекватно реагувати на параметри, що динамічно змінюються, а також забезпечує масштабованість і максимальну незалежність між мережними засобами та додатками користувачів. Відомі методи і способи управління комп'ютерними мережами в основному розраховані на мережі з фіксованою структурою зв'язку і не враховують специфіки динамічної зміни навантаження.

Висока швидкість передачі інформації в комп'ютерних мережах необхідна для інтеграції різних видів інформації, ефективної організації зв'язків між мережами різного рівня та надання кожному користувачеві або мережному додатку необхідних мережних ресурсів.

Інтелектуальність мереж передбачає збільшення гнучкості і надійності мереж, спрощення питань управління мережами, що, у свою чергу, створює нові можливості для користувача, перетворюючи його з пасивного споживача послуг на активного клієнта, який може не тільки замовляти послуги, але й самостійно управляти мережею.

Аналітичний огляд робіт з використання інтелектуальних агентів в комп'ютерних мережах і системах показав, що розглядаються питання організації архітектури мультиагентних систем, питання забезпечення заданого рівня якості обслуговування за допомогою інтелектуальних агентів та організація мобільних агентів в комп'ютерних мережах.

З метою підвищення ефективності керування комп'ютерними мережами запропоновано використовувати багаторівневу систему інтелектуальних агентів.

Більшість існуючих способів забезпечення заданого QoS характеризуються статичним управлінням ресурсів і контролем параметрів перевантаження. Такий підхід не оптимальний і може бути вдосконалений за рахунок використання інтелектуальних агентів.

На основі аналізу систем управління мережами можна зробити висновок, що на сьогодні їх основна функція полягає в інформуванні адміністратора мережі про зміни станів обладнання та реалізації керуючих впливів. Основна ж робота по управлінню мережею – аналіз даних, що надходять, визначення режиму функціонування мережі, а також вибір стратегії управління мережею – повністю лежить на людині.

Як вже було сказано вище, системи управління обчислювальними мережами здійснюють наступні функції:

- ідентифікацію станів мережного обладнання;
- вироблення керуючих впливів;
- реалізацію керуючих впливів на об'єкт управління.

Якщо уявити стан телекомунікаційного обладнання як крапку в багатовимірному просторі, і при цьому класифікувати весь простір можливих станів обладнання (виділити різні області чітко відповідають різним станам), то в такому випадку завдання управління корпоративною мережею можна звести до задачі розпізнавання образів.

На основі проведеного порівняльного аналізу процедур розпізнавання образів і управління обчислювальними мережами, можна стверджувати, що основні етапи процесу управління мережами за своєю суттю ідентичні відповідним етапам процесу розпізнавання образів.

У зв'язку з цим логічно застосувати методи розпізнавання образів у процесі управління корпоративною мережею, і тим самим створити інтелектуальну керуючу систему, яка буде не просто реагувати на заздалегідь запрограмовані ситуації, а й буде здатна забезпечувати якусь логіку зіставлення даних і евристично аналізувати інформацію, що надходить.

ОСОБЛИВОСТІ ЗАХИСТУ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Розвиток комп'ютерних мереж і інформаційних технологій неможливий без комплексного вирішення завдання підвищення ефективності передачі інформації спільно з вирішенням завдання захисту переданої інформації.

Відомі методи і засоби захисту інформації вимагають додаткових матеріальних ресурсів у вигляді програмного, програмно-апаратного забезпечення або апаратних витрат.

Оскільки локальні мережі досить вразливі до сторонніх втручань, з цієї причини розроблені спеціальні методи протистояння їм, адже інформація, що зберігається в кожному з комп'ютерів локальної мережі, безумовно, важлива і одночасно її витік і використання шахраями вкрай небажаний.

Захист локальної мережі базується, перш за все, на безпечній архітектурі всіх комп'ютерів, які в цю мережу входять. Централізована політика безпеки є необхідним, але недостатнім компонентом в плані захисту локальних комп'ютерних мереж. Тому додатково вимагають особливої уваги такі аспекти:

- застосування протоколів обміну, які могли б забезпечити достатню безпеку комп'ютера, інкапсуляція одного з них в інший;
- шифрування даних за допомогою спеціальних алгоритмів;
- застосування в цілях безпеки в архітектурі комп'ютера так званої ДМЗ – демілітаризованої зони, яка буде обслуговуватися парою файрволів;
- застосування програмних засобів по виявленню несанкціонованих вторгнень у локальну мережу, а також механізмів перетворення мережевих адрес – NAT;
- використання засобів захисту периферійних пристроїв за допомогою спеціальної системи доступу, заснованої на принципі двоетапної автентифікації.

Одна з найбільш використовуваних стратегій полягає в установці брандмауера (Firewalls, міжмережеві екрани). Найбільш

поширене місце для встановлення міжмережевих екранів - межа периметра локальної мережі для захисту внутрішніх хостів від атак ззовні. Однак атаки можуть починатися і з внутрішніх вузлів - в цьому випадку, якщо атакується хост розташований в тій же мережі, трафік не перетне кордон мережевого периметра, і міжмережевий екран не буде задіяний. Тому в даний час міжмережеві екрани розміщують не тільки на кордоні, але і між різними сегментами мережі, що забезпечує додатковий рівень безпеки.

Для локальних комп'ютерних мереж зазвичай потрібні стратегії внутрішньої безпеки. Вони включають в себе додавання таких елементів, як захист від вірусів або шкідливих програм. Антивірусна програма – програма для виявлення і видалення програм, що заражені комп'ютерним вірусом, а також для запобігання їх розповсюдження, а також відновлення програм заражених ними. Багато сучасних антивірусів дозволяють виявляти і видаляти також троянські та інші шкідливі програми. І навпаки - програми, що створювалися як файрволи, також знаходять функції, що ріднять їх з антивірусами (наприклад, Outpost Firewall).

Одним із способів захисту інформації всередині мережі є керування доступом, який включає ідентифікацію користувачів та перевірку повноважень. Для розмежування доступу різних груп користувачів потрібно визначати права кожного. Права користувача визначають дозволені типи дій для цього користувача. Дії, регульовані правами, включають вхід у систему на локальний комп'ютер, вимикання, установку часу, копіювання й відновлення файлів сервера й виконання інших завдань.

Таким чином, захист мережі обов'язково повинен включати побудову демілітаризованої зони, яку контролює міжмережевий екран, систему переадресації NAT та систему виявлення вторгнень. Захист локальної мережі також включає наявність на всіх без винятку комп'ютерах, що входять в неї, новітнього програмного забезпечення, причому установка оновлень повинна мати регулярний характер.

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ МЕТОДОМ БАГАТОКРИТЕРІАЛЬНОЇ МАРШРУТИЗАЦІЇ

У даний час комп'ютерні мережі знаходять широке застосування в системах зв'язку, навігації, спостереження та організації повітряного руху. На базі комп'ютерних мереж розробляються інтелектуальні системи управління повітряним рухом. У зв'язку з цим відзначається безперервне зростання складності комп'ютерних мереж, які використовуються для спостереження та організації повітряного руху.

Зростання складності комп'ютерних мереж, підвищення обсягів переданої інформації істотно збільшують вимоги до рівня захищеності інформації від несанкціонованого доступу до неї. Завдання підвищення рівня захищеності комп'ютерних мереж необхідно вирішувати комплексно, спільно із завданнями підвищення ефективності їх функціонування. Актуальність завдання забезпечення інформаційної безпеки користувачів комп'ютерних мереж пов'язана також з широким використанням їх у державних і фінансових організаціях, в промислових авіапідприємствах і в організаціях оборонного комплексу. Один з напрямків підвищення рівня захищеності комп'ютерних мереж пов'язаний з удосконаленням методів маршрутизації передачі інформації в мережах з урахуванням ризиків втрати інформації, її модифікації, а також впливів зовнішніх факторів на канали передачі інформації. Аналіз останніх досліджень і публікацій дозволяє зробити висновок про те, що проблема оцінки і підвищення рівня захищеності комп'ютерних мереж недостатньо повно досліджена. Удосконалення методів маршрутизації в комп'ютерних мережах в даний час розвивається в напрямку забезпечення гарантованої якості обслуговування користувачів комп'ютерних мереж за такими критеріями якості, як пропускна здатність, затримка передачі даних, надійність передачі інформації, завантаження вузлів мережі і ряд інших, до складу яких не входять кількісні оцінки рівня захищеності комп'ютерних мереж.

Тому необхідно розробити метод багатокритеріальної маршрутизації в комп'ютерних мережах, який дозволяє враховувати якість обслуговування та інформаційну безпеку користувачів комп'ютерних мереж.

Пропонується математичну модель комп'ютерної мережі представити графом, вершини якого моделюють вузли-джерела і вузли-приймачі інформації. Гілкам графа присвоюється вага, яка характеризує якість обслуговування і рівень захищеності каналу передачі інформації, що моделюється.

З метою кількісної оцінки ваг гілок графа необхідно скласти систему часткових критеріїв якості для оцінки інформаційної безпеки і якості обслуговування.

Для формулювання задачі багатокритеріальної маршрутизації на графовій моделі необхідно навести всі часткові критерії якості до випадку їх мінімізації.

Таким чином, привласнення гілкам графа, що моделює комп'ютерну мережу, ваг відповідно до багатокритеріальної оптимізації ваг гілок графа з урахуванням системи обмежень дають підстави поставити задачу багатокритеріальної маршрутизації від джерела до приймача інформації, як задачу про найкоротший шлях між вузлом джерелом і вузлом-приймачем, якщо довжина гілки графа пропорційна її вазі. Тому, багатокритеріальна маршрутизація реагує на атаки противника і підвищує рівень захищеності користувачів комп'ютерної мережі.

Розроблений метод багатокритеріальної маршрутизації дозволяє врахувати загрози противника, ризики втрати інформації або її модифікації, пов'язані з несанкціонованим доступом до каналів передачі інформації. Інформаційна безпека комп'ютерної мережі підвищується без залучення додаткових програмних і апаратних засобів захисту інформації. Крім цього, багатокритеріальна маршрутизація забезпечує заданий рівень якості обслуговування по пропускній здатності і надійності передачі інформації, а також враховує зовнішні впливи на канали передачі інформації.

Перевагою запропонованого методу багатокритеріальної маршрутизації є адаптація до зміни ситуацій, в яких функціонує комп'ютерна мережа.

**О. В. Мельничук,
О. А. Пастухов,
О. О. Фатькова**

Національний авіаційний університет, Київ

МОНІТОРИНГ ЗНОСУ ТА ПРОГНОЗУВАННЯ ВІДМОВ МОДУЛІВ КОСМІЧНИХ АПАРАТІВ ЗА ДОПОМОГОЮ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ ТА ОПЕРАЦІЙНОЇ СИСТЕМИ РЕАЛЬНОГО ЧАСУ

Інтелектуалізація вимірювального процесу є підходом до підвищення ефективності функціонування засобів вимірювання. Під поняттям інтелектуалізації процесів отримання і обробки вимірювальної інформації мається на увазі велике коло завдань, спрямованих на підвищення точності вимірювань, передачі і обробки даних, надійності, швидкодії функціонування не тільки вимірювальних пристроїв, але і засобів передачі даних і обробки вимірювальної інформації.

Управління складними комплексами, котрі висувають високі вимоги до часу виконання завдань здійснюється операційними системами реального часу. Вони забезпечують гарантований час реакції на зовнішні події і мінімальні затримки. Великий інтерес до вивчення таких систем обумовлений широкими можливостями застосування сенсорних мереж, через їх здатності до самоорганізації, автономності та високою відмовостійкістю.

Значна увага приділяється створенню нових космічних апаратів з застосуванням сучасних технологій з урахуванням їх функціонування в умовах реального часу. Незалежно від функцій і призначення, вони отримують механічні пошкодження від космічного пилу та сміття. Згодом, в залежності від безлічі факторів, деталі та комплекси систем космічних апаратів зношуються. Питання постійного моніторингу стану і передбачення відмови модулів є дуже важливою та актуальною задачею, особливо в умовах функціонування модулів у реальному часі. Для вирішення даної проблеми можна задіяти набір датчиків, які є частиною безпроводових сенсорних мереж. Управління функціонування мережею здійснюється за допомогою операційної системи реального часу.

Використання пристроїв безпроводових сенсорних мереж (БСМ), побудованих на технології ZigBee, є доцільним для вирішення цієї задачі. Технологія має власний однойменний стек протоколів, який базується на технології IEEE 802.15.4 і працює з операційною системою реального часу TinyOS, яка функціонує на мікропроцесорах з розрядної сіткою від 8 до 32 біт і оперативною пам'яттю 2 Кбайт і вище. У складі TinyOS є набір функцій API, що дозволяє організувати попередню обробку даних безпосередньо на моті (кінцевому пристрої БСМ, який безпосередньо здійснює збір інформації).

Здатність до самоорганізації та самовідтворення, mesh-топологія, захищеність, висока стійкість, низьке енергоспоживання і відсутність необхідності отримання частотного дозволу роблять ZigBee-мережу відповідною основою для систем позиціонування у реальному часі. Можливості технології ZigBee дозволяють використовувати його безпосередньо на космічних апаратах різного призначення.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Міночкін А.І., Романюк В.А., Жук О.В. Перспективи розвитку сенсорних мереж // Зв'язок. – 2008. – № 1. – С. 16 – 22.
2. Сергиевский М. Беспроводные сенсорные сети // Компьютер Пресс. - М., 2009. - №8. - С. 12-17.
3. Системы реального времени. Виды ОС РВ. Требования к ОС РВ // інтернет-джерело: <http://www.4stud.info/rtos/lecture1.html>

ПРОГНОЗУВАННЯ РОЗГАЛУЖЕНЬ КОНВЕЄРНОГО ПРОЦЕСОРА

Підвищення продуктивності комп'ютерних систем може бути досягнуто як завдяки технологічному розвитку елементної бази так і внаслідок покращення організації роботи процесора. Реалізація концепції конвеєрного процесора стимулювала нові технологічні рішення та суттєво підвищила продуктивність комп'ютерних систем [1, 4].

Архітектура конвеєрних процесорів передбачає паралельне виконання комп'ютерних (машинних) команд, для чого цикл машинної команди розбивається на декілька стадій. Для однієї команди всі її стадії виконуються у часі послідовно, а в цілому для конвеєрного процесора – різні стадії декількох команд виконуються одночасно, створюючи паралельний конвеєр для декількох команд.

Концепція конвеєрного процесора базується на принципі паралельного виконання окремих стадій команд, що мають бути приблизно однакової тривалості і будуть використовувати різні апаратні засоби процесорної частини комп'ютера.

В роботі розглянуті проблеми обґрунтованого вибору сукупності машинних інструкцій та розв'язання типових конфліктів, що виникають в конвеєрних процесорах. Поряд із конфліктами структурними та конфліктами даних потребують прогнозування та розв'язку конфлікти управління конвеєрними процесорами.

Прийняття обґрунтованих рішень прогнозування розгалужень (Branch Prediction) знаходиться в сфері інтересів розробників конвеєрних та суперскалярних процесорів і сьогодні залишається важливою науковою проблемою, що має бути розв'язана на рівні проектування мікроархітектури і суттєво впливає в цілому на пропускну спроможність процесорів.

Необхідність швидкісного та обґрунтованого рішення для обробки умовних розгалужень (переходів) впливає з задачі оптимального завантаження конвеєрного процесора.

Дизайнерами процесорів протягом останніх тридцяти років були запропоновані та імплементовані різноманітні статичні та динамічні методи для прогнозування найбільш вірогідного ходу виконання подальшої послідовності машинних інструкцій після точки розгалуження в програмі.

Мета апаратного блока прогнозування (предиктора) полягає в організації ефективного потоку інструкцій для завантаження конвеєрного процесора з метою досягнення високої продуктивності конвеєрних мікропроцесорних архітектур.

Матеріали містять результати аналізу точності динамічного прогнозування розгалужень в програмі на основі персептрона та прогностичного механізму з використанням моделей Маркова для побудови високопродуктивних архітектур процесорів [2-3].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Babak Salamat, Amirali Baniasadi, Kaveh Jokar Deris, "Area-Aware Optimizations for Resource Constrained Branch Predictors Exploited in Embedded Processors", Embedded Computer Systems: Architectures Modeling and Simulation 2006. IC-SAMOS 2006. International Conference on IEEE, 2006.
2. Elkhoully Reem, El-Mahdy Ahmed, Elmasry Amr, "2-Bit Branch Predictor Modeling Using Markov Model", Procedia Computer Science, vol. 62, pp. 650-653, 2015.
3. Daniel A. Jimenez, Calvin Lin Dynamic Branch Prediction with Perceptrons, in Proceedings of the Seventh International Symposium on High Performance Computer Architecture (HPCA-7) pp. 197-206, Monterrey, NL, Mexico, 2001.
4. A. Patterson, J. L. Hennessy, Computer Organization and Design: The Hardware/Software Interface, Morgan Kaufmann Publishers Inc., 2008.

¹П. М. Павленко, д.т.н.,

¹А. В. Темніков,

²К. Б. Балущок, к.т.н.,

¹Національний авіаційний університет, Київ

²АТ «МоторСіч», Запоріжжя

СИСТЕМА УПРАВЛІННЯ ТЕХНІЧНОЮ ПІДГОТОВКОЮ МАШИНОБУДІВНОГО ПІДПРИЄМСТВА

Однією з найбільш складних і слабо формалізованих задач для підготовки управлінських рішень є етап технічної підготовки виробництва підприємств дискретного типу: авіабудівних, машинобудівних, приладобудівних та інших, як в пострадянських країнах так і в промислово розвинутих країнах світу.

В Національному авіаційному університеті в рамках держбюджетних та господарчих робіт розроблено теоретичні методи управління проектними та виробничими даними та їх практичну реалізацію в вигляді інформаційної системи управління технічною підготовкою машинобудівного виробництва, яка функціонує в інтегрованому інформаційному просторі автоматизованих систем від різних виробників. Коротко розглянемо суть однієї з інформаційних технологій, а саме технології управління ефективністю технічної підготовки виробництва (ТПВ).

Встановлено, що на підприємствах машинобудівної галузі для оцінки якості ТПВ використовується в середньому 40 основних різноманітних показників діяльності підрозділів підприємств. Отримати єдину комплексну оцінку ефективності ТПВ на їх основі та здійснювати моніторинг динаміки їх змін та управління не доцільно.

Базуючись на методології функціонального моделювання та теорії експертних оцінок виділені об'єктні області ТПВ: «продукт», «процес» і «ресурс» та ключові показники оцінки якості кожної з виділених областей ТПВ. Розроблено метод оцінки процесів управління ТПВ. Стан управління системою ТПВ у дискретні моменти часу може бути визначений через оцінку ключових показників діяльності підрозділів, які виконують функції ТПВ. Кожний із ключових показників можна представити рядом дискретних значень у певний момент часу.

У загальному вигляді стан системи ТПВ може бути представлений вектором у просторі Φ_E , який характеризується парою точок. За базову будемо розглядати таку точку, яка характеризує початковий стан системи Φ_{E0} . Стан системи в певний момент часу характеризується точкою Φ_E та є кінцем вектора Φ_E . Величина вектора характеризує рівень ефективності системи ТПВ у даний момент часу.

Суть методу оцінки інформаційних процесів управління ТПВ полягає у встановленні ключових показників процесів ТПВ, та розрахунку цільової функції Φ_E в необхідний момент часу. На прикладі конкретного підприємства побудовані організаційні, інформаційні та процесні моделі управління ТПВ. Використовуючи інструментальні засоби ARIS Simulation проведено імітаційне моделювання процесів ТПВ з оцінкою їх якості. Введено поняття індексу керівництва I_k , та запропонована шестифакторна модель для його розрахунку. Запропоновано моделі розрахунку необхідної кількості фахівців ТПВ. Розроблено метод управління ТПВ, який поєднує запропонований алгоритм та підходи щодо оптимізації ключових показників діяльності та розрахунку ефективності управління ТПВ в рамках її оцінки. Суть методу управління ТПВ полягає в оцінці стану ТПВ у певний момент часу, моніторингу та корегуванню ключових показників інформаційних процесів управління ТПВ, та забезпечення позитивного стану показника ефективності ТПВ (в ході імітаційного моделювання).

Інформаційна система управління ТПВ представлена у вигляді програмних модулів, відповідальних за обробку конкретних даних та здійснення розрахунків та реалізована програмно із застосуванням відповідного інструментального забезпечення.

Створена система реалізує розроблені моделі, методи та відповідне алгоритмічне, інформаційне та програмне забезпечення і забезпечила в процесі промислової апробації на АТ «МоторСіч» (м. Запоріжжя) до 30% зменшенню операційного часу виконання процесів ТПВ.

¹**Н. В. Пащенко,**

²**В. М. Мокійчук, к.т.н.,**

³**О. В. Самойліченко, к.т.н.,**

¹*Національний авіаційний університет, Київ*

²*Національний технічний університет України,*

«КПІ ім. І.Сікорського», Київ

³*ТОВ «НМЦ «Міжнародна школа технічного
законодавства та управління якістю», Київ*

ОЦІНЮВАННЯ РИЗИКІВ ЛАБОРАТОРНИХ КОМП'ЮТЕРНИХ СИСТЕМ ІЗ ЗАСТОСУВАННЯМ МЕТОДУ FMEA

Для підвищення ефективності системи управління, поліпшення результатів та запобігання негативних наслідків та потенційних збоїв, стандарти [1, 2] вказують, що лабораторії у своїй діяльності повинні приймати до уваги ризики та можливості, планувати та реалізовувати заходи з управління ними. Також зазначені стандарти містять вимоги до систем управління інформацією в лабораторії (лабораторних комп'ютерних систем), такі як захищеність від несанкціонованого доступу, втручання і втрат даних, забезпечення точності ведення записів, цілісності даних та інформації, реєстрація збоїв системи та відповідних негайних та коригувальних дій.

Для оцінювання ризиків лабораторних комп'ютерних систем пропонується використовувати метод FMEA (Failure Mode and Effects Analysis – Метод аналізу видів та наслідків відмов). Це метод систематичного аналізу системи для ідентифікації видів потенційних відмов, їх причин і наслідків, а також впливу відмов на функціонування системи (як системи в цілому, так і її компонентів). FMEA-аналіз дозволяє ідентифікувати тяжкість наслідків видів потенційних відмов та забезпечити засоби зі зниження ризиків [3].

Кожен виявлений ризик оцінюється за наступними показниками: тяжкість наслідків (табл.1), ймовірність реалізації та ймовірність виявлення ризику. Показники, в свою чергу, мають кількісну шкалу оцінювання. Для ранжування всіх ризиків за ступенем значущості, для кожного виявленого ризику обчислюється загальне число ризику (Risk Priority Number, RPN) як добуток кількісних

значень показників, за якими оцінювався ризик. Далі за значенням RPN визначається прийнятність ризику – рівень та необхідні дії щодо мінімізації ризику.

Таблиця 1. Тяжкість наслідків

Значення	Найменування	Опис
5	Катастрофічні	Повна втрата даних без можливості відновлення
4	Критичні	Часткова втрата даних з можливістю довготривалого відновлення
3	Середні	Часткова втрата даних з можливістю швидкого відновлення
2	Невеликі	Збої в роботі системи з можливістю швидкого відновлення
1	Незначні	Незначні помилки в системі, які автоматично виправляються

Розглядаючи ризики лабораторних комп'ютерних систем, їх можна поділити на три основні групи – порушення конфіденційності інформації, втрата цілісності інформації, технічні збої в роботі системи. Прикладами таких ризиків є неавторизований та несанкціонований доступ до інформації, розголошення конфіденційних даних, втрата та несанкціоновані зміни даних, внесення хибних даних, відмова комп'ютерного обладнання та ін.

Слід зазначити, що даний метод оцінювання ризиків лабораторних комп'ютерних систем був вибраний через зручність і відносну доступність інтеграції в систему управління якістю лабораторії.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. ДСТУ ISO/IEC 17025:2017 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій. – ISO, 2017. — 30 с.
2. ДСТУ ISO 15189:2015 Медичні лабораторії. Вимоги до якості та компетентності. – К.: ДП «УкрНДНЦ, 2015. — 46 с.
3. IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA). – IEC, 2018. – 165 с.

СУМІСНІ РОЗПОДІЛИ ДЕЯКИХ СТАТИСТИК ВИПАДКОВИХ БІТОВИХ ВЕКТОРІВ

Випадкові числа використовуються давно та в багатьох сферах. Перерахуємо деякі галузі їх застосування:

1. Криптографія та інформаційна безпека.
2. Оптимізація функціональних залежностей.
3. Прийняття рішень в автоматизованих експертних системах.
4. Розваги та ігри.
5. Хімічна промисловість.

І скрізь постає питання: що таке «істинно» випадкове число, якою має бути послідовність випадкових чисел, яким може бути розподіл випадкових чисел на деякому інтервалі[1].

Для виявлення закономірностей до випадкових або псевдовипадкових послідовностей (ВП або ПВП), які аналізуються, застосовують широкий спектр різних статистичних тестів, розроблених в останні десятиліття.

Незважаючи на чималу кількість існуючих реалізацій статистичних тестів ПВП, даний напрямок постійно розвивається. Аналіз існуючих пакетів [2] для статистичного тестування призводить до висновку, що багато тестів можуть успішно використовуватися для дослідження ПВП на випадковість за умови довжини послідовності понад 10^6 біт. Разом з тим, особливості прикладних задач показують, що класична математична модель статистичного тестування не цілком адекватно відображає потреби в дослідженні послідовностей довжиною до 100 біт на випадковість.

В роботі запропоновано критерій для перевірки (0, 1) - послідовностей невеликої довжини (до 100 біт), які названі бітовими векторами.

Опишемо відповідну математичну модель. Дано

де $y_i = \{0, 1\}$, $i = 1, 2, \dots, n$, $n > 0$.

Підпослідовність $y_j, y_{j+1}, \dots, y_{j+s-1}$ послідовності (1) називається s-ланцюжком, $j = 1, 2, \dots, n-s+1$, $s = 1, 2, \dots, n$.

Позначимо $\eta(t_1, t_2, \dots, t_s)$ число s -ланцюжків в послідовності (1), які співпадають з $t_1, t_2, \dots, t_s$, де $t_i = \{0, 1\}$, $i = 1, 2, \dots, s$.

Умова (У): послідовність (1) складається з n , $n > 0$, незалежних однаково розподілених випадкових величин; $P\{Y_i = 1\} = p$, $P\{Y_i = 0\} = q$, $p + q = 1$, $i = 1, 2, \dots, n$.

Твердження. Нехай виконуються умова (У), k_1, k_2, k_3, t, t_1 – цілі числа такі, що $k_1 \geq 0, k_2 \geq 0, n \geq k_1, k_3 \geq 0, t, t_1 \in \{0, 1\}$. Тоді $P\{\eta(t, t^*) = k_1, \eta(t_1 t^*) + \eta(t_0 t^*) = k_2\} = \sum_{m_1=k}^{n-k_1} p^{m_1} q^{m_0} \times$

$$\sum_{i=0}^1 C_{k_1}^{\delta_i} C_{m_1-k_1}^{k_2-\delta_i}$$

, де $m_0 = n - m_1$, символ $\sum$ позначає сумування по усім невід'ємним числам δ_0 та δ_1 таким, що $\delta_0 + \delta_1 = 2k_1 - k_2$, $t^* \stackrel{\text{def}}{=} 1 - t$.

Проілюструємо (рис. 1) використання твердження для малої вибірки n , $n = 20$, і деяких значень k_1 та k_2 .

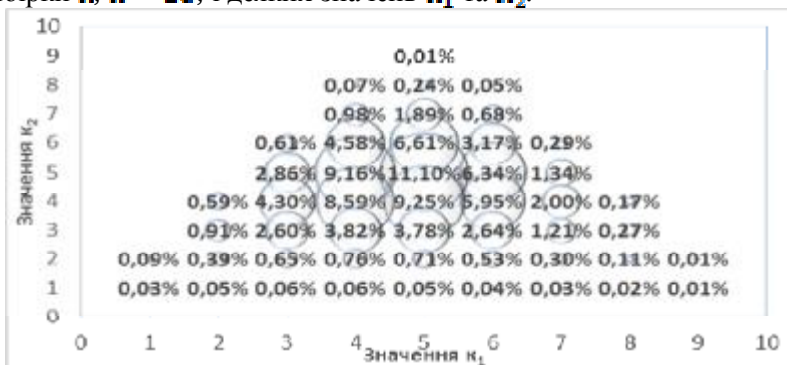


Рис.1. Розподіл ймовірностей зазначеної події в залежності від k_1 та k_2 .

На рис. 1 представлено бульбашкову діаграму, в якій перший параметр (горизонтальна вісь) – значення k_1 , другий (вертикальна вісь) – значення k_2 , третій (розмір бульбашки) – ймовірність події $\{\eta(t, t^*) = k_1, \eta(t_1 t^*) + \eta(t_0 t^*) = k_2\}$, яка подана в відсотках.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Слеповичев И.И. Генератор псевдовыпадных чисел. Учебное пособие – 2017. – 118 с.
2. А.М. Коренева, В.М. Фомичёв. Статистическое тестирование псевдослучайных последовательностей // Безопасность информационных технологий. - № 2 - 2016.

M. M. Protsenko, associate professor,
M. M. Guzii, associate professor
National Aviation University, Kyiv

SD-WAN TECHNOLOGY PROSPECTS

Recently, there has been an interest in technologies of corporate global networks, whose principles were developed in 2006 by specialists from the Universities of Stanford and California (Berkeley). According to the aspects of use, they are divided into three groups but have a common name: Software Defined Network (SDN).

One of SDN is SD-WAN technology, developed in 2012. The term “software defined” in the name of technologies reflects their essence: the network flows are controlled automatically by special software that implements intelligent control algorithms. As it is known, the traditional way to manage a network implies configuring the network equipment in manual mode by the network administrator.

SD-WAN technology is aimed at using in global networks of large companies with a range of territorially separate units. For them, effective data flow management is considered to be essential. SD-WAN provides:

- dynamic routing of traffic, directing it through the cheapest and least-loaded channels without losing the speed and efficiency of user applications;
- configuring connections in real time, which allows you to refuse expensive network VPN channels;
- required encryption level of transported information.

The SD-WAN contains a central device called a controller, which independently and automatically controls the access devices of remote offices to the corporate network. The controller provides a centralized adjustment of the current configuration of the equipment for accessing remote offices networks by using configuration templates, tracking the current network status, channel congestion, as well as promptly detecting and responding to failures in communication channels.

In fact, SD-WAN uses cloud technologies and cloud software. Software virtualization simplifies the network service management by abstracting the high-level functionality.

The technology allows reducing the total cost of network bandwidth. Moreover, it is actively introduced into computer networks in the USA

and Western Europe. Prospects for this technology are noted by analytical companies, in particular, Gartner predicts SD-WAN rapid growth during the next two years.

A significant advantage of SD-WAN is the ease of installation, which makes it attractive for separate units with a small staff. The market offers “boxed” options for supplying the SD-WAN equipment with installation manuals designed for an IT specialist with ordinary technical skills.

After installation and connection to the network, the device independently communicates with the controller, receives all configuration changes, and the office network becomes a component of the company's secure network.

According to open source data, the compound annual growth rate (CAGR) in SDN segment for the next five years (starting from 2018) will achieve 32%, and the total market volume will increase from \$ 7 billion in 2015, up to \$ 28 billion in 2020.

The catalyst for the growth of the SDN market will primarily be the creation of new SD-WAN networks, as well as the deployment of SDN-based services. According to analysts, 58.5% of enterprises around the world are planning to launch SD-WAN in the next couple of years.

In conclusion, the advantages of SD-WAN, which contribute to the commercial success of this promising technology, should be emphasized:

- SD-WAN provides centralized traffic management, which can be adapted to your needs;
- SD-WAN, having a cloud-optimized architecture, provides access to cloud-based applications and an automated control mode for network devices;
- companies can implement SD-WAN technology without making changes to existing networks since it is compatible with such transport technologies as Ethernet, MPLS, Wi-Fi, 3G, LTE, etc.;
- SD-WAN networks are characterized by high performance, low cost and higher reliability compared to traditional ways of creating corporate WANs with one security source.

ВИКОРИСТАННЯ МЕРЕЖЕВОГО RTSP - ПРОТОКОЛУ В СИСТЕМАХ, ЩО ПРАЦЮЮТЬ З МУЛЬТИМЕДІА ДАНИМИ

Потоковий протокол реального часу RTSP (Real Time Streaming Protocol) – мережевий протокол, розроблений IETF в 1998 році, є прикладним протоколом, що дозволяє клієнтові віддалено управляти потоком мультимедійних даних [1].

Список команд (методів):

- OPTIONS - запит підтримуваних методів;
- DESCRIBE-запит опису контенту, наприклад, у форматі SDP;
- PLAY - запит початку мовлення контенту;
- PAUSE - запит тимчасової зупинки мовлення;
- RECORD - запит на записування контенту сервером;
- REDIRECT – переорієнтація на інший контент;
- SETUP - запит установки транспортного механізму для медіа;
- ANNOUNCE - оновлення даних опису контенту;
- GET_PARAMETER - запит вказаних параметрів в сервера;
- SET_PARAMETER - установка параметрів сервера;
- TEARDOWN - зупинка потоку і звільнення ресурсів.

Протокол призначений для використання в комунікаційних системах для управління поточковим сервером, для встановлення та управління сеансами мультимедіа між кінцевими точками. Клієнти медіа серверів використовують VCR подібні команди, такі як PLAY та PAUSE, щоб полегшити управління в реальному часі програванням медіа файлів з сервера.

Більшість серверів RTSP використовують RTP у поєднанні з RTCP для доставки медіа потоку, проте деякі виробники реалізують власні транспортні протоколи, наприклад, серверне програмне забезпечення RTSP використовує протокол RDT.

RTSP з використанням RTP і RTCP дозволяє здійснення адаптації швидкості передавання.

На рис. 1 наведені подібності та різниця між HTTP та RTSP в управлінні відтворенням мультимедійного контенту.

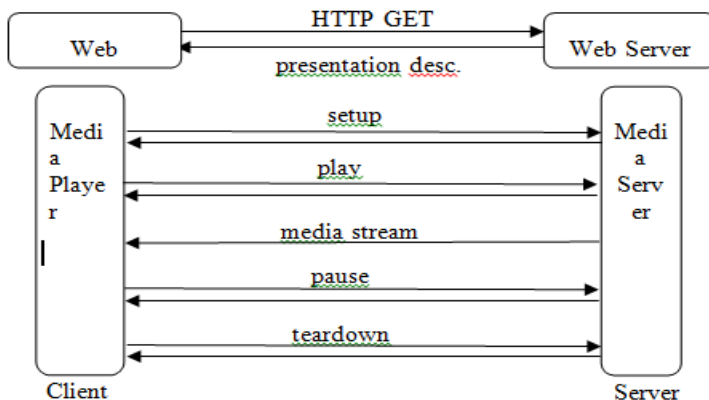


Рис.1 Функціональна взаємодія RTSP на рівні клієнт-сервер

Задачі, які може вирішувати RTSP-протокол:

- підключення до хмарного сховища;
- трансляція за допомогою плеєра;
- онлайн трансляція відео на сайт;
- додавання камери в додатки на Android і iOS;
- налаштування відео реєстраторів.

RTSP працює спільно з протоколами нижнього рівня, такими, як RTP, RSVP, IP і TCP /UDP.

Унікальною властивістю протоколу RTSP є те, що він надає користувачеві можливість керування процесом доставки поточкових даних по мережах з комутацією пакетів, перегляд за запитом кінофільмів з різних фільмотек, відеофайлів і іншого мультимедійного контенту.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Matthew Syme, Philip Goldie. Optimizing Network Performance with Content Switching: Server, Firewall and Cache Load Balancing. Prentice Hall, New Jersey 2003. – 288 p.

А. Т. Рахманов к.т.н.,
Р. Х. Хамдамов, д.т.н.,
К. Ф. Керимов, к.т.н.
Ш. К. Камалов

*Ташкентский университет информационных технологий имени
Мухаммада аль-Хорезми, Ташкент*

АЛГОРИТМ АВТОМАТИЧЕСКОГО ОБНАРУЖЕНИЯ УЯЗВИМОСТИ ВИДА SQL ИНЪЕКЦИИ

Атаки на веб-приложения являются относительно новым видом атак. Если в веб-приложении не осуществляется фильтрация входящих параметров должным образом, то злоумышленники могут получить возможность фальсифицировать базу данных, используя форму на веб-странице либо изменяя другие входящие данные.

В работе предлагается математический способ идентификации атак SQL инъекций с помощью ограниченной снизу функции, которая зависит от входной строки. Для построения такой функции использованы специальные знаки и ключевые слова, которые часто встречаются в построении атак злоумышленников.

В предлагаемом методе, мы можем обнаруживать атаки по инъекции SQL, используя один символ. Тем не менее, экспериментально показано, что предлагаемый метод обнаружения с использованием набора многочисленных символов позволяет более точно определить уязвимость вида SQL инъекция.

Таблица 1

Переменная	Символ
u_1	Пробел
u_2	Точка-запятая(,)
u_3	Апостроф(')
u_4	Правая скобка())
u_5	Левая скобка(

Для определения SQL инъекции вводим характеристики атак SQL инъекций с помощью специальных символов из таблицы 1 и специальных ключевых слов из таблицы 2. Пусть наблюдается некоторая входная строка L и пусть $x_1, x_2, \dots, x_{20}$ частота

появления в L специальных знаков из таблицы 1 и пусть $x_{21}, x_{22}, \dots, x_{30}$ являются частотой появления специальных ключевых слов из таблицы 2, x_{31} частота появления всех остальных знаков и чисел 0,1,2,...,9 в строке L . С точки зрения определения атак SQL инъекций обычные символы $a, b, \dots, z$ и числа 0, 1, ..., 9 не играют важную роль. По этому в данной работе мы всегда считаем что частота появления всех этих символов и чисел в наблюдаемой строке L равно 1, т.е. $x_{31} = 1$. Таким образом, любую строку L можно определить с помощью характеристик следующим образом:
 $L = (x_1, x_2, \dots, x_{20}, x_{21}, \dots, x_{30}, x_{31})$, как элемент некоторого фазового пространства X .

Таблица 2

Переменная	Ключевые слова
u_{21}	and
u_{22}	or
u_{23}	union
u_{24}	where
u_{25}	limit

В предлагаемом методе создан набор символов, который сочетается как с атакой, так и с нормальными обнаружениями, и с ранее известным порогом, используя примерные данные атакующих и нормальных строк. Согласно экспериментам с искусственными данными, набор содержит пробел, точку с запятой, и правая скобка хорошо зарекомендовала себя для большего диапазона веса для атаки и нормальной строки.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Козлов Д.Д., Петухов А.А. Методы обнаружения уязвимостей в web-приложениях. // Программные системы и инструменты, 2006. - № 7. - С. 156-166.

O. V. Rusanova, assistant professor

A. V. Korochkin, assistant professor

O. P. Shevelo, assistant

NTUU “Igor Sikorsky Kyiv Politechnical Institute”, Kyiv

CLASSIFICATION OF SCHEDULING PROBLEMS FOR MODERN PARALLEL COMPUTER SYSTEMS

This paper is dedicated to the classification of scheduling problems for all types high performance computers. It's known that scheduling is one of the important factors in increasing real performance of parallel computer systems. Scheduling belongs to *NP*-complete class problems. Therefore most of researches concentrate their activity on different scheduling heuristics.

There are many classifications of scheduling problems, for example in paper [1], but most of them don't take into account all features of modern high performance computers.

In this work firstly we consider the main characteristics of modern parallel computer systems such as: great core number; multi-core architecture of nodes; different system topologies that support interconnection switches (*Gigabit Ethernet*, *Infiniband* etc); heterogeneity (for example, *CPU+GPU* platform) .

It's known that initial data for scheduling problem are: computer system architecture, application characteristics and optimization criteria.

We analyses various last works [2],[3] and propose different kinds of computer system architectures in our classification, such as:

- § single multi-core CPU;
- § single multi-core CPU+GPU;
- § set of single-core CPU;
- § set of multi-core CPU;
- § set of multi-core CPU+GPU;
- § size of memory, cache, i/o unit characteristics for given CPU;
- § topology type for CPU (computer system nodes) set (fully-connected or implete topologies).

We consider also different kinds of application characteristics for scheduling problems, such as:

- § single application with their labuor intensity and initializing time;

- § sequence of the same or different independent applications with their labor intensity and initializing time;
- § single application presented in the form of *directed acyclic graph (DAG)* ;
- § set of independent applications presented in *DAG* ;
- § set of applications presented in *DAG* with dependencies (two level hierarchical *DAG*)

We analyze kinds of computer systems architectures and applications characteristics that can be used for dynamic and static scheduling.

In paper we consider the main optimization criteria for scheduling problems, such as:

- § minimal run time of application with the given computer system cost;
- § minimal cost of computer system with the given application run time;
- § minimal application run time that provided by computer system with minimal cost.

We analyze also cases in which each of these criteria is used.

All results this paper can be used for improvement of scheduling methods in modern high performance computers.

REFERENCES

1. 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.- 55 p.
2. Русанова О. В. Спосіб планування обчислень для мультитядерних кластерів/ О.В. Русанова// Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. наук. пр. – К.: Век+, - 2016. – No 64. – С. 31-37.
3. Hongyang Sun, Redouane Elghazi, Ana Gainaru, Guillaume Aupy, Padma Raghavan. Scheduling Parallel Tasks under Multiple Resources: List Scheduling vs. Pack Scheduling. RR-9140, Inria Bordeaux Sud-Ouest. 2018. - 33 p.

С. В. Сімченко, к.ф.-м.н.,
О. С. Таратонova
Відділ науково-технічної освіти ЦДЮТ
ім. Є.М.Руднєвої, Бердянськ

ДІОДНІ ПРИЙМАЧІ З НАНОТЕКСТУРОВАНИМ ПОКРИТТЯМ ДЛЯ ОПТОВОЛОКОННИХ ЛІНІЙ ЗВ'ЯЗКУ

Передача цифрових сигналів по оптоволоконних лініях зв'язку, є актуальною на даний момент. З розвитком цифрових технологій та комп'ютерних потужностей передача сигналу через лінії зв'язку на коаксимальному (мідному) кабелі або по радіоканалу вже не здатна забезпечити необхідної швидкості та якості сигналу. Також вказані вище способи мають ряд інших технічних недоліків: на сигнал в значній мірі впливають зовнішні наводки, відбувається електромагнітне забруднення навколишнього середовища, ці способи є малоефективними при передачі сигналу на великі відстані.

Останнім часом, як альтернативу якісної передачі сигналу використовують оптоволоконні цифрові лінії. Такі лінії – не чутливі до дії зовнішніх наводок та мають низькі втрати при передачі сигналу на великі відстані [1]. Оптичні лінії зв'язку по вартості конкурують з коаксимальними та дозволяють обмінюватись інформацію з рекордною швидкістю ~ 1.5 Терабіт/с. В якості передавача та приймача сигналу в оптоволоконних лініях використовують світло- та фотодіоди. Покращення електрофізичних параметрів та мініатюризація розмірів квантових передавачів та приймачів для оптоволоконних ліній є дуже важливим завданням.

Нами досліджено покращення характеристик фотодіода завдяки створенню на його «активній» поверхні нанотекстурованого шару. В дослідженні ми використовували кремнієві фотодіоди (стандартні зразки сонячних елементів). Порувату поверхню отримували методом електрохімічного травлення. Травлення відбувалось в розробленій нами фторопластовій комірці оригінальної конструкції з платиновим кільцевим електродом. З використанням багатоканального АЦП в процесі роботи контролювали та фіксували час, струмову кінетику травлення,

напругу, температуру електроліту. Електрохімічне травлення проводили тільки фронтальної поверхні фотодіода. На зразках з текстурованою поверхнею спостерігається зменшення коефіцієнта відбиття, що свідчить про збільшення ККД перетворення таким фотоелементом. Також на виготовлених фотодіодах знімалися вольт-амперні характеристики (ВАХ). На рис. 1. представлені ВАХ для елементів з поруватим шаром (2) товщиною 80 нм (пористість 55 %) і без поруватого шару (1). ВАХ досліджені для зразків площею поверхні 81 мм^2 при інтенсивності випромінювання 10 Вт/м^2 і температурі 300К .

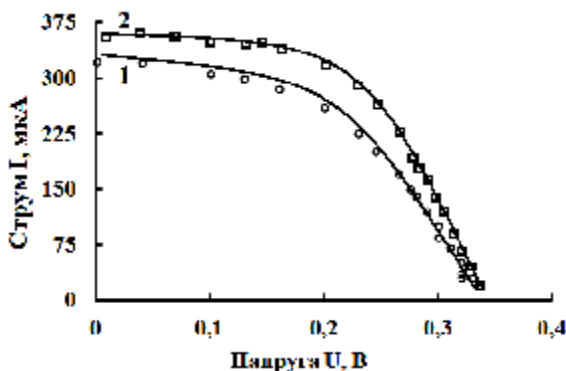


Рис. 1. Вольт-амперні характеристики сонячних елементів з поруватим шаром (2) та без поруватого шару (1) $T=25^{\circ}\text{C}$

Як видно з рисунка, значення струму короткого замикання в фотодіодах з поруватим шаром збільшується $\sim$ на 2-3 % порівняно з монокристалічним зразком таких же розмірів. Напруга холостого ходу для обох зразків майже не змінюється.

Поліпшення параметрів фотодіодів можна пояснити збільшенням активної площі поверхні поруватого шару. Це дозволяє зменшити втрати світла на відбиття та збільшити фотогенерацію додаткових носіїв заряду у сформованому поруватому шарі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Волоконно-оптические системы передачи и кабели. Справочник. Под ред. Гроднева И.И., Мурадяна А.Г., Шарафутдинова Р.М. и др.; М.: Радио и связь, 1993.

Yu. Sinko, Candidate of pedagogic sciences
National Aviation University, Kyiv

THE USE OF CLOUD COMPUTING IN HIGHER EDUCATION INSTITUTIONS

Today, without the use of modern information technology, no educational institution can work effectively. At the same time, the maintenance and development of its own IT infrastructure at each educational center is very expensive. Every year the level of such expenses is growing significantly. Institutions spend large sums on computer equipment, telecommunications equipment and software. In addition to the above costs, significant financial investments are needed to maintain a high level of professionalism of these employees.

Cloud computing is a good alternative to the classical learning model. Its main advantage can be considered a significant savings in the educational institution in which they are used. Indeed, in this case, the computer infrastructure and / or information services are provided as services of the "cloud" provider. Documents, emails, programs and other data of participants in the educational process are stored on remote servers of the provider. At the same time, an institution does not need to maintain its own expensive IT infrastructure and overpay for computing resources, which in most cases are not used at full capacity. The only thing is needed for teachers and students to provide using cloud technologies is access to the Internet.

Today there are many providers of cloud solutions. Such large companies as Amazon, Google, Microsoft and others offer significant discounts to educational institutions, due to which they get access to cloud services free of charge.

Reliability, availability and ease of distribution are key advantages of cloud technologies. Can all this mean that soon most educational services will be provided based on cloud computing? Will this lead to the complete rejection of educational institutions from their own bulky IT infrastructures?

Therefore, there is a need to set a goal to review and evaluate all the advantages and disadvantages of using cloud computing in the field of education, as well as to give practical recommendations on the use of

cloud computing in the learning process both at school and in higher education institutions.

One of the first cloud services that European educational institutions began to use was e-mail. Ensuring the efficiency (outsourcing) of the e-mail service is not a difficult task, as it definitely does not play a key role in the work of an educational institution. Corporations Google and Microsoft provide employees and students of educational institutions access to e-mail free of charge.

In addition to e-mail services, these corporations provide the ability to use in the cloud the functions of a standard office suite for collaboration with electronic documents, spreadsheets and for creating presentations. Cloud services for educational organizations Google Apps for Education and Microsoft Office 365 for education allow you to use embedded systems for instant messaging, calendars for collaborative planning, and general address books. Each cloud user receives significant disk space to store any information that was obtained as a result of working with the cloud.

It may seem strange that these services are provided to educational institutions free of charge, while for commercial organizations the prices for software both were and remain traditionally high. This pricing policy is explained as follows. In today's cloud market, there is high competition among software vendors, so they are trying to provide their services to educational institutions free of charge. The calculation goes to the future graduates who, after receiving an education, will get a job and will be able to convince the future employers to purchase a software product, the benefits of which they already know. It will also ensure the commitment and loyalty of users to products of a certain brand and its recognition and popularity.

If for an educational institution the danger of data access is not a priority, then it may be beneficial to use low-level IaaS services as data storage systems, for example, for video and audio materials.

For some educational institutions, it may be beneficial to move to the cloud of internal learning management systems (LMS, Learning Management Systems). This is a good opportunity for institutions that cannot afford to purchase and maintain expensive equipment and software, and allows you to optimize the cost of IT-infrastructure in the current post-crisis conditions.

И. Е. Терентьева, к.т.н.

В. В. Уланский, д.т.н.,

И. А. Мачалин, д.т.н.,

Национальный авиационный университет, Киев

ИССЛЕДОВАНИЕ УРОВНЯ ДОСТУПНОСТИ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ МЕТОДА МОНТЕ-КАРЛО

Компьютерные и телекоммуникационные сети нового поколения состоят из большого числа отдельных устройств (контроллеров, шлюзов, серверов и т.д.). Поскольку для работы всей сети необходима совместная работа отдельных устройств, то от надежности оборудования зависит доступность всей сети.

В настоящее время к доступности сетей предъявляются высокие требования [1], желательное время простоя сети должно составлять не более 5 минут за год, что соответствует уровню доступности 0,99999. Обеспечить такой уровень можно только резервированием аппаратных и программных средств. Однако, для того чтобы оценить кратность и виды резервирования, необходимо иметь математические модели для оценки основного показателя доступности – коэффициента готовности. Авторами в работе [2] получены аналитические модели, позволяющие оценить этот показатель, но рассчитать его можно только при наличии исходных данных, которые не всегда можно получить на практике, особенно в начальный период эксплуатации. Поэтому авторами предложена имитационная модель, позволяющая методом Монте-Карло получить статистические оценки коэффициента готовности (уровня доступности).

Исходными данными для имитационного моделирования являются следующие параметры: интенсивность явных отказов; интенсивность скрытых отказов; интенсивность перемежающихся отказов; время восстановления после явного отказа; время восстановления после перемежающегося отказа; полнота контроля; количество реализаций случайного процесса – 100 итераций; длительность одной итерации – длительность одного цикла – 1000000 ч;

Длительность и количество итераций выбраны с учетом бесконечного интервала наблюдения за случайным процессом

технической эксплуатации сети. Обобщенный алгоритм имитационного моделирования случайного процесса следующий:

Шаг 1. Ввод исходных данных. Шаг 2. Вычисление интенсивностей отказов. Шаг 3. Генерирование случайных чисел и формирование потока явных, скрытых и перемежающихся отказов. Шаг 4. Имитация времени восстановления после явного и перемежающихся отказов. Шаг 5. Обработка случайных событий и вычисление коэффициента готовности. Шаг 6. Вывод и отображение результатов.

В табл. 1 представлены результаты имитационного моделирования и значения среднего времени нахождения модулей в состояниях работоспособности, неработоспособности и восстановления, а также коэффициента готовности, рассчитанные по аналитическим формулам.

Таблица 1

№	$M(T_1)$	$M(T_2)$	$M(T_3)$	$M(T_4)$	КГ
1.	9799,07	70,3242	0,88	0,05	0,970990
2.	9794,713	204,206	1,04	0,04	0,979477

98.	9888,443	110,501	1,008	0,046	0,988844
99.	9889,560	109,385	1,007	0,047	0,988956
100.	9890,654	109,291	1,009	0,053	0,989965
Теор.	9894,444	110,365	1,0944	0,055	0,990562

Как видно из таблицы, результаты моделирования дают высокую степень схождения статистических и аналитических результатов, относительное отклонение не превышает 3%. Предложенный метод может быть полезен при проектировании компьютерных и телекоммуникационных сетей для оценки уровня доступности сетей.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Документ SP-3-0092: (Стандарт TIA-942, редакция 7.0, февраль 2005). – NY, 230 с.
2. Ulansky V., Terentyeva I. Availability modeling of a digital electronic system with intermittent failures and continuous testing. Engineering Letters. – 2017. – V. 25, № 2. – P. 104-111.

ОСНОВНІ ПІДХОДИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному суспільстві перед кожним підприємством електроенергетики, постає питання про організацію системи захисту інформації, яка б дозволила у повній мірі забезпечити безпеку функціонування інформаційно-телекомунікаційної системи (ІТС). Ефективність захисту інформації залежить від підходу до її організації та правильного вибору методів оцінки ризиків інформаційної безпеки.

З розвитком ІТС гостро постає проблема забезпечення інформаційної безпеки та технічного захисту інформаційних ресурсів в автоматизованих системах (АС). Одним з важливих організаційних заходів захисту інформації в АС є визначення переліку загроз інформації, які порушують її властивості – конфіденційність, цілісність та доступність. Перелік загроз, у свою чергу, пов'язаний з уразливістю таких систем. Ці два фундаментальні поняття лежать в основі теорії оцінювання ризиків як одного з найважливіших етапів побудови підсистеми захисту інформації.

Визначення терміну «інформаційна безпека» (ІБ) у більш вузькому значенні має характер процесу забезпечення конфіденційності, цілісності та доступності. Існує досить великий клас систем обробки інформації, під час розробки яких фактор безпеки відіграє першорядну роль (наприклад, енергетичні, банківські, інформаційні, медичні, економічні та лінгвістичні системи). Одним з важливих організаційних заходів захисту інформації в АС є визначення переліку загроз інформації, які порушують її властивості – конфіденційність, цілісність та доступність. Одна або декілька загроз можуть використовувати ряд уразливостей інформації. Будь-яка зміна загроз та уразливостей може мати значний вплив на ІБ. Раннє виявлення або знання про ці зміни збільшує можливості щодо прийняття необхідних заходів для обробки ризику та забезпечення безпеки ІТС у цілому. Це

досягається за рахунок інструментальних методів визначення ризиків інформаційної безпеки в ІТС.

Питання аналізу ризиків інформаційної безпеки висвітлені у наукових працях та інформаційно-довідкових матеріалах. Проблемами дослідження інформаційної безпеки в ІТС займаються як вітчизняні вчені (Мохор В.В., Винничук С.Д., Гончар С.Ф., Горбенко І.Д., Домарев В.В., Корченко О.Г., Юдін О.К., Бучик С.С.), так і зарубіжні (Астахов А.М., Daniel Wentre, Thomas R., Whitman M.).

Відповідно до стандартів ISO/IEC 27005 та ISO/IEC TR 13335-2 оцінювання ризиків включає такі етапи:

1. Оцінку ймовірності можливих загроз і уразливостей.
2. Розрахунок ступеню впливу, який може мати загрозу на кожен актив.
3. Визначення кількісної (вимірної) або якісної (описуваної) вартості ризику.

Оцінювання ризиків полягає у визначенні кількісних та якісних показників, формуванні реєстру ризиків та ранжируванні ризиків.

Більш поширені способи оцінки інформаційних ризиків використовують змішані методи оцінки, які включають кількісні та якісні показники.

Як показує огляд інформаційних джерел, у галузі оцінки та управління інформаційними ризиками в ІТС на даний момент переважають інструментальні засоби їх оцінки такі, як CRAMM, Risk Watch, ГРИФ 2006, NIST, COBRA, OCTAVE.

ВИКОРИСТАНІ ДЖЕРЕЛ

1. Юдін О.К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О.К.Юдін, С.С.Бучик. – К.: НАУ, 2015. – 213 с.
2. Корнієнко Б.Я. Прикладні програми управління інформаційними ризиками / Б.Я.Корнієнко, Ю.О.Максімов, Н.М.Марутовська // Захист інформації. — К. : Науково-практичний журнал, 2012. – Вип. 4. – С. 60–64.
3. Бучик С.С. Методика оцінювання інформаційних ризиків в автоматизованій системі / С.С.Бучик, С.В.Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. — Житомир: ЖВІ ДУТ, 2015. – Вип. 11. – С. 33–43.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСІ РОЗРОБКИ ПРИКЛАДНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Штучний інтелект прогресує з неймовірною швидкістю, разом з цим змінюється статистика промисловості і всіх галузей, так чи інакше пов'язаних з поняттям штучного інтелекту.

Вдосконалення процесу розробки прикладного програмного забезпечення (ППЗ) з застосуванням штучного інтелекту є актуальною задачею. У процесі розробки ППЗ розробники можуть звертатися до екосистеми готових розробок, отримуючи готові блоки і інструментарій для інтеграції функціоналу штучного інтелекту в розроблювані рішення. Але є ще один рівень можливостей при розробці ППЗ, який обумовлений можливістю застосування штучного інтелекту до самого процесу розробки, зокрема, для автоматизації різних функцій інтелектуального аналізу даних, розробки і тестування додатків.

При розробці ППЗ доцільно використовувати набір рекомендованих шаблонів до конкретного ППЗ. Виявлення цих шаблонів та їх використання у процесі розробки ППЗ з застосуванням штучного інтелекту може бути більш глибоким для ідентифікації та класифікації типів помилок. Для цього необхідно використати алгоритм поглибленого навчання, який може позначати відомі помилки і прискорювати процес налагодження розробленого ППЗ. Після достатнього рівня навчання ЕВМ зможе автоматично виконати налагодження, тобто виправити широкий спектр помилок. У випадку коли спосіб вивчення алгоритму повністю непрозорий для зовнішнього спостерігача, тобто має ефект чорного ящика, то єдиний спосіб взаємодіяти з алгоритмом полягає в наданні підготовлених наборів даних і аналізувати вихідні результати, тобто реакції. Але слід звернути увагу, що цей спосіб не є досить ефективним, коли йдеться про тонке налаштування. Використання цього способу може призвести до не прогнозованих результатів.

Наявність розумного помічника прискорює процес розробки і допомагає дізнатися особливості розробки та функціонування конкретного ППЗ набагато швидше, ніж через спроби та помилки. Штучний інтелект може виступати в ролі тренера і виносити рекомендації, пропонувати приклади коду, запобігати простим помилкам програмування.

Використання штучного інтелекту дає можливість виконувати функцію автоматизації генерації коду. Система штучного інтелекту може генерувати код, комбінуючи разом деякі наперед визначені модулі. Це важлива функція для використання її в структурі само-програмованих ЕВМ.

Система штучного інтелекту дозволяє виконати автоматизацію тестування. Одним із завдань тестування програмного забезпечення є створення всеохоплюючого списку, який включає ймовірні випадки, а також деякі екстремальні ситуації, які можуть мати значний вплив на продуктивність програми. Система штучного інтелекту може зробити це, переглянувши попередні журнали і генеруючи список тестів автоматично для запуску через систему. Вона може передбачати результати тестування, навіть не виконуючи фактичні тести, і зосередитися лише на тих проблемах, які можуть бути проблематичними, що заощадить час [1-4].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. (<https://www.juniperresearch.com/researchstore/fintech-payments/ai-in-retail>)
2. Онлайн видання Jaxenter (jaxenter.com/ai-change-development-processes148462.html).
- 3.Онлайн видання PacktHub (hub.packtpub.com/5-ways-artificial-intelligence-is-upgrading-software-engineering/).
4. (<https://robo-sapiens.ru/stati/oblasti-primeneniya-iskusstvennogo-intellekta/>)

N. B. Fomina, assistant professor of CSN Department
National Aviation University, Kyiv

NEURAL NETWORKS AND UNIVERSITY EDUCATIONAL PROCESS FORECASTING

Despite the increased in recent years, attention to the full range of issues that are associated with forecasting and long-term planning in the field of education, both in our country and abroad. Predominant attention of researchers is attracted by quantitative indicators: forecasting the quantitative growth of educational institutions various types, the number of students in them, the definition of prospective personnel needs of skilled workers and specialists of a particular profile, etc. [1].

The advanced information, which was obtained as a result of prognostic research, acts as a tool that allows not only to foresee possible changes in the organization, structure and content of educational activities in the distant future, but also to go in practice to the predicted working conditions of educational institutions. It allows you to make the necessary adjustments to the daily educational process, and the results of prognostic studies to consider in terms of operational restructuring of the modern educational institutions, taking into account the natural trends identified in the forecasting process.

Forecasting is an assessment, a prediction, a prediction of the future development of a selected management object. It must precede planning. The main goal of forecasting is the scientific prerequisites forming for a management decisions making.

With the accelerated development of scientific and technological progress and the growing trends of globalization, uncertainty about the future behaviour of management objects increases sharply, the cost of managerial decisions errors increases. Therefore, the role of forecasting in the XXI century. fundamentally increasing.

The purpose of forecasting is to reduce risk in decision making. Also the choice of forecasting method is very important, which depends on the task set according to its fallacy degree, taking into account the influence of various factors.

Neural networks are an extremely powerful simulation method that allows you to reproduce extremely complex dependencies [2]. In particular, neural networks are non-linear in nature.

An artificial neural network (ANN) is a set of neurons that are interconnected [3]. Generally, transfer functions of neurons in the neural network are fixed, and the weight is neural network parameters and may vary.

Neural networks are not programmed in the usual sense of the word, they are learning. Ability to study is one of the main advantages of neural networks in the traditional algorithms.

Considering the types of direct-propagation neural networks, it is expedient to designate a system for forecasting the educational process to choose recurrent neural networks (RNNs), which, unlike neural networks of direct distribution, can use their internal memory for arbitrary input sequences handling.

Currently, there are various applications and programming languages that are used to develop forecasting systems using NM. The selected Python language with the Matplotlib application is a full competitor of MATLAB or Mathematica.

The library is low-level, which means a large amount of code for the extended visualization. But productivity and work with the usual language allow you to close your eyes to this disadvantage.

ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ивахненко А. Г. Долгосрочное прогнозирование и управление сложными системами. – К.: Техника, 1975. - 311 с.
2. Барский А.Б. Обучение нейросети методом трассировки. [Труды VIII Всероссийской конференции «Нейрокомпьютеры и их применение»: Сборник докладов.] / А.Б. Барский – 2002. – С. 862-898.
3. Битачевский Е.А. Использование нейронных сетей для распознавания визуальных образов [Материалы IV РНТ конференции «Вузовская наука Северо-Кавказского региона»: Сборник докладов.] / Е.А. Битачевский, В.В. Козуб. – 2000. – С. 52-54.

ДИСТАНЦИОННЫЙ МОНИТОРИНГ ЗЕМЕЛЬ СЕЛЬСКОХОЗЯЙСТВЕННОГО НАЗНАЧЕНИЯ ПО МУЛЬТИСПЕКТРАЛЬНЫМ СПУТНИКОВЫМ СНИМКАМ SENTINEL 2

Одним из наиболее передовых, эффективных и надежных источников информации о свойствах земель сельскохозяйственного назначения и о состоянии посевов являются данные спутниковых снимков Земли.

Спутниковый мониторинг позволяет получать однородную и сравнимую по качеству информацию единовременно для обширных территорий, что практически недостижимо при любых наземных и околоземных обследованиях.

Применяется множество методов по выявлению признаков, позволяющих проанализировать состояния посевов, выявить границы, определить принадлежность к конкретному типу посева. Наиболее часто используемым признаком в таких исследованиях выступает вегетационный индекс нормированной разности NDVI (Normalized Difference Vegetation Index) [1].

NDVI – количественный показатель количества фотосинтетически активной биомассы [1, 2], вычисляемый по формуле

$$NDVI = \frac{r_{NIR} - r_{RED}}{r_{NIR} + r_{RED}} \quad (1)$$

где r_{NIR} - отражение в ближней инфракрасной области спектра,

r_{RED} - отражение в красной области спектра.

Для отображения индекса NDVI используется стандартизованная непрерывная градиентная шкала, показывающая значения в диапазоне от -1..1 в % или в так называемой масштабированной шкале в диапазоне от 0 до 255 (используется для отображения в некоторых пакетах обработки

ДЗЗ, соответствует количеству градаций серого). Благодаря особенностям отражения в NIR -RED областях спектра, природные объекты, не связанные с растительностью, имеют фиксированное значение NDVI, (что позволяет использовать этот параметр для их идентификации):

Тип объекта	Значение NDVI
Густая растительность	0.7
Разряженная растительность	0.5
Открытая почва	0.025
Облака	0
Снег и лед	-0.05
Вода	-0.25
Искусственные материалы (бетон, асфальт)	-0.5

В качестве источника использовались мультиспектральные спутниковые снимки Sentinel_2b (на 2018.03.21). Мультиспектральные спутниковые снимки Sentinel_2 имеют разрешающую способность 10 метров, то есть одному пикселю изображения соответствует участок земной поверхности размером 10×10 метров. Тестовые поля расположены на территории Пахтакорского района Джизахской области Республики Узбекистан [3-4].

Алгоритм мониторинга на примере одного поля.

1) Вычислили вегетационный индекс по ближнем и инфракрасным снимкам по формуле (1). Далее загрузив векторный слой поля, вырезаем поле из растрового изображения. На рис. 1а представлен результат. Что отображает изображения поле оттенком серого с расширением 10×10 м.

2) Чтоб улучшить качество изображения, выполняем процедуру сглаживания изображения методом локальной фильтрации. Суть метода заключается в том, что в ходе обработки по растру скользит прямоугольное окно, которое выхватывает пиксели, используемые для вычисления цвета некоторого текущего пикселя. Если окрестность симметрична, то текущий пиксель находится в центре окна [5].

На практике был использован фильтр с окном 3×3 , результат функции сглаживания представлен на рис. 1б.

3) На третьем этапе для удобства нахождения проблемных участков инвертируем изображения и получаем результат. По изображению (рис. 1в) выделенные карандашом области, имеющие более темные окраски, что означает низкий вегетационный индекс в этих пикселях.

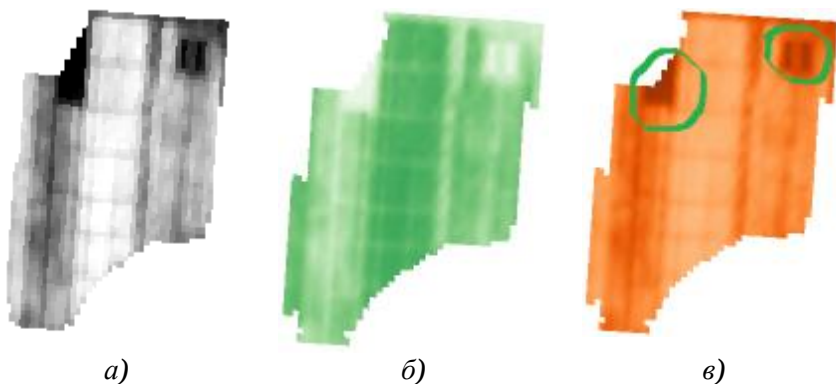


Рис. 1. Алгоритм мониторинга на примере одного поля

Используя при дешифрировании информации об изменении спектральной яркости растительности в течение вегетационного периода и индекса NDVI (Normalized Difference Vegetation Index), по тону изображения полей можно судить об их агротехническом, мелиоративном состоянии и т. д.

Результаты мониторинга дают более объективные и точные сведения, когда совмещаются с актуальными и достаточно точными картами сельхозугодий. Сами же задачи мониторинга решаются на этом фоне эффективнее и с существенно меньшими затратами.

Работа выполнена в рамках проекта, при финансовой поддержке инновационного гранта РУз (№13/19-Ф от 07.01.2019 г).

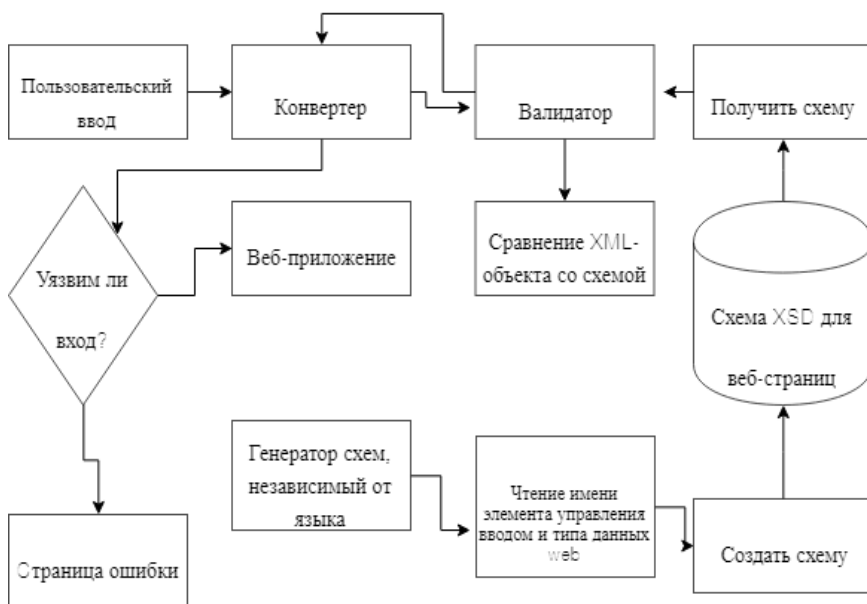
МЕТОДЫ БЛОКИРОВАНИЯ УЯЗВИМОСТЕЙ ВИДА XSS НА ОСНОВЕ СЕРВИС-ОРИЕНТИРОВАННОЙ АРХИТЕКТУРЫ

Веб-приложения разрабатываются на нескольких языках и развертываются в различных операционных системах. Это связано с различными функциями, которые веб-приложение предоставляет своим пользователям. Web-приложения разрабатываются с использованием различных языков, таких как PHP, ASP, JSP, .NET, Python и т.д. на основе требований веб-приложения.

Авторы предлагают сервис-ориентированную архитектуру для предотвращения уязвимостей XSS на разных языках. Решение разработано с использованием языка PHP расширяемого языка разметки (XML) и определений схем XML (XSD). Решение направлено на предоставление независимых служб с определенными интерфейсами, которые могут быть вызваны для выполнения их задач стандартным способом, без предварительного знания вызывающего приложения службой и без знания приложением того, как служба фактически выполняет свои задачи.

Решение основано на подходе сервис-ориентированной архитектуры (SOA). Процедура решения использует XML и XSD для взаимодействия между службами. Это включает в себя создание XML-документа на основе всех элементов управления формы, представленных пользователем. Этот XML-документ будет проверен на соответствие схеме на стороне сервера. Любой вредоносный сценарий приведет к созданию недопустимого или неправильно сформированного XML-файла и, таким образом, не позволит пользователю отправить вредоносные сценарии.

Ниже приведены действия, выполняемые до и после получения HTTP-запроса на стороне сервера: схема для каждой веб-страницы, на которой присутствует элемент управления вводом, создается и хранится разработчиком в автономном режиме в структуре папок или в базе данных; при получении запроса http-запрос передается преобразователю;



конвертер преобразует, входные данные в объект XML и отправляет его в валидатор; средство проверки извлекает соответствующую схему для запроса и сопоставляет объект XML с документом схемы. Если входные данные сопоставляются со схемой, то преобразователю возвращается состояние "да", в противном случае возвращается состояние "нет", если статус "да" получен от валидатора, то запрос перенаправляется в веб-приложение. В противном случае запрос перенаправляется на страницу ошибки.

Преимущества данного подхода заключаются в следующем:

1. Основная часть системы защиты от уязвимостей вида XSS не зависит от платформы и языка.
2. Методы, разработанные авторами, позволяют создать различные системы защиты, основанные на технологиях XML и XSD.
3. Предлагаемый подход строиться на модульном принципе, а также на основе шаблонов регулярных выражений.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Низамутдинов М.К. Тактика защиты и нападения на ИТ-приложения. – Санкт-Петербург: БХВ-Петербург, 2005. – С. 10 – 60.

**Р. Х. Хамдамов, д.т.н.,
Х. Э. Рахманов,
Т. Р. Сакиев**

*Ташкентский университет информационных технологий имени
Мухаммада аль-Хорезми, Ташкент*

РАСПОЗНАВАНИЕ ДЫМА И ОГНЯ МЕТОДОМ КОНТУРНОГО АНАЛИЗА ПО ДАННЫМ ВИДЕОИЗОБРАЖЕНИЯ

В последние годы в Узбекистане большое внимание уделяется развитию интеллектуальных систем, в которых используется подсистема видеоаналитики. Так как возможность использования анализа информации для автоматического извлечения полезной информации из видеоданных приобретает все большее значение при выборе систем видеонаблюдения. Видеосерверы и видеокамеры, становятся все более интеллектуальными благодаря наращиванию процессорных мощностей и увеличению масштабов развертывания систем видеонаблюдения.

Описывается метод фильтрации изображений для детектирования дыма и огня по камерам видео наблюдения на основе платы raspberry pi 3. Детектирование дыма и огня по видеоизображению имеет ряд преимуществ по сравнению с традиционными методами. Во-первых, можно обнаружить дым и огонь даже на открытых пространствах, где обычные методы химического анализа бесполезны. Во-вторых, реакция на возникновение пожара является практически моментальной (обнаружение огня происходит в момент его возникновения). В-третьих, видео позволяет точно определить месторасположение очага возгорания, что дает возможность передачи координат очага через GSM_GPRS(SIM800L)-модуль подключаемым к плате raspberry pi3.

Рассмотрены основные этапы распознавания дыма и огня по видеоизображению. После того, как видео изображения получено с камер видео-наблюдения, оно передается к блоку обработки и анализа изображений raspberry pi. Этот блок включает в себя три этапа реализации: выделения фона от переднего плана (неподвижный объектов называют фоном или задним планом, а движущиеся объекты называют переднеплановыми),

формирования блоков динамических объектов (набор координат составляющий его пикселей) и процедура классификации динамических объектов.

1) Для выделения фона известен целый ряд методов, которые могут быть сгруппированы в зависимости от используемых характерных признаков изображения. В работе был применён метод вычитание фона – это наиболее широко распространенный в настоящее время подход к обнаружению движущихся объектов в видеоизображениях. Суть метода заключается попиксельном сравнении текущего кадра с шаблонным, который обычно называют моделью фона. Для каждого кадра видеопоследовательности необходимо построить двоичную маску изображения, в которой значение 1 соответствует переднему плану, а 0 – фону.

Для отделения объекта от фона в присутствии шума, необходимо выполнить процедуру бинаризации растра, результатом которой будет разделение пикселей растра на два класса: объект и фон. Пусть $R = \{r_{m,n}\}$ $m = \overline{1, M}$, $n = \overline{1, N}$ – изображение, содержащее отдельный динамический объект, тогда правило бинаризации данного изображения будет иметь вид:

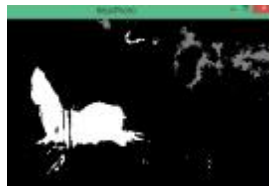
$$\hat{r}_{m,n} = \begin{cases} 0 & \text{если } r_{m,n} \leq b \\ 255 & \text{если } r_{m,n} > b \end{cases}$$

где $\hat{R} = \{\hat{r}_{m,n}\}$ – бинаризованное изображение, b – пороговое значение, которое выбирается по гистограмме распределения яркости пикселей $H = \{h_k\}$, $k = \overline{0, 255}$ текущего растра.

$$b = k, \text{ если } \frac{H_k}{\sum_{l=0}^{k-1} H_l} \leq 0,01$$



а) исходное изображения



б) фильтрованное изображения



в) выделенный блок огня

Рис. 1. Этапы получения выделенных областей огня

2) Так как большая часть информации о форме и ориентации объекта сосредоточена в его граничных точках, формирующих контур объекта, то отпадает необходимость в хранении всех точек объекта. Контур объекта – это совокупность точек (пикселей), отделяющих объект от фона. В системах компьютерного зрения используется несколько способов кодирования контура, наиболее известные из которых – комплекснозначный код, при которых контур кодируется последовательностью комплексных чисел, определяющих смещение текущей точки контура относительно предыдущей. Каждый вектор смещения представляется комплексным числом вида $a + i \cdot b$, где a – смещение точки по оси X , а b – смещение по оси Y , i – мнимая единица. Для однозначного определения положения контура в растре, необходимо также хранить начальную точку контура, определяющую положение контура относительно осей координат растра. Контур всегда замкнут и не может иметь самопересечения. Это позволяет однозначно определить путь обхода контура (с точностью до направления обхода – по или против часовой стрелке). Последний вектор контура всегда приводит к начальной точке.

Для формирования контура используется алгоритм Розенфельда, который состоит из нескольких шагов. На первом шаге необходимо просканировать сцену с целью отыскания верхнего левого граничного пикселя контура. На втором шаге необходимо проследить линию контура, согласно граничным точкам. На третьем шаге нужно сформировать код, которым будет описываться контур. Таким образом, на выходе алгоритма Розенфельда будет сформирован контур выделенного объекта, представляющий собой вектор комплексных чисел, $\Gamma = \{g_k\}_{0,K-1}$ сформированный по следующему правилу:

$-1+i$	i	$1+i$
-1		1
$-1-i$	$-i$	$1-i$

Рис. 2. Координаты элементарного вектора при комплекснозначном кодировании

Так как форма области огня обычно постоянно изменяется и при этом осуществляет стохастические перемещения, зависящие от внешних факторов, таких как тип горящего материала и охватывающие очаг возгорания воздушные потоки [3].

Пиксели огня имеют характерный цвет. Например, в цветных снимках центр огня обычно ярко-белого цвета, который постепенно переходит в желтый, оранжевый и красный, если двигаться по направлению к периферии пламени. В полутоновых изображениях центральная часть значительно более яркая по сравнению с приграничными областями. Необходимо отметить, что область огня может включать в себя несколько отдельных ярких участков. Область огня на отдельно взятом изображении может быть описать как, во-первых, имеющая наибольший контраст с соседними областями и, во-вторых, имеющая вложенную кольцевую структуру цвета, начиная от белого в центре и заканчивая красным на периферии.

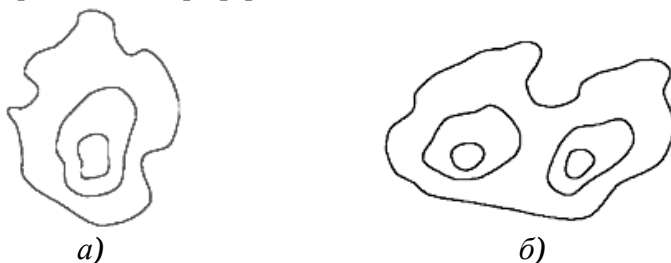


Рис. 3. Кольцевая структура огня.

- а) Контур огня с одним очагом пламени,
- б) контур огня с двумя очагом пламени.

Разработанный алгоритм выделения контура динамических объектов, дает возможность распознать дым и огонь контурным методом. Несмотря на недостатки, присущие контурному анализу при слиянии контуров близко расположенных объектов, методы контурного анализа привлекательны своей простотой и быстродействием. При наличии четко выраженного объекта на контрастном фоне методы контурного анализа хорошо справляется с распознаванием дыма и огня.

Работа выполнена в рамках проекта, при финансовой поддержки инновационного гранта РУз (№13/19-Ф от 07.01.2019 г).

МОДЕЛЬ ІЄРАРХІЇ ПРОЦЕСІВ ТЕСТУВАННЯ

Основна мета тестування програмного забезпечення, підвищити ймовірність того, що додаток, буде працювати правильно при будь-яких обставинах [1, 2].

Більш того, тестування має на меті іншу задачу ніж написання коду – в його основі лежить «деструктивний» підхід: треба довести, що програма не працює. А програмісту, який написав програму, дуже складно переключитися на її випробування, що носять «руйнівний» характер.

Існує три терміна, які легко переплутати: тестування (Testing), контроль якості (QC - Quality Control) і забезпечення якості (QA - Quality Assurance). Всі вони пов'язані один з одним: QA – найширше поняття, воно включає в себе QC, в яке входить тестування [3].

В таблиці представлені порівняльні характеристики.

Забезпечення якості, QA	Контроль якості, QC	Тестування, Test Engineer
комплекс заходів, який охоплює всі технологічні аспекти на всіх етапах розробки, випуску та введення в експлуатацію програмних систем для забезпечення необхідного рівня якості програмного продукту	процес контролю відповідності розроблюваної системи висунутим до неї вимогам	процес, який відповідає безпосередньо за складання та проходження тест-кейсів, знаходження і локалізацію дефектів і т.д.
фокус більшою мірою на процеси і засоби, ніж на безпосередньо виконання тестування	фокус на виконання тестування шляхом виконання	фокус на виконання тестування як такого

системи	програми з метою визначення дефектів з використанням затверджених процесів і засобів	
процесно-орієнтований підхід	продуктно-орієнтований підхід	продуктно-орієнтований підхід
превентивні заходи	коригувальний процес	превентивний процес
підмножина процесів Software Test Life Cycle цикла тестування ПЗ	підмножина процесів QA	підмножина процесів QC

Таким чином, ми можемо побудувати модель ієрархії процесів забезпечення якості: Тестування - частина QC. QC - частина QA.

Належне забезпечення якості може скласти 25-50% від вартості розробки програми.

Критичних проблем можливо уникнути, але невеликі проблеми можуть виникати, навіть в застосуваннях, що випускаються Microsoft, Google і Facebook, якими щодня користуються мільйони, знаходяться проблеми і недоліки. Спосіб створити ідеальний застосунок з першої спроби поки не винайшли, але є методи, що дозволяють звести ймовірність помилок до мінімуму і запобігти їх появі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Уїттакер Д., Арбон Д., Каролло Д. Как тестируют в Google ООО Издательство "Питер"; Санкт-Петербург; 2014. – 106 с.
2. Куликов С. Тестирование программного обеспечения. Базовый курс.: ЕРАМ Systems, 2015–2017. – 106 с.
3. Канер Сэм и др. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений: Пер. с англ. / Сэм Канер, Джек Фолк, Енг Кек Нгуен. – К.: «ДиаСофт», 2001. – 544 с.

МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ОПТИМІЗАЦІЇ РОБОТИ МІКРОПРОЦЕСОРНИХ СИСТЕМ

Проблема оптимізації роботи мікропроцесорних систем, мікроконтролерів, на основі яких побудовано великий спектр вбудованих та мобільних систем, є багатогранною проблемою, в якій пов'язано швидкодію, параметри апаратних засобів, енергоспоживання, тощо. Сучасні мікропроцесорні системи є або багатопроцесорними, або багатоядерними обчислювальними системами. Таким чином, досягнення оптимальності роботи в значної мірі залежить від оптимальності програмного забезпечення, як системного, так і програм користувача. Оптимізація програмного забезпечення - це процес модифікації або трансформації вихідного програмного коду для досягнення певної мети, в якості якої можуть виступати скорочення часу виконання програми, підвищення продуктивності, створення програмного коду компактним, економія пам'яті, мінімізація енерговитрат, зменшення кількості операцій вводу-виводу.

Оптимізація програми здійснюється за допомогою послідовності оптимізуючих перетворень, алгоритмів, які приймають програму і змінюють її для отримання семантично еквівалентного варіанту, який більш ефективний з точки зору будь-якого набору цілей оптимізації. В [1] показано, що деякі проблеми оптимізації коду є NP-повними або навіть нерозв'язними. Однак, на практиці вони вирішуються наближеними методами, які дають результат за задовільний час обробки вихідного тексту програми.

Оптимізація на рівні алгоритму це засіб оптимізації загальної послідовності обчислень. Оптимізація цього рівня, як правило, виконується розробником програмного забезпечення або математиком. Оптимізація на рівні команд представляє великий інтерес, але аналіз і оптимізація програми на системному рівні, тобто, коли аналізуємо алгоритм обчислень, представлений мовою високого рівня, то це обіцяє значний виграш в покращенні роботи системи, оскільки на даному рівні можна виявити принципи

алгоритмічні та мовні конструкції, які підлягають оптимізації. Ця робота, як правило, покладається на компілятори. Оскільки основна обчислювальна робота зосереджена в циклах, то розпаралелювання і оптимізація циклів являє собою найбільш актуальне завдання.

Оптимізаційна задача для кожного i -го обчислювального циклу може бути визначена формулою

$$F_i = \operatorname{argmin} \left(f \left(\vec{M}_i, \vec{P}_i \right) \right) \quad (1)$$

де F_i - параметри, які підлягають оптимізації, M - вектор оптимізаційних методів, P - вектор параметрів оптимізаційних векторів. $\operatorname{argmin}()$ визначається як пошук такого аргументу (одного або декількох) функції, при яких досягається мінімальне значення функції:

$$\operatorname{argmin}_x (f(x)) \in \{x \mid \forall y: f(x) \leq f(y)\} \quad (2)$$

Оптимізаційна задача для всієї програми, яка складається з N обчислювальних циклів в цьому випадку визначається формулою:

$$F = \operatorname{argmin} \overbrace{\sum_{i=1}^N [f(\vec{M}_i, \vec{P}_i)]} \quad (3)$$

Робота спрямована на використання методів розбиття циклу на блоки (tiling) [2]. Однак відкритим залишається питання про розміри блоків і їх формі. В даний час діють наступні обмеження: 1) розглядають тільки прямокутну форму блоку і 2) блоки розбиття ітераційного простору однакового розміру. В [3] було проведено дослідження про характер впливу розмірів блоків на час виконання різних тестових програм. Експерименти показали, що не можна виділити деякий патерн залежності часу виконання від розмірів блоків. Експерименти було проведено з пакетом Polybench і деякі результати представлено на рис. 1, де показано вплив розмірів прямокутних блоків на час виконання конкретної програми.

Використання методів штучного інтелекту для даної задачі полягає в використанні так званого «роевого інтелекту». Ця множина методів визначається як методи глобальної оптимізації, які з великою часткою ймовірності знайдуть глобальний

екстремум. Автори концентруються на методі рою часток як найбільш узагальненого в множині методів «ройового інтелекту».

Таким чином, використання методу рою часток для знаходження оптимальних розмірів блоків розбиття дозволить скоротити час автоматичного розпаралелювання програм або час проектування паралельної програми, оптимізувати роботу мікропроцесорної системи і, зокрема, знизити її енергоспоживання.

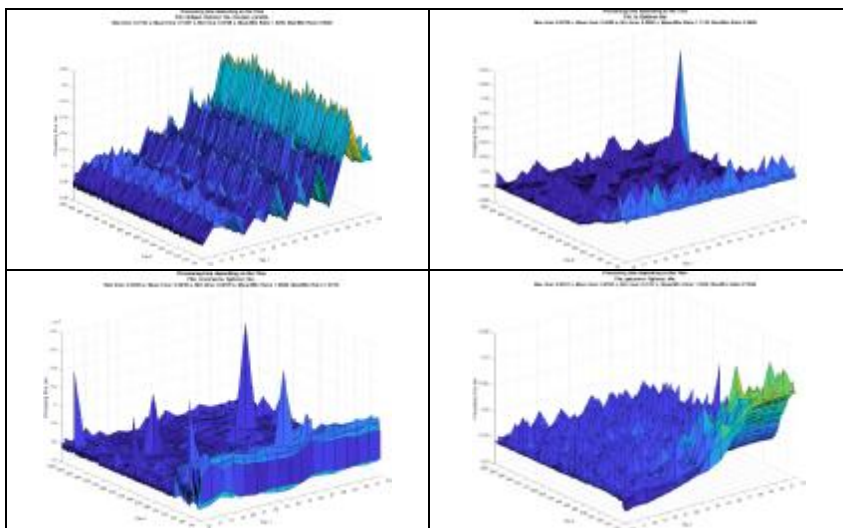


Рис.1. Залежності часу виконання різних програм від розмірів прямокутних блоків розбиття ітераційного простору циклу.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Альфред Ахо. Компиляторы: принципы, технологии и инструментарий. - Compilers: Principles, Techniques, and Tools. / Альфред Ахо, Моника Лам, Рави Сети, Джеффри Ульман — 2-е издание // М.: «Вильямс», 2008. — 1184 с.
2. Xue, J. Loop Tiling for Parallelism. Kluwer Academic Publishers. 2000. – 256 p.
3. Сушко С. В. Вплив розмірів блоків розбиття операторів циклів на час виконання комп'ютерних програм / С. В. Сушко, О. А. Чемерис // Моделювання та інформаційні технології. - 2018. - Вип. 82. - С. 110-117.

**АЛГОРИТМ БАГАТОКРИТЕРІАЛЬНОГО ВИБОРУ
МАРШРУТІВ У ГЕТЕРОГЕННІЙ МЕРЕЖІ**

Гетерогенність – невід’ємна властивість сучасних складових обчислювальних мереж. Характеристики окремих сегментів, що входять до складу мережі, можуть значно відрізнятися одна від одної. Наприклад, пропускна здатність одного сегмента може на порядок і більше перевищувати пропускну здатність іншого сегмента. Такий розкид параметрів призводить до істотного дисбалансу навантаження на окремі сегменти і маршрути передачі, нераціонального використання ресурсів мережі.

Для управління корпоративними комп'ютерними мережами, що включають велику кількість активного обладнання, необхідні складні системи управління, які здійснюють моніторинг, контроль і управління кожним елементом комп'ютерної мережі.

Існуючі системи управління, не зважаючи їх функціональну надмірність, не мають в своєму складі розвинених засобів, що дозволяють якісно прогнозувати поведінку комп'ютерної мережі. Більшість засобів управління насправді мережею не керує, а всього лише пасивно здійснює її моніторинг.

Головним завданням є розробка системи аналізу та прогнозування навантаження комп'ютерної мережі в цілому, окремих сегментів мережі і окремих маршрутів. Це дасть можливість за різними критеріями вибирати найкращі маршрути, заздалегідь виявляти можливі вузькі місця і вживати заходів щодо завчасної їх ліквідації. Тому завдання вдосконалення методів маршрутизації на основі більш повного врахування інформації про стан мережі в цілому і окремих маршрутів є, безумовно, актуальною.

Серед методів вирішення завдань багатокритеріального вибору маршрутів, що мають, з одного боку, теоретичну обґрунтованість, а з іншого боку, що задовольняють вимогам універсальності, найбільшого поширення набули методи аналізу ієрархій (MAI), зокрема, метод, запропонований Сааті [1]. Він заснований на парних порівняннях альтернативних варіантів за різними критеріями і подальшим ранжуванням набору альтернатив за всіма

критеріями і цілями із застосуванням парних порівнянь. Метод відрізняється порівняльною простотою і наочністю, дає гарну відповідність інтуїтивним уявленням про фізичну природу вирішуваних завдань.

Розглянута задача вибору класу топології мереж і відповідних їм пучків маршрутів. У математичному сенсі це завдання багатокритеріальної оптимізації на точковій множині рішень (номерів маршрутів). Особливістю завдання є дискретність цільової функції, тобто якості того чи іншого маршруту.

У цьому завданні робиться вибір між економічністю і якістю сервісу на основі суб'єктивних суджень експертів і математичних моделей достовірності інформації про стан мережі.

Загальні альтернативи розпадаються на групи приватних альтернатив, таких як надійність, ефективність, вартість, точність, завадостійкість, наявні і необхідні ресурси та інші показники. Тут з використанням порядкових шкал можна розрізняти об'єкти і в тих випадках, коли фактор (критерій) не заданий в явному вигляді, тобто коли ознака порівняння не відома точно [2].

Метод аналізу ієрархій може застосовуватися для вирішення широкого кола прикладних задач вибору топології мережі, найкращих маршрутів, програмного забезпечення тощо. При використанні ефективних чисельних методів для точної оцінки власних значень матриць пріоритетів чутливість рішення до помилок завдання вихідних даних виявляється досить низькою. Можна стверджувати, що збоїв процедури вибору найкращого рішення будуть вельми рідкісними подіями, а ймовірність таких подій – величина другого порядку малості.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Саати Т.Л. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.
2. Бешелев С.Д., Гурвич Ф.Г. Математико-статистические методы экспертных оценок. – М.: Статистика, 1980. – 263 с.

Наукове видання

**ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
XII МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

**«КОМП'ЮТЕРНІ СИСТЕМИ
ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»
(CSNT-2019)**

28–30 березня 2019 року

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

ДЛЯ ЗАМІТОК

Підп. до друку 21.03.19. Формат 60х84/16. Папір офс.
Офс. друк. Ум. друк. арк. . Обл.-вид. арк. 8,375
Тираж 60 пр. Замовлення № 111-1

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

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002