ЗМІСТ

Сопронюк И. И., Лысечко В. П.

ИССЛЕДОВАНИЕ ОСНОВНЫХ ПРИНЦИПОВ ФУНКЦИОНИРОВАНИЯ КОГНИТИВНЫХ РАДИОСЕТЕЙ

В докладе кратко изложена проблема регулирования радиочастотных взаимодействий и представлены основные пути ее решения:

Модель частной собственности на спектр;

Модель «открытого (нелицензируемого) спектра».

Альтернативным решением данной проблемы может служить модель сосуществования двух систем, примером которой может быть концепция «когнитивного радио».

В докладе представлено определение термина «когнитивное радио», были исследованы основные элементы когнитивных радиосетей, рассмотрены их особенности и назначение, а также приведен пример реализации когнитивного радио в разрабатываемом стандарте IEEE 802.22.

Подход к построению интеллектуальных радиосистем, получивший название когнитивное радио, является передовой технологией, позволяющей обеспечить рациональное использование радиочастотного спектра.

К отличительным особенностям когнитивного радио следует отнести то, что эти радиосистемы способны получать и передавать сигнал на адаптивно изменяемых радиочастотах, а также изменяя вид модуляции, тип кодирования и другие параметры системы.

УДК 004.056:336.71

Євтухова О.Ю.

ПОБУДОВИ ЛАЗЕРНИХ СИСТЕМ АКУСТИЧНОЇ РОЗВІДКИ З ВИКОРИСТАННЯМ ТВЕРДОТІЛЬНИХ ЛАЗЕРІВ

Останнім часом з розвитком новітніх технологій з'явилася тенденція до розробки та вдосконалення засобів розвідки. Найбільш сучасними та ефективними вважаються лазерні системи акустичної розвідки (ЛСАР), котрі дозволяють відтворювати мову, будь-які інші звуки та акустичні шуми при лазерно-локаційному зондуванні віконного скла.

Типова схема ЛСАР розрахована на використання газового лазеру. Розглянемо можливість використання твердотільного лазеру для побудови ЛСАР.

Типова схема ЛСАР (рис. 1) заснована на принципі інтерферометра Майкельсона [1]. Принцип роботи даної схеми описується наступним чином: когерентний промінь лазера розчіплюється дільником пучка (сплітером) на 2 частини: опорний промінь та інформаційний. Опорний промінь відбивається від опорного дзеркала і направляється на фотодетектор. При відбиванні інформаційного променя від віконного скла відбувається його модуляція звуковою частотою. Відбитий промодульований промінь направляється на фотодетектор, де інтерферує з опорним променем. Сигнал на фотодетекторі після фільтрації підсилюється і подається для подальшого аналізу.

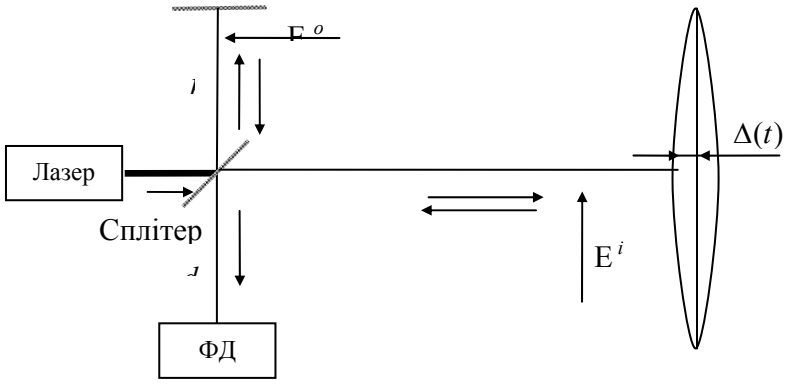


Рис. 1. Типова схема ЛСАР (Інтерферометр Майкельсона)

Дана схема створює значну оптичну різницю ходу δ_1 інформаційного та опорного променів

$$\delta_1 = \left(a+2r+d+2\Delta(t)\right)-\left(a+2b+d\right)=2\left(r+\Delta(t)-b\right) \quad (1)$$

Така схема використовується для ЛСАР з газовим лазером. Для використання ЛСАР з твердотільним лазером типова схема повинна бути модифікована з наведених нижче причин.

Твердотільні лазери володіють малою в порівнянні з газовими когерентністю. Це пояснюється наступним чином. Часова когерентність визначається часом t_k, на протязі якого випромінювання, випущене з однієї точки джерела, залишається когерентним (наприклад, дає інтерференційну картину на інтерферометрі Майкельсона). Часова когерентність пов'язана з монохроматичністю [2]. Цей зв'язок виражається формулою:

$$t_k = \frac{1}{\Delta н}, \quad (2)$$

де Δv - ширина спектру випромінювання, Гц. Величина оптичної різниці ходу двох хвиль, при якій зберігається їх здатність інтерферувати, обмежується довжиною когерентності, що обчислюється наступним чином:

$$l_k = t_k \times c, \quad (3)$$

де c - швидкість світла, м/с. Тому для отримання інтерференційної картини на фотодетекторі різниця ходу інформаційного та опорного променів має бути меншою за довжину когерентності лазера ($\delta < l_k$).

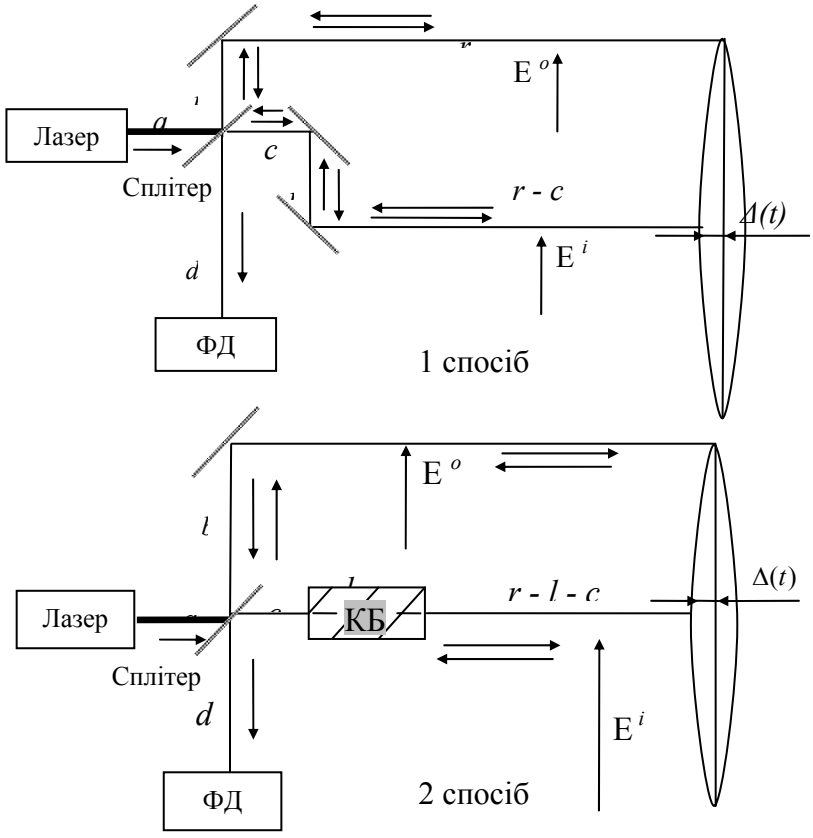


Рис. 2. Вдосконалена схема ЛСАР

Твердотільні лазери, на відміну від газових, мають в своєму випромінюванні значний діапазон частот (порівняно велике значення Δv), тобто відрізняються невисокою монохроматичністю. Як видно з формул 2 та 3, широкий спектр випромінювання призводить до зменшення довжини когерентності l_k, а для отримання чіткої інтерференційної картини треба забезпечити якомога меншу оптичну різницю ходу інтерферуючих променів ($\delta < l_k$). Тому для ЛСАР з твердотільним лазером схему, зображену на рис. 1, можна вдосконалити, звівши оптичну різницю ходу опорного та інформаційного променів до мінімуму (рис. 2), де - оптична різниця ходу променів $\delta = n_1 \cdot \Delta l_1 - n_2 \cdot \Delta l_2$, де n_1, n_2 – показники заломлення середовищ, Δl_1, Δl_2 – відстані, що проходять промені. В даному випадку середовище – повітря, тому $n_1 = n_2 = 1$, а $\delta = \Delta l_1 - \Delta l_2$.

Оптична різниця ходу для даної схеми виражається формулою:

$$\delta_2 = \left(a+2c+2b+2(r-c)+d+2\Delta(t)\right)-\left(a+2b+2r+d\right)= \\ = a+2c+2b+2r-2c+d+2\Delta(t)-a-2b-2r-d = 2\Delta(t) \quad (4)$$

На схемі, що зображена на рис. 2, КБ - компенсаційний блок. КБ, крізь який проходить інформаційний промінь, призначений для зменшення оптичної різниці ходу між інформацій-

ним та опорним променем. Він являє собою тіло, протилежні грані якого паралельні, довжиною l, виготовлене з напівпрозорого матеріалу (наприклад, деяке скло), оптична густина n_B якого більша за оптичну густину повітря, тобто $n_B > 1$. Тоді для оптичної різниці ходу справедливе співвідношення (5):

$$\delta_3 = \left(a+2c+2b+2l\cdot n_B+2(r-l-c)+d+2\Delta(t)\right)-\left(a+2b+2r+d\right)= \\ =2\left(l\cdot n_B-l+\Delta(t)-b\right) \quad (5)$$

Для отримання чіткої інтерференційної картини бажано забезпечити якомога меншу оптичну різницю ходу інтерферуючих променів, тобто потрібно щоб $\delta_4 \to 0$. Оскільки $\Delta(t) << l$, $\Delta(t) << b$, то для визначення l величиною $\Delta(t)$ можна знехтувати. Тоді справедливе наступне співвідношення:

$$\delta_4 = 2\left(l\cdot n_B-l-b\right)=0. \quad (6)$$

Зі співвідношення (6) випливає, що для отримання оптичної різниці ходу близької до нуля, КБ, виготовлений з матеріалу з відомою оптичною густиною n_B повинен мати довжину l, що обчислюється за формулою:

$$l=\frac{b}{n_b-1}. \quad (7)$$

Таким чином, використання вдосконалених схем (рис. 2 та 3) дозволяє застосовувати твердотільний лазер з невисокою когерентністю випромінювання для побудови ЛСАР.

Список використаних джерел

1. Laser microphone - http://www.williamson-labs.com/laser-mic.htm

2. Сэм М. Ф. Лазеры и их применение// Соросовский образовательный журнал – 1996 . – № 6.

УДК 621.396 : 534.143

Мартиненко Т.М.

ЕЛЕКТРОСТАТИЧНИЙ ТА МАГНІТОСТАТИЧНИЙ СПОСОБИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ ВІД "ЛАЗЕРНИХ МІКРОФОНІВ"

Забезпечення захисту мовної інформації від "лазерних мікрофонів" може здійснюватися засобами активного захисту у складі генератора шуму та вібровипромінювача, закріпленого на шибці вікна. Наявність такого вібровипромінювача на вікні розкриває факт застосування засобу захисту від «лазерного мікрофону», що може бути небажано. Таким чином, виникає потреба у приховуванні засобу захисту. Крім того, обмежена маса вібровипромінювача не дає змогу створювати достатню амплітуду коливань шибки на низьких частотах.

Можливим шляхом подолання зазначених недоліків є застосування електростатичних та магнітостатичних сил для впливу на рух скла. Елементом, що може рухати скло, є уплавленні в нього тонкі дротики, тонкі напилені металеві смуги або сполошний тонкий шар металу на віконних шибках. Генератор шуму створює струми або напруги, які породжують взаємодію даних провідників і, як наслідок, коливання скла.

Способи захисту, що досліджуються, основуються на використанні електричних або магнітних сил у подальшому і будуть нести відповідні назви.

Магнітостатичний спосіб реалізовується шляхом металевого нанесення доріжок або дротиків, розміщених паралельно на різних шибках (рис.1). До цих металевих провідників подається струм.

При проходженні струму через провідник за рахунок руху зарядів виникає магнітна взаємодія струмів і навколо провідників починає створюватись магнітне поле. Враховуючи, що металевий провідник є електрично нейтральним, то Кулоновські сили компенсуються. На довжину одного провідника приходиться сила, яка є аналогічною і для іншого провідника і визначається як сила Ампера [1].

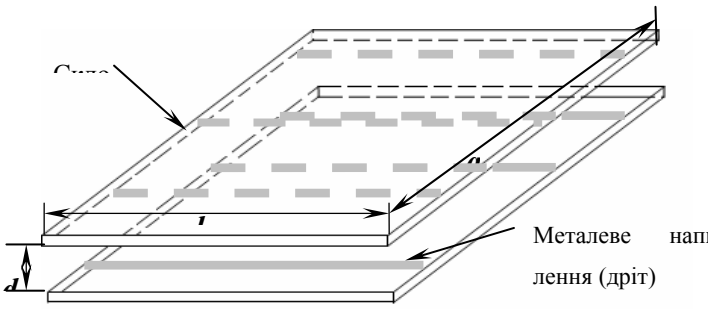


Рис.1. Модель віконного скла з металевим напиленням

При наявності на пластині скла паралельних провідників зі струмом необхідно враховувати силу взаємодії не тільки паралельних провідників, але й сусідніх.

Нехай на пластинах скла шириною a знаходяться N паралельних провідників зі струмом. Тоді сила взаємодії провідника n з m буде визначатися як

$$F_{nm} = F \cdot \cos\psi_{nm}$$

де F – сила взаємодії двох паралельних провідників зі струмом;

значення кута між векторами сили взаємодії провідників, визначається як

$$\cos\psi_{nm} = \frac{d}{d_{nm}} = \frac{d}{\sqrt{d^2 + \left[(n-m)\frac{a}{N}\right]^2}},$$

де d_{nm} – відстань між провідниками n і m.

Сила, з якою взаємодіють провідники зі струмом протилежної пластини скла на провідник зі струмом n буде визначатися як сума сил

$$F_{\eta_n} = \mu_0 \frac{I_1 I_2 l d}{2\pi} \sum_{m=1}^{N} \frac{1}{d^2 + \left[(n-m)\frac{a}{N}\right]^2} \text{ [2].}$$

Тоді сумарна сила тиску буде визначатися за формулою:

$$F_\eta = \sum_{n=1}^{N} F_{\eta_n} = \mu_0 \frac{I_1 I_2 l d}{2\pi} \sum_{n=1}^{N}\sum_{m=1}^{N} \frac{1}{d^2 + \left[(n-m)\frac{a}{N}\right]^2} = \mu_0 \frac{I_1 I_2 l d N^2}{2\pi a^2} \sum_{n=1}^{N}\sum_{m=1}^{N} \frac{1}{\left(\frac{N^2 d^2}{a^2}\right) + (n-m)^2}. \quad (1)$$

Нехай звуковий тиск в приміщенні від людської мови P_1**.** Реально це складає величини 0,2 … 1 Па у діапазоні частот 150 Гц … 1 кГц. При розмірах віконної шибки 0,9*м* х 1,2 *м* і тиску в 0,2*Па* маємо F_1=0,216 Н. Розраховане значення сили можна розцінювати як мінімальним для сили, з якою повинні взаємодіяти віконні шибки під впливом магнітностатичного поля. Рівень потрібних струмів можна оцінити наступним чином. Підставивши в формулу (1) F_1 розрахуємо значення прикладеного струму, враховуючи, що $I_1 = I_2$, відстань між віконними шибками d=0,02*м* і кількість провідників на склі N (табл.1).

Таблиця 1

N, шт	10	30	100	300
I, A	47	22	7	2

З таблиці 1 видно, що одержані значення струмів можна фізично реалізувати. Для реалізації цього генератор шумових струмів повинен створювати шумові струми на кожній шибці як у співпадаючих, так і у протилежних напрямах. Фізично це можна реалізувати на 2-х незалежних шумових генераторах, під'єднаних кожний до своєї шибки.

Електростатичний спосіб можна реалізувати шляхом напилення шару металу по всій площині віконних стекол. При подачі напруги до напиленого шару виникає електричне поле.

Відстань між шибками значно менше, ніж їх лінійні розміри. Тому можна знехтувати малими областями неоднорідності електричного поля по краях металевого напилення і вважати, що утворене поле є однорідне і зосереджене між паралельними шарами металу[1]. В даній схемі необхідно подавати до пластин напруги, що будуть в часі змінювати свої знаки і чередуватись. Це призведе до того, що під дією електростатичного поля пластини почнуть відштовхуватись чи притягуватись, в залежності від прикладеного знаку напруги.

Враховуючи, що в даному випадку провідниками є паралельні пластини, то ця модель

розглядається як плоский конденсатор, в якому діелектриком виступає повітря. Для визначення необхідного потенціалу напруги, що прикладається до обкладинок конденсатора необхідно провести розрахунки. Скориставшись значенням, розрахованим вище для сили і знаючи, що діелектрична проникність вакууму $\varepsilon = 1$ значення заряду складе $q = \sqrt{2F\varepsilon\varepsilon_0 s} = 2{,}03201 \cdot 10^{-6} (Кл)$.

Вирахуємо ємність конденсатора [2] $C = \frac{1 \cdot 8{,}85 \cdot 10^{-12} \cdot 1{,}08}{0{,}02} = 4.779 \cdot 10^{-10} = 477{,}9 (пФ)$.

Тоді значення напруги у вигляд формули $U = \frac{q}{C} = 4{,}2 (кВ)$.

Одержана величина напруги для електростатичного методу показує, що його фізично можливо реалізувати.

Таким чином, було проведено дослідження способів захисту інформації від «лазерних мікрофонів» шляхом створення електростатичного і магнітостатичного полів навколо віконних стекол, що приводить до створення шумових коливань шибки. Показана можливість фізичної реалізації запропонованих способів. У подальшому доцільно провести дослідно-конструкторські роботи по створенню пристроїв із запропонованим принципом дії.

Список використаних джерел

1. Афанасьев С.Б. Краткий справочник по физике / С.Б. Афанасьев, С.В. Бубликов, С.Н. Сашов; под ред. С.Д. Ханина. – СПб.: Питер, 2000. – 285 с.

2. Феодосьев В.И. Сопротивление материалов: В 8 т.; Т. 2/ В.И. Феодосьев. – М.: Изд-во МГТУ, 1999. – 590 с.

УДК 378.147

Метешкин К.А., Левковская А.П.

ВОЗМОЖНОСТИ ГИС-АНАЛИЗА В УПРАВЛЕНИИ ВЫСШИМ ОБРАЗОВАНИЕМ НА РЕГИОНАЛЬНОМ УРОВНЕ

Розглядаються можливості використання геоінформаційних технологій в управлінні вищими навчальними закладами на регіональному рівні.

Современное состояние образовательной системы Украины, в частности высшей школы, имеет сложную структуру, которая постоянно развивается и совершенствуется.

В настоящее время, так и не решена задача построения информационно-управляющей системы образованием Украины, которая обеспечивала бы сбор, хранение и обработку информации о состоянии высших учебных заведений, в первую очередь на региональном уровне. На наш взгляд, для решения этой задачи необходимо воспользоваться специальными возможностями геоинформационных технологий, и в частности, существующими прикладными программами, обеспечивающими пространственно-временное представление данных об образовательной системе. В настоящее время существует ряд работ [1, 2], в которых изложены принципы и задачи построения геоинформационной системы управления образовательной системой, а также возможность интеллектуализации принимаемых решений на уровне региона. Кроме того, в работе [3] предложены подходы к созданию виртуальной модели высшего учебного заведения.

Возникает задача научного обоснования целесообразности решения задач управления образовательной системой на основе ГИС-анализа ее структуры, качественных и количественных характеристик. Важной задачей является оценка связей образовательной системы с другими городскими и региональными структурами и видами обеспечения, например, транспортного, медицинского, социально-культурного и т.д. На наш взгляд, ГИС-анализ можно использовать при оценки занятости и трудоустройства выпускников вузов с учетом их спе-

циальностей. Кроме того, актуальной задачей является оценка территориального распределения интеллектуального потенциала высших учебных заведений.

Таким образом, на основе результатов ГИС-анализа можно разработать соответствующие формализмы и интеллектуальные модели, которые бы обеспечивали поддержку принятия решений в образовательной системе регионального уровня.

Список использованных источников

1. Метешкін, К.О. Концепція використання геоинформатики в побудові інформаційно-кіруючої системи «Вища школа України»/ К.О. Метешкін, І.М. Патракєєв, О.В. Постоєнко. – Інформаційні технології і засоби навчання: електронне наукове фахове видання/ Гол. ред.: В.Ю. Биков; Ін-т інформ. технологій і засобів навчання АПН України, Ун-т менеджменту освіти АПН України. – 2009. – № 5(13). – Режим доступу http://www. nbuv. gov.ua/e-journals/ITZN/ em6/emg.html. – Заголовок з екрану.

2. Метешкин, К.А. Особенности организации пространственно-иерархических данных в системе управления образованием на региональном уровне/ К.А. Метешкин, И.М. Патракеев, Е.А. Семенихіна// Восточно-Европейский журнал передовых технологий. – 2010. – №3/5(45). – С.42-45.

3. Шипулин В.Д. ГИС управляет вузом/ В.Д. Шипулин, А.В. Постоенко// Геоинформационные системы в Украине. – Спец. вып. – Август 2010. – www. cad.in.ua. – С.30 – 32.

УДК 621.317.7

Козлов Ю.В.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПОБУДОВИ НВЧ-МУЛЬТИМЕТРІВ

Розглянуто можливості використання апаратних, спеціальних і універсальних програмних компонентів для побудови віртуального мультиметра НВЧ-діапазону, що відповідає сучасним вимогам.

Енергія коливань надвисоких частот (НВЧ) широко використовується в радіолокації і радіонавігації, телебаченні, військовій техніці, а також у технологічних процесах і наукових дослідженнях (системи термоядерного синтезу, прискорення елементарних часток, вивчення дії електромагнітних коливань на матеріали і т.п.). Невід'ємною частиною таких процесів є вимірювання параметрів електромагнітних коливань:

- випромінюваної потужності (середньої або імпульсної);
- частоти і стабільності частоти передавального пристрою;
- фазових зсувів і коефіцієнта стоячої хвилі у приймально-передавальних трактах або модуля і аргументу комплексного коефіцієнта відбиття (ККВ) навантаження.

Такі вимірювання доцільно виконувати за допомогою НВЧ-мультиметрів, які можуть застосовуватися також для пошуку несправностей, а в ряді випадків – для прогнозування відмовлень.

Сучасні тенденції створення автоматизованих засобів вимірювальної техніки (ЗВТ) передбачають реалізацію концепції віртуального приладу (ВіПр) у складі персонального комп'ютера (ПК), апаратних та програмних компонентів. Агрегатний (модульний) принцип побудови та апаратні компоненти із раціонального ряду уніфікованих функціональних модулів і базових конструкцій дозволяють розробляти ВіПр, призначені для вирішення будь-яких вимірювальних завдань.

В якості модулів ВіПр можуть використовуватися:

- контролери і модеми;
- модулі введення-виведення – сукупність каналів аналого-цифрового та цифро-аналогового перетворення різної розрядності;
- сигнальні процесори, виконані під спеціальне математичне і програмне забезпечення типу MatCad або MatLab;

- спеціальні процесори, що перепрограмуються, або із жорсткою логікою функціонування, в тому числі на базі програмуємих логічних матриць (ПЛМ) і програмуємих логічних інтегральних схем (ПЛІС) тощо.

Апаратні засоби ВіПр об'єднуються за допомогою інтерфейсів RS-232, RS-435, токових (0-5, 0-20, 4-20 мА), шини VXI, яка включає канал загального користування (приладовий інтерфейс) як одну зі складових, різноманітних комунікаційних модулів-перетворювачів інтерфейсів, а також інтерфейсів ПК.

У теперішній час для створення ВіПр більше сотні закордонних фірм випускають окремі модулі та комплекти модулів для роботи з ПК. Вони підключаються або безпосередньо через слот розширення, або за допомогою кабелю та спеціального інтерфейсного модуля.

Головною особливістю ВіПр є їх програмне управління, що визначає важливу перевагу – прилад можна перепрограмовувати, змінюючи його функціональні можливості, розширюючи галузь застосування, підвищуючи універсальність, роблячи менш схильним до морального старіння.

Програмні компоненти ВіПр включають звичайно програмне забезпечення (ПЗ) персонального комп'ютера, а також спеціальні засоби, призначені для програмування віртуальних приладів.

Такими засобами є, наприклад, пакети FIDES-95, N-FIDES 1.0, SEDIF 2.0 із спеціальним графічним інтерфейсом. Вони дозволяють реалізовувати вимірювальні й обчислювальні процедури з використанням віртуального калькулятора, який програмується для виконання арифметичних операцій, логарифмування и т.п. Недоліком цих пакетів є неможливість програмування складних формул, які мають більше двох аргументів, а також обмежений склад елементів управління й відображення.

Інструментальне середовище VisiDAQ, призначене для розробки систем збору даних, автоматизації лабораторних вимірювань і випробувань, розроблене на мові сценаріїв, сумісній з мовою Visual Basic. Це середовище дозволяє реалізовувати складні алгоритми обробки даних, їх графічне подання, містить багато вбудованих функціональних блоків і графічних елементів відображення, що дозволяють суттєво зменшити витрати на розробку ВіПр і систем промислової автоматизації.

Розповсюджені також програмні середовища HP VEE фірми Hewlett-Packard і LabWindows фірми National Instruments. Обидва середовища розроблені на мові Visual Basic і використовуються для створення комплексів збору і обробки вимірювальних інформації. Особливістю обох середовищ є можливість створення і використання ВіПр сумісно з реальними вимірювальними приладами, підключеними до комп'ютера.

Програмне середовище (ПС) HP VEE має більш зручний користувацький інтерфейс, розширений математичний апарат і широкі можливості конвертації форматів даних.

Середовище LabWindows більш широко використовується через те, що основні виробники вимірювальних засобів забезпечують інтеграцію з LabWindows наявністю програмних драйверів для управління приладами.

Підкреслимо, що особливістю сучасного мультиметра НВЧ-діаназону є використання дискретної вимірювальної лінії (ДВЛ), що робить непридатними для застосування більшість вище перелічених апаратних та програмних засобів. І взагалі, описані програмні засоби «імітують» реальні прилади. Створення оригінальних розробок із їх використанням утруднено. Для цього доцільно використовувати універсальні засоби (системи) візуального програмування.

Серед систем візуального програмування загального призначення можна назвати програмні середовища Delphi й Visual Basic.

ПС Delphi є одним із удосконалень мови програмування Pascal, призначеним для роботи з операційною системою Windows у версіях 3, 4 та вище.

ПС Visual Basic – удосконалення алгоритмічної мови Basic - дозволяє достатньо легко й швидко створювати додатки для Windows, навіть не маючи фундаментальної підготовки у використанні мов програмування високого рівня.

Програмні середовища Delphi й Visual Basic схожі за призначенням і можливостям. Вони мають графічний інтерфейс, у якому можна конструювати екранні форми й елементи управління, які використовуються в додатках. Серед інструментів, що спрощують розробку додатків, є проекти, форми, об'єкти, шаблони, нестандартні елементи управління, менеджер баз даних та ін.

Перелічені ПС реалізують об'єктно-орієнтований підхід у програмуванні. В прийнятій за кордоном термінології їх називають також інтерактивними програмними середовищами або інтегрованими середовищами розробки. Їх застосовують шляхом «конструювання» інтерфейсу користувача, його графічного оточення і програмування процедур обробки дій користувача та отриманих даних.

Використання ПС Delphi дозволило автору розробити макет віртуального НВЧ-мультиметра, який реалізує на ПК складні процедури ітераційної обробки даних, отриманих від зондів ДВЛ, і відображує результати вимірювання параметрів електромагнітних коливань.

Козлов В.Є., Козлов Ю.В.

ТАХИСТОСКОП

Розглянуто питання застосування програмного тренажера для набуття навичок швидкісного читання.

Основу всякого навчання складає самонавчання. Воно ґрунтується на умінні планувати і організовувати свою роботу, раціонально читати, вести записи, на знанні своїх психічних можливостей і умінні їх використовувати, тобто на знанні так званої технології учіння (діяльності *учня - особи, що навчається,* – в оволодінні знаннями, уміннями та навичками). Одним із найважливіших умінь в технології учіння є уміння раціонально, тобто швидко і ефективно (у сенсі розуміння прочитаного) читати.

Традиційному методу читання властиві такі недоліки:

1) відсутність гнучкої стратегії читання, обумовлена нездатністю правильно вибрати спосіб читання для смислового сприйняття тексту;

2) нестійкість уваги, невміння зосередитися;

3) регресія – мимовільні зворотні рухи очей із повторною фіксацією погляду, що викликаються гаданими трудностями тексту;

4) мала зона ясного бачення – ділянки тексту, який чітко сприймається при одній фіксації погляду;

5) артикуляція – промовляння тексту вголос або про себе.

Ці недоліки обумовлені відсутністю навичок швидкісного читання.

Швидкісне читання передбачає наявність спроможності розуміти прочитане й уміння раціонально організувати процес читання. При швидкісному читанні читаються не слова, а думки. Читач бачить усю графічну інформацію на сторінці й, минаючи мовноруховий і слуховий канали, спрямовує інформацію в мозок. Головним завданням при засвоєнні техніки швидкісного читання є усунення регресії. Основне правило при цьому: текст будь-якого ступеня трудності завжди читається тільки один раз. Для вправ вибираються прості тексти описового характеру без прямої мови з мінімальною кількістю чисел, імен, формул, назв і т.п.. Спочатку це можуть бути вузькі газетні, потім журнальні колонки, потім книжкові сторінки.

В психології з метою визначення швидкості й точності сприйняття, а також уваги, яка при цьому проявляється, колись застосовували механічний прилад – тахістоскоп, який із встановленою швидкістю подавав зорові подразники (літери, геометричні фігури, цифри, окремі слова і т.п.). Використання принципу побудови тахістоскопа і сучасних інформаційних технологій дає змогу автоматизувати процес надбання навичок швидкісного читання. У програмному середовищі Visual Basic розроблено програмний виріб-тренажер для персонального комп'ютера (див. рис. 1), який дає змогу подавати інформацію із заданою швидкістю (від 20

до 100 знаків за секунду) у рядках, ширина яких відповідає типу тексту – газетний, журнальний або книжковий. Тексти, що містять до 5 тисяч знаків (приблизно 2 сторінки формату А4, шрифт Times New Roman, кегль 12, інтервал полуторний), із науково-популярних або публіцистичних видань готуються завчасно у текстовому форматі.

Після ініціалізації програми читають файл і встановлюють швидкість подання тексту від 1200 до 6000 знаків за хвилину. Задають вид текстового документу для читання: газета, журнал, книга. Натискають кнопку ЧИТАТИ: рядки тексту «видаються» один за одним із заданим темпом в рамку на полі вікна до моменту закінчення тексту, про що видається сповіщення КІНЕЦЬ. Якщо заданий темп читання надто високий, процес подання інформації можна зупинити натисканням кнопки СТОП.

Якість засвоєння тексту необхідно постійно контролювати. Контроль засвоєння вправ провадиться шляхом переказу про себе або вголос, а краще шляхом письмового викладу змісту тексту з наступною перевіркою повноти і правильності.

Засвоєння методики швидкісного читання потребує витрат часу порядку 70-100 годин. Якщо не ставити перед собою завдання досягнення максимальної швидкості читання, а пам'ятати, що суть швидкісного читання – «вичерпування» корисної інформації, то позитивних результатів можна досягти за 10-12 годин, займаючись по 0,5 години 3-4 рази на тиждень. Починати тренування доцільно з газетних текстів, ширина яких складає 20 знаків, і малої швидкості подання тексту, поступово збільшуючи її. Потім таким же чином читати журнальні тексти (шириною 30 знаків) і наостанок – книжні (шириною 60 знаків з більшим шрифтом).

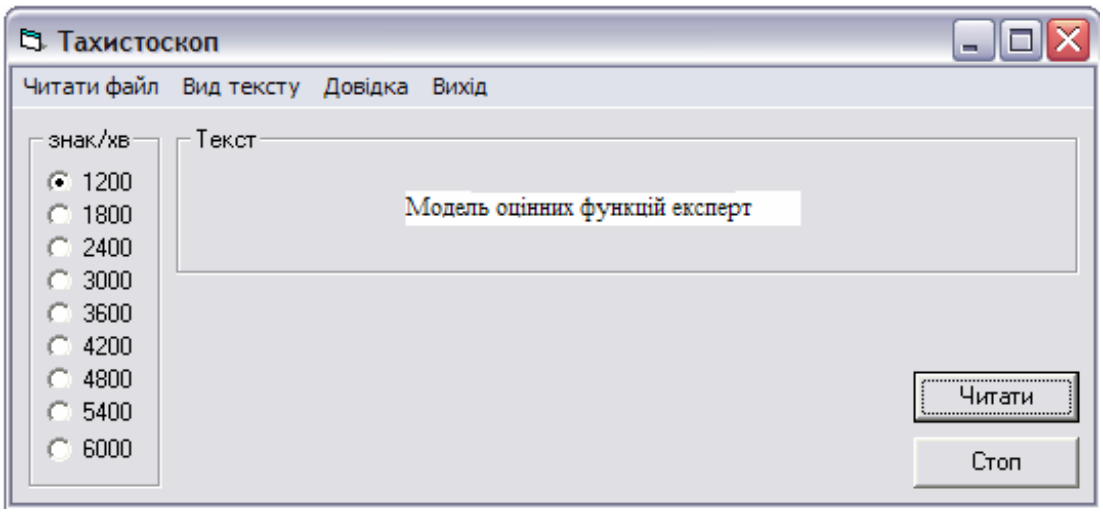


Рис. 1. Вікно додатку «Тахістоскоп» в режимі читання тексту виду «Журнал»

Тренування за персональним комп’ютером привчає читати тільки вертикальним рухом очей, щоб подолати регресію, опосередковано вирішує проблему придушення артикуляції та розширення зони ясного бачення, тобто дозволяє усунути три останні недоліки традиційного читання.

Земляна Н.В., Козлов В.Є., Краузе В.Г., Товма Л.Ф.

БАЗА ДАНИХ «ТЕХНОЛОГІЯ ПРИГОТУВАННЯ ЇЖІ»

Розглянуто питання створення бази даних із технології приготування їжі з використанням сучасних інформаційних технологій.

Зміст бази даних «Технологія приготування їжі» доцільно скласти за такою структурою:
- загальний опис страви;
- технологічна карта приготування страви:
  1) назва страви;

2) назва сировини;

3) маса сировини (брутто, нетто, на одну та десять порцій);

4) нормативна документація, що регламентує вимоги до якості сировини;

5) технологія приготування страви.

Таку базу даних (БД) можна створити двома способами: з використанням засобів системи управління базами даних (СУБД) MS Access і можливостей файлової системи операційної системи (ОС) Windows.

Перший спосіб передбачає розробку декількох типів таблиць відповідно до виду страви: перші, другі страви, десерти, напої тощо. В межах таблиць розміщуються:

- назва таблиці – назва страви;
- текстове поле – загальний опис страви;
- текстове поле – назва сировини;
- чотири числових поля (маса сировини – брутто, нетто, на одну та десять порцій);
- текстове поле – нормативна документація, що регламентує вимоги до якості сировини;
- поле МЕМО – технологія приготування страви.

Розроблена БД зберігається на відповідному носії інформації (диск, папка, робочий стіл тощо).

Пошук потрібної інформації здійснюється в такій послідовності:

- відкривається БД, розміщена на відповідному носії;
- відкривається таблиця або завчасно сформований запит з назвою відповідної страви (при потребі такий запит формується за правилами СУБД MS Access);
- відкрита таблиця може бути використана безпосередньо або скопійована для подальшого роздруку.

Особливістю побудови БД другим способом є використання можливостей файлової системи операційної системи (ОС) Windows для пошуку необхідної інформації. Документи, що містять загальний опис і технологічна карта приготування страви, збираються у відповідні папки (вид страви) і файли (страви) і зберігаються на носії інформації.

Пошук здійснюється в такій послідовності:

- натискається кнопка **Пуск** вікна ОС;
- відкривається вікно **Поиск** для вибору параметрів пошуку;
- в лівій стороні вікна **Результаты поиска**, що відкриється, набирають частину імені файлу або ім’я файлу в цілому, слово або фразу у файлі, носій інформації (диск, папка, робочий стіл), на якому міститься документ, що розшукується, та інші дані, що розширюють можливості пошуку;
- натискається кнопка **Найти**.

Результати пошуку відображаються в правій стороні вікна і дозволяють відкрити потрібний документ. Він може бути прочитаний в електронному вигляді або роздрукований.

Таким чином, створення БД зводиться до розробки документів, які відповідають змісту бази, а їх назва є унікальною, щоб забезпечити однозначний пошук потрібної інформації, можливість її редагування та поповнення.

УДК 621.396

Бережний Д.О., Щербак Г.В.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВІДОМЧОГО РАДІОЗВЯЗКУ УПРАВЛІННЯ В КОРОТКОХВИЛЬОВОМУ ДИАПАЗОНІ

В роботі проведено аналіз використання радіозв’язку короткохвильового діапазону в підрозділах МНС України, запропоновано заходи щодо вдосконалення роботи системи на невеликих відстанях, та намічено підходи до вирішення проблеми по усуненню «мертвої» зони поблизу радіостанцій короткохвильового діапазону, що працюють в мережах управління, оповіщення і взаємодії МНС України.

Організація радіозв’язку міського і позаміського пунктів управління МНС України з пун-

ктами управління Головного управління МНС в АР Крим, Головних управлінь (Управлінь) МНС в областях, містах Києві та Севастополі, з відповідними вузлами зв'язку Центрального командного пункту ГШ Збройних Сил України, МВС України, Державної прикордонної служби України здійснюється згідно з Розпорядженням по зв'язку МНС України в повсякденній діяльності, при виникненні та ліквідації надзвичайних ситуацій, на навчаннях та тренуваннях.

Використання короткохвильового діапазону для організації радіомереж управління, оповіщення і взаємодії МНС України розглядається, перед усім як резервна система зв'язку і управління аварійно-рятувальними підрозділами. На відміну від всіх існуючих систем зв'язку, короткохвильовий (декаметровий) зв'язок відновлюється набагато швидше і значно з меншими економічними витратами. При виході з ладу систем супутникового, проводового чи будь-якого іншого відомчого зв'язку, оперативність реагування на надзвичайні ситуації підрозділів та управління силами МНС зменшуються до нуля, що може призвести до тяжких наслідків. Якими б великими не були матеріальні витрати на вдосконалення систем зв'язку, «економічний ефект» дасть позитивний результат, адже критерієм ефективності у даному випадку слід розглядати мінімізацію збитків (в тому числі людських жертв) від тієї чи іншої надзвичайної ситуації.

Труднощі зв'язку в короткохвильовому діапазоні виникають тому, що декаметрові радіохвилі мають властивість розповсюджуватись на досить великі відстані з якими важко співставити навіть розміри нашої країни. На менших відстанях (радіусом до 500 км) через особливості розповсюдження радіохвиль виникає так звана «мертва» зона, зона де радіосигнал слабкий або зовсім відсутній — тобто зв'язок між кореспондентами буде неможливим.

Для вирішення цієї проблеми пропонується встановлення ретрансляторів короткохвильового діапазону на достатньо великій відстані від території нашої держави, наприклад в Санкт-Петербурзі (Росія), або в Стокгольмі (Західна Європа). У цьому випадку ретранслятор приймає радіосигнал переданий радіостанцією будь-якого підрозділу МНС України та підсиливши, відправляє його в зворотному напрямку, де його приймають радіостанції-кореспонденти, які знаходяться в «мертвій» зоні.

Таким чином вирішується проблема створення надійної системи зв'язку на території України, яка враховує просторову розв'язку і забезпечить безперервність управління підрозділами МНС. Крім того, слід зауважити, що додатково утворюється лінія міжнародного відомчого зв'язку, що надасть змогу ефективно і надійно здійснювати обмін оперативною інформацією з підрозділами аварійно-рятувальних сил інших країн європейської спільноти під час вирішення сумісних завдань з ліквідації надзвичайних ситуацій.

УДК 354.3

Білоус І.О., Щербак Г.В.

ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ СИЛАМИ І ЗАСОБАМИ МНС ПРИ ПРОВЕДЕННІ ПОШУКОВО-РЯТУВАЛЬНИХ РОБІТ ІЗ ЗАСТОСУВАННЯМ АВІАЦІЇ

Надано пропозиції щодо вдосконалення існуючої системи управління силами і засобами МНС, які дозволять забезпечити необхідний рівень ефективності повсякденного керування та управління черговими авіаційними силами при проведенні авіаційних робіт з пошуку і рятування.

Нестабільність політичної обстановки у багатьох регіонах світу та збільшення кількості проведених різними екстремістськими організаціями терористичних актів, погіршення економічної ситуації на Україні потребує проведення постійного моніторингу великої кількості територіально розподілених потенційно небезпечних об'єктів, а також здійснення контролю повітряного простору держави, з метою попередження виникнення надзвичайних ситуацій (НС) та зменшення загального часу на їх ліквідації.

Існуюча система управління авіацією при проведенні авіаційних робіт з пошуку і рятування (АРПР) МНС складається з наступних органів управління: Головного центру координації АРПР, регіональних координаційних центрів з пошуку і рятування, органів управління у зонах відповідальності на діючих аеродромах МО, МНС, МВС, цивільної авіації України де здійснюється чергування вертольотів та літаків, які задіяні в проведенні пошуково-рятувальних операцій.

Система управління авіацією при проведенні АРПР МНС має ряд недоліків, які ускладнюють виконання завдань за призначенням:

- взаємодія авіаційних (аеромобільних) сил та засобів міністерств, центральних органів виконавчої влади в районі пошуку здійснюється тільки шляхом особистого спілкування посадових осіб відповідних пунктів управління (ПУ) із використанням існуючих каналів зв'язку без застосування засобів автоматизації;
- існуючий стан системи управління авіацією при проведенні АРПР МНС не відповідає сучасному рівню розвитку телекомунікаційних мереж і не може стати основою для об'єднання перспективних засобів автоматизації, що будуть розроблюватись у найближчий час;
- чергові сили авіації (екіпажі вертольотів та літаків, парашутно-десантні групи), які задіяні в проведенні операцій з пошуку і рятування від МО, МВС, МНС, цивільної авіації мають різний рівень підготовки та кваліфікації;
- аеродроми базування чергових сил авіації мають різне обладнання для забезпечення управління польотами екіпажів в різних метеоумовах, вдень та вночі, а також різну можливість щодо матеріально-технічного забезпечення, обслуговування та підготовки до застосування різнорідної авіаційної техніки;
- відсутність єдиного інтегрованого радіолокаційного поля суб’єктів системи проведення АРПР МНС та неможливість відображення єдиної повітряної обстановки в районі лиха на ПУ, які відповідальні за виконання операцій з пошуку і рятування, за допомогою засобів автоматизації збору, обробки та передачі радіолокаційної інформації МО, МВС, МНС тощо.

Тому необхідно зазначити, що вдосконалення існуючої системи управління авіацією при проведенні АРПР Міністерством з питань надзвичайних ситуацій має дуже актуальне значення.

З метою усунення вказаних недоліків існуючої системи управління авіацією при проведенні АРПР МНС необхідно:

- здійснити розробку сучасної телекомунікаційної мережі системи управління авіацією при проведенні АРПР МНС;
- здійснити інтеграцію автоматизованих радіолокаційних полів ВПС ЗС України, Державного підприємства обслуговування повітряного руху України, МВС та МНС з метою створення єдиної повітряної обстановки на усіх ПУ, які відповідають за організацію і проведення АРПР;
- розробити єдину програму підготовки чергових сил (льотного складу та парашутно-десантних груп) різних міністерств та відомств щодо проведення АРПР;
- здійснити розробку уніфікованих програмно-технічних засобів, здатних отримувати аеронавігаційну інформацію від різних відомчих систем і забезпечити автоматизоване управління силами та засобами при проведенні АРПР;
- створити науково-дослідний підрозділ, який би проводив наукові дослідження з питань удосконалення системи управління авіацією при проведенні АРПР МНС та здійснював якісне наукове супроводження розробок перспективних технічних та програмних засобів автоматизації з управління силами і засобами при проведенні АРПР.

Виконання вказаних заходів щодо вдосконалення існуючої системи управління силами і засобами МНС дозволить забезпечити необхідний рівень ефективності повсякденного керування та управління черговими авіаційними силами при проведенні АРПР і зберегти найдорожче — життя багатьох людей при виникненні НС на території України.

УДК 621.397:681.32
Григорьева Д.А., Щербак Г.В.

РЕЗУЛЬТАТЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ РАДИОЛОКАЦИОННОГО «ПОРТРЕТА» ПЛАСТИКОВОЙ ПРОТИВОПЕХОТНОЙ МИНЫ

Приведены подходы к созданию базы радиолокационных «портретов» взрывоопасных предметов в укрывающих средах на примере математического моделирования частотных откликов пластиковой противопехотной мины DM11.

Анализ основных существующих электромагнитных методов зондирования взрывоопасных предметов в укрывающих средах показал, что для решения задач гуманитарного разминирования, в первую очередь присущих спецподразделениям МЧС, наиболее перспективным является радиолокационный метод. Данное утверждение базируется на способности метода к обнаружению любых взрывоопасных предметов (металлы, пластмассы и др.) в грунте и на его поверхности, а также принципиальной возможности распознавания (формы, размеров, материала и др.) обнаруженных объектов.

Процессы обнаружения и, особенно, распознавания взрывоопасных предметов заключаются в сравнении электромагнитных откликов от объектов, расположенных в укрывающих средах, с радиолокационным «портретом» взрывоопасных предметов, полученным априорно. Чем больше таких «портретов», тем выше вероятность правильного обнаружения. Отсюда следует необходимость формирования базы радиолокационных «портретов» взрывоопасных предметов.

При математическом моделировании электромагнитных откликов от объектов расположенных в почве, в том числе взрывоопасных предметов, нашли применение различные методы: метод интегральных уравнений; метод дискретных источников; метод конечных разностей во временной области. Из анализа указанных методов следует, что при решении задачи математического моделирования электромагнитных полей, рассеянных взрывоопасными предметами, предпочтительным является метод интегральных уравнений. Данный факт объясняется возможностью сведения граничной задачи в бесконечной области к интегральному уравнению по поверхности рассматриваемого объекта с учетом всех особенностей рассматриваемой граничной задачи. Метод интегральных уравнений позволяет моделировать отклики от взрывоопасных предметов произвольной формы и изготовленных из различных материалов в достаточно широком диапазоне частот, моделировать радиолокационные миноискатели, обеспечивающие передачу и прием волн не только в дальней, но и в ближней зоне. Метод позволяет учесть дисперсионные свойства различных типов почв, а также влажность и плотность почвы.

Проведенное моделирование частотных откликов пластиковой противопехотной мины DM11 является очередным шагом на пути создания базы радиолокационных «портретов» взрывоопасных предметов. Результаты, полученные в ходе моделирования, возможно использовать при создании алгоритмов обнаружения и идентификации взрывоопасных предметов. Это, в свою очередь, позволит наиболее полно реализовать возможности радиолокационного метода при создании дистанционных систем поиска взрывоопасных предметов, находящихся в толще укрывающих сред. Учет полученных результатов позволит повысить условную вероятность правильного обнаружения, что особенно актуально при разведке неметаллических взрывоопасных предметов (пластиковых или бескорпусных мин) и, как следствие, повысит эффективность предотвращения чрезвычайных ситуаций военного характера.

УДК 004.9
Ищенко В.Н., Щербак Г.В.

ЭКСПЕРТНАЯ СИСТЕМА ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Приведены результаты разработки системы поддержки принятия решений, используемой в задачах аудита корпоративных информационных систем на соответствие требованиям стандартов информационной безопасности.

В настоящее время информационная безопасность является одной из важнейших проблем современного информационного мира. Наряду с развитием информационных систем, актуальным является обеспечение необходимого уровня их защиты. Анализируя существующий спектр программных продуктов, применяемых для защиты информации, становится очевидным нехватка эффективных инструментов, которые позволяли бы провести комплексную диагностику, предоставить аргументированные выводы и рекомендации для повышения уровня информационной безопасности той или иной информационной системы.

Проблемы, связанные с безопасностью информационных систем следует рассматривать при помощи системного подхода. Известно, что информационная система, как и любая другая, подвергается влиянию внешних и внутренних факторов. В контексте информационной безопасности под факторами будем понимать потенциальные угрозы — воздействия, направленные на нарушение безопасности информационной системы. Во избежание нарушения безопасности системы следует систематически выявлять угрозы и принимать меры к их устранению. Исходя из этого, задача сводится к разработке экспертной системы поддержки принятия решений для аудита комплексной защиты информационной системы, а также выявления возможных угроз в области информационной безопасности.

Для практической реализации системы поддержки принятия решений была выбрана программная экспертная система CLIPS (C Language Integrated Production System), которая включает полноценный объектно-ориентированный язык COOL. CLIPS является широко используемой экспертной системой благодаря своему быстродействию, эффективности и отсутствию необходимости лицензирования.

Предлагаемая экспертная система «Expert Information Security System» (EISS), посредством анализа ответов на ряд задаваемых вопросов, предоставляет возможность лицу, принимающему решение выявить проблемы в информационной безопасности анализируемой системы. Преимуществом EISS является всесторонний анализ информационной системы: пути проникновения в систему, возможные пути раскрытия, сокрытия, модификации информации. Экспертная система указывает на актуальные угрозы, предлагает необходимые меры и методы достижения требуемого уровня информационной безопасности согласно действующим стандартам в сфере информационной безопасности. Анализ угроз проводится по семи уровням безопасности — физическому, сетевому, сетевых приложений, защиты ОС, защиты СУБД, защиты приложений и бизнес-процессов. Развернутые рекомендации даются по всем уязвимым уровням безопасности.

Разработанная экспертная система EISS апробирована в рамках комплексного обследования корпоративной информационной системы на соответствие требованиям стандартов ISO 17799: Code of Practice for Information Security Management и COBIT 3rd Edition. Рекомендации, предложенные EISS, были учтены и приняты меры по устранению угроз, что позволило достичь требуемого уровня информационной безопасности упомянутой корпоративной информационной системы.

УДК 621.396.96
Романюк В.А.

ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ И ГИС

Говоря простым языком, ГИС — это современная компьютерная технология для решения широкого круга задач — начиная с построения цифровых трехмерных карт и виртуального туризма и заканчивая задачами анализа объектов и событий, происходящих на нашей планете.

Иными словами, технология ГИС объединяет традиционные операции работы с базами данных, такими как запрос и статистический анализ, с преимуществами полноценной визуализации и географического (пространственного) анализа, которые предоставляет топографи-

ческая карта.

В контексте такого определения дистанционное зондирование местности является одним из поставщиков информации для практически любой географической информационной системы. С прикладной точки зрения системы дистанционного зондирования используются для обработки и анализа аэрокосмической информации, которая потом может использоваться в интересах различных служб. К таким задачам относятся оценка состояния окружающей среды, картографирование местности, выделение объектового состава местности (леса, озера, реки, дороги) и т.п. Отметим, что съемка Земли из космоса гораздо информативнее, чем используемая в настоящее время наземная информационная система.

Она дает возможность получать единовременную пространственную информацию с необходимым пространственно-временным разрешением и отображением поверхности Земли в спектральных диапазонах разных излучений. Это позволяет создавать различные образы земной поверхности, порой самые неожиданные для человека. Съемки Земли выполняются также и с самолета. Однако космические снимки по сравнению с аэроснимками имеют большую обзорность изображения, комплексное отображение компонентов геосферы, регулярную повторяемость, возможность получения информации для объектов, недоступных для изучения другими средствами. При съемке с высоты 250 км обзорность в 50 раз больше, чем при аэрофотосъемке, выполняемой с высоты 5 км. Один космический снимок в данном случае отображает такую же площадь, что и 10 тыс. аэроснимков. Это очень важно учитывать, когда возникает вопрос о выборе способа дистанционного зондирования и стоимости съемочных работ. Однако полученный объем информации требует значительных вычислительных затрат. В частности, по причине большого объема цифровых данных для обработки космических снимков на обычном персональном компьютере могут потребоваться сутки, в то время как обработка аэроснимков займет лишь несколько часов.

Для решения задач автоматической и автоматизированной обработки двухмерной цифровой информации в задачах дистанционного зондирования используют алгоритмы и методы компьютерного зрения. Среди способов решения задач в арсенале алгоритмов и методов машинного зрения представлены как монокулярные5 , так и бинокулярные6 подходы.

Методы монокулярного компьютерного зрения, как правило, используют для выделения на исходных или предобработанных изображениях объектов интереса, или, как их еще называют в задачах дистанционного зондирования, объектового состава. К объектовому составу относят города и населенные пункты, дороги, линии электропередач, леса, сельскохозяйственные угодья, озера, строения и т.п. Для решения этих задач обычно используются весьма сложные в математическом и вычислительном отношении методы машинного зрения. С помощью этих методов решают, в частности, задачи сегментации, или разделения изображения на зоны интереса, задачи классификации выделенных областей (например, определения того, что находится внутри выделенной области — лес, поле или озеро), задачи принятия решения об объектовом составе и многие другие. Методы бинокулярного компьютерного зрения используют для восстановления трехмерного рельефа местности, измерения на восстановленной поверхности и т.п. Раздел теории компьютерного зрения, решающий данные задачи, называется цифровой стереофотограмметрией.

К основным трудностям, возникающим у разработчиков систем дистанционного зондирования и ГИС, относятся наличие на аэрокосмических изображениях облаков, теней, зданий, изломов у крыш, солнечных бликов и ряда других факторов, которые помешали бы и человеку точно распознать анализируемую сцену, если бы он не делал свои выводы на основе каких-либо косвенных факторов и не обладал бы опытом в данной области. В таких случаях на помощь человеку приходят многозональные датчики. То, что вызывает нежелательные помехи в одном диапазоне, не мешает в другом. Например, затененные участки в видимом диапазоне легко опознать в инфракрасном, получив тем самым недостающую информацию и избежав ошибки.

Основными результатами работы алгоритмов компьютерного зрения в задачах дистанционного зондирования являются, как это уже стало ясно из всего вышесказанного, трехмер-

ные карты местности с восстановленными (методами машинного зрения) и размещенными на цифровых картах домами, дорогами, лесами, реками, озерами и т.п. Иными словами, в результате работы алгоритмов обработки и анализа изображений происходит перенос всего реального мира в область цифровых технологий.

Нетрудно догадаться, что в настоящее время ГИС — это многомиллионная индустрия, в которую вовлечены сотни тысяч людей во всем мире.

ГИС изучают в школах, колледжах и университетах. Эту технологию применяют практически во всех сферах человеческой деятельности — от анализа проблем перенаселения и мониторинга окружающей среды до решения частных задач, таких как выбор наилучшего маршрута, подбор оптимального расположения нового офиса, поиск дома по его адресу, прокладка трубопровода на местности, различные муниципальные задачи, задачи рекогносцировки на местности и т.п. Одной из основных целей, которая в недалеком будущем станет для нас повседневной реальностью и на которую направлены силы разработчиков, является построение глобальных трехмерных цифровых карт земной поверхности. Установив такую карту на обычный персональный компьютер, можно будет легко спланировать поездку, проложить туристический маршрут, предварительно пройдя сложные участки на компьютере или пролетев по маршруту на виртуальном летательном аппарате и совершив посадку в нужных местах. К карте будут прилагаться подсоединяемые к компьютеру стереоскопические очки с жидкокристаллическими затворами для визуализации трехмерной информации. С их помощью человек может погрузиться в виртуальный мир оцифрованной реальной местности, которая если и будет отличаться от настоящей, то только отсутствием людей, животных и звуков. Но, видимо, и это ненадолго.

С дальнейшим ростом процессов автоматизации технологий ГИС за компьютерным зрением закрепятся постоянные задачи, без которых уже сейчас не может обойтись ни одна современная справочно-измерительная система. Все дело в том, что современный мир меняется слишком быстро, карты и информация требуют постоянного уточнения, дополнения и обновления. Поэтому столь важна роль объединенных методов машинного зрения и цифровой фотограмметрии, позволяющих получить с помощью датчиков различной физической природы комплексную информацию.

УДК 335.351
Фик О.І.

МОДЕЛЮВАННЯ І ПРОГНОЗ ВЕКТОРА ПРАВОПОРУШЕНЬ У МЕГАПОЛІСІ ПРИ ВИРІШЕННІ ЗАДАЧ ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ ПІДРОЗДІЛАМИ МВС ПІД ЧАС ПЛАНУВАННЯ, ПІДГОТОВКИ ТА ПРОВЕДЕННЯ МІЖНАРОДНИХ СПОРТИВНИХ ЗМАГАНЬ

Розроблено методику моделювання вектора правопорушень для забезпечення можливості раціонального розподілу сил і засобів підрозділів і частин внутрішніх військ по найбільш важливих об'єктах і районам мегаполіса в ході виконання задач ОГП.

Відповідно до Закону внутрішні війська МВС України беруть “участь в охороні суспільного порядку і боротьбі зі злочинністю”. У сучасному мегаполісі обсяг служби для виконання таких задач перевершує можливості дислокованих у районі частин і підрозділів ВВ. Для забезпечення виконання задач при обмежених ресурсах необхідно передбачати очікувану кількість правопорушень (пограбувань, розбійних нападів, тяжких тілесних ушкоджень, крадіжок, убивств і ін.) за місцем та у часі, що дозволяє раціонально розподіляти сили і засоби по найбільш важливих об'єктах і районам міста. Кількість правопорушень по типах для кожного району мегаполіса відрізняється і може бути скорочено представлене у виді вектора, кожна компонента якого відповідає своєму типу правопорушень (грабежі, розбійні напади, тяжкі тілесні ушкодження, крадіжки, убивства й ін.).

Необхідний прогноз може бути виконаний за допомогою моделей, що дозволяють проро-

кувати кількість правопорушень по типах і районам мегаполіса на основі наявної інформації про різнорідні ознаки районів (загальна площа, щільність населення, кількість вокзалів, пляжів, банків, ресторанів, стадіонів, вулиць і т.п.). Кожен вид правопорушень визначається своєю ієрархічною послідовністю ознак. Ці ознаки непорівнянні по фізичному змісті (довжина вулиць і кількість осіб, засуджених з виправним терміном), по одиницях виміру і по абсолютній величині (площа району [200 км^2] і кількість кінотеатрів у районі [1 шт]).

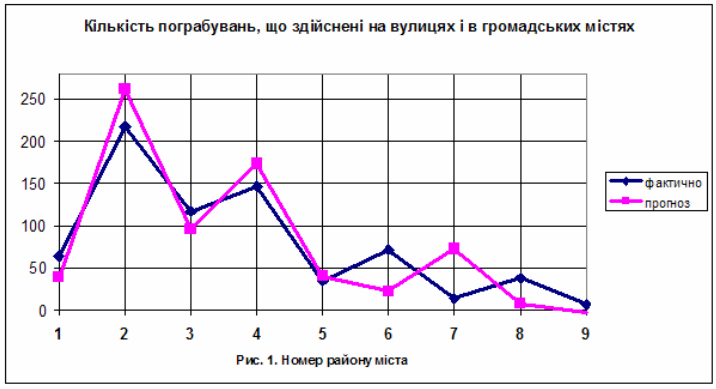
Кожна ознака має різний статистичний зв'язок з кількістю правопорушень відповідних типів. Для виявлення і виміру ступеня такого зв'язку може бути використаний математичний апарат багатофакторного дисперсійного аналізу, в основі якого лежить ідея виміру коефіцієнтів кореляції (r_{ij}) значень випадкових розмірів-ознак (x_j) багатомірних об'єктів. Процесу виміру коефіцієнтів кореляції необхідно передує перехід до центрованого і потім до нормованих значень досліджуваних ознак.

При незначному часі прогнозу зміни значень шуканих показників (кількість грабежів, крадіжок, убивств, розбійних нападів, тяжких тілесних ушкоджень, і ін.) може бути представлене в лінійному наближенні для кожного району мегаполіса:

$$\bar{y}_i = \sum_{j=1}^{n} r_{ij} \bar{x}_j + b_i \ ,$$

де i=1,…,m–номер компонента вектора правопорушень у даному районі (грабежі, розбійні напади, тяжкі тілесні ушкодження, крадіжки, убивства й ін.)

Перевірка працездатності моделі проведена на реальних даних одного з мегаполісів України. Результати перевірки для одного показника – кількості грабежів представлені на рис. 1 для всіх районів мегаполіса.



Отримана формульна схема моделювання вектору правопорушень дозволяє прогнозувати кількість різних правопорушень у залежності від динаміки показників районів міста і забезпечує можливість раціонального розподілу сил і засобів підрозділів і частин внутрішніх військ по найбільш важливих об'єктах і районам мегаполіса.

Надалі становить інтерес вибір системи найбільш важливих показників до здійснення протиправної діяльності, що дозволить перейти до розробки методики оптимізації варіантів застосування сил і засобів внутрішніх військ України для підвищення своєчасності чи попередження припинення правопорушень у мегаполісах України.

УДК 621.396

Алешин Г.В., **Сербин А.В.**

ОПТИМИЗАЦИЯ ПОДСИСТЕМЫ СИНХРОНИЗАЦИИ ПО УСЛОВНОМУ КРИТЕРИЮ ПОМЕХОУСТОЙЧИВОСТИ

Жесткие технические требования к цифровым системам связи на железнодорожном транспорте, в том числе технико-экономические, массо-технические, ресурсные ограничения приводят к необходимости, со стороны проектных учреждений, научно исследовательских институтов, заводов-изготовителей, модернизации или создания в большей степени оптимальных систем. Для того чтобы, например, сертифицировать модернизированные существующие или вновь создаваемые системы, необходимо сначала получить эталоны соответствующего качества. Как эталоны могут быть использованы результирующие оптимальные зависимости между показателями качества системы, которые получаются при решении задач

синтеза [1]. В этом случае будут рассматриваться функциональные зависимости между показателями качества подсистем. Научно-техническая задача синтеза данного класса подсистем ранее не решалась, а значит, представляет интерес для исследователей.

Практически на первом этапе можно ограничиться одним полезным и одним затратным показателем, которые считаются равноправными. Если показателей много, то далее следуют очередные этапы синтеза до полной адекватности и оптимальности модели эффективности системы. Модель эффективности для подсистемы синхронизации телекоммуникационных систем может быть представлена показателем срыва синхронизации (1) и затратным показателем, представляющем собою сумму цен (2) комплектующих функциональных элементов.

$$\min\ p_{ош} = 1 - [1 - p_1(q_1)][1 - p_2(q_2)], \tag{1}$$

$$C(q_1) + C(q_2) = C, \tag{2}$$

где $p_1(q_1)$ и $p_2(q_2)$ - соответственно вероятности срыва генераторного оборудования за счет сбоя дешифратора цикловой синхронизации и срыва за счет тактовой синхронизации, q_1, q_2 - соответственно отношение сигнал/шум в канале дешифратора и в канале тактовой частоты.

Если в канале связи действует «белый шум», тогда, в частности, для систем PDH E1

$$p_1(q_1) = 1 - (1 - p_{ber}(q_1))^7 = 1 - \left(1 - \left(1 - \mathrm{erf}\left(\frac{\sqrt{q_1}}{2\sqrt{2}}\right)\right)\right)^7, \tag{3}$$

$$p_2(q_2) = 1 - \mathrm{erf}(\pi\alpha\sqrt{2q_2}), \tag{4}$$

где α – параметр который показывает смещение значащих моментов цифровой последовательности от идеального положения.

Собрав, технико-экономическую статистику, для рассматриваемых функциональных элементов и сглаживая последнюю (методом наименьших квадратов) получаем функциональную связь между C (затратный показатель) и q_1, q_2. Аналитически, последняя имеет вид:

$$C\left(\frac{1}{q_1}, \frac{1}{q_2}\right) = 411{,}3 + \frac{3}{20 \cdot \left(\frac{1}{q_1}\right)^3} + \frac{0{,}019}{\left(\frac{1}{q_2}\right)} \tag{5}$$

Таким образом, имеем упрощенную задачу нелинейного программирования

$$\min p_{ош} = \min_{\{q1,q2\}}\left(1 - \mathrm{erf}^7\left(\frac{\sqrt{q_1}}{2\sqrt{2}}\right)\mathrm{erf}(\sqrt{2\pi}\alpha\sqrt{q_2})\right), \tag{6}$$

при

$$C\left(\frac{1}{q_1}, \frac{1}{q_2}\right) = 411{,}3 + \frac{3}{20 \cdot \left(\frac{1}{q_1}\right)^3} + \frac{0{,}019}{\left(\frac{1}{q_2}\right)} \tag{7}$$

Решая задачу (6)-(7) известными методами (метод множителей Лагранжа) и варьируя затратным показателем получаем оптимальные зависимости (т. н. «кривые обмена») между $p_{ош}$ и C при различных α.

«Кривые обмена» являются, по существу, эталонами качества для всего диапазона показателей качества подсистем. Если использовать какой-либо критерий близости показателей качества реальных подсистем к кривым обмена при тех же ассигнованиях, что и для реальных подсистем, то это дает возможность их оценки качества для всего диапазона ассигнований.

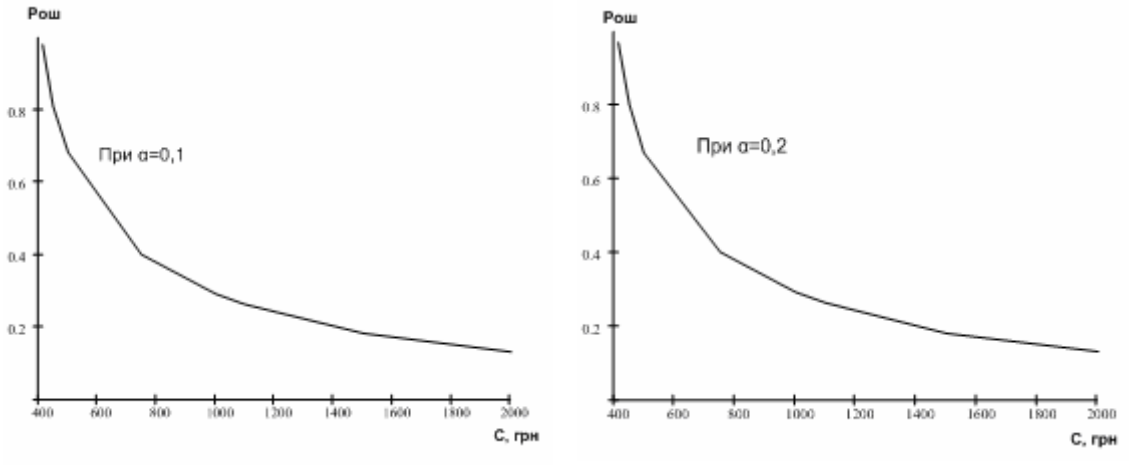


Рис.1. Оптимальные зависимости для $P_{ош}$ при ограничении С

В перспективе, задача (6)-(7) усложняется (учитываются модели других функциональных элементов подсистемы, а также составляются соответствующие технико-экономические ограничения) и вновь решается задача математического программирования. Процесс продолжается до верхней границы реализуемости решения (учитывая, при этом, известный принцип У. Оккама т.н. «бритва Оккама»).

Список использованных источников

1. Альошин Г. В. Оцінка якості інформаційно-вимірювальних систем/ Г.В. Альошин – Х.: 2008.– 294 с.

УДК 681.3

Карасюк В.В., Кобзев В.Г.

ОНТОЛОГИЧЕСКОЕ ОПИСАНИЕ БАЗЫ ЗНАНИЙ ДЛЯ ОБУЧЕНИЯ В ПРАВОВЕДЕНИИ

Технологическими предпосылками недостаточной информатизации правовой сферы являются: большие объемы юридической информации, которые используются на практике; структурные особенности используемой юридической информации; сложность процессов обработки юридической информации и, соответственно, отсутствие эффективных программных инструментов. Каждый нормативный акт должен иметь необходимые реквизиты, которые отражали бы его юридическую силу, предмет регулирования, сферу действия, придавали бы ему официальность. Традиционными достоинствами языка права являются четкость, краткость, определенность, стереотипность, единообразие, его сухость, доступность для понимания.

В то же время особенности обработки правовой информацией позволяют сформулировать задачу разработки знаниеориентированной обучающе-консультационной системы для области правоведения на новых интеллектуальных основах представления правовой информации..

1. Концептуализация знаний

Классические модели баз данных – сетевые, иерархические и реляционные лишь частично могут обеспечить требования по сохранению и обработке элементов данных [1]. Особенностью таких систем хранения является распределенный характер просмотра и внесения изменений в соответствующую базу. Поэтому более перспективным направлением для решения задач обработки правовых данных является использование баз знаний. Среди моделей искусственного интеллекта для работы с правовой информацией наиболее подходящими является фреймовая модель знаний. Классическое представление фреймов позволяет использовать фреймовые модели в практических задачах представления различных предметных областей.

Современной реализацией фреймовой модели являются онтологические системы. Онтология представляет собой знания, представленные на базе концептуализации. Концептуализация допускает описание множества объектов и понятий, знаний о них и связей между ними. То есть онтологией является эксплицитная спецификация концептуализации. Формально онтология состоит из терминов, организованных в таксономию, их определений и атрибутов, а также связанных с ними аксиом и правил вывода:

$$O = \langle X, R, \Phi \rangle,$$

где X - конечное множество концептов (понятий, терминов); R - конечное множество отношений между элементами X, Φ - конечное множество функций интерпретации, которые заданы на концептах и/или отношениях онтологии O. Для целей данного исследования множества X и R расширяются в процессе наполнения онтологии, а множество Φ - пустое. Основным преимуществом онтологического представления по сравнению с базами данных есть возможность построения иерархии классов. Эффективность адаптации онтологии базы знаний к особенностям предметной области определяют заложенные в ее структуру элементы и механизмы оптимизации во время эксплуатации. В связи с этим актуальным является вопрос о сравнении разнотипных объектов, то есть определении их семантического подобия – функции, принципиально не существующей в базах данных [2]. В работе предлагается использовать данный подход в задаче создания информационной обучающе-консультационной системы.

2. Модель базы знаний

В обобщенном представлении база знаний опирается на структуру базы данных, которая представлена на рис 1. Основным источником знания является исходный (учебный) текст, который обрабатывается в системе (на сегодняшний день – автоматизировано, в перспективе – автоматически). Из текста выделяются понятия (концепты X) с их словесным представлением и определяются связи (отношения R) между группами понятий. Далее выделяются использования в тексте существующих понятий, связок и связей [3].

Так как текст в базе данных представлен в виде набора предложений, при этом каждое может быть отнесено к соответствующему разделу (для структурного представления при прочтении), то механизм заполнения базы данных можно представить такой последовательностью:

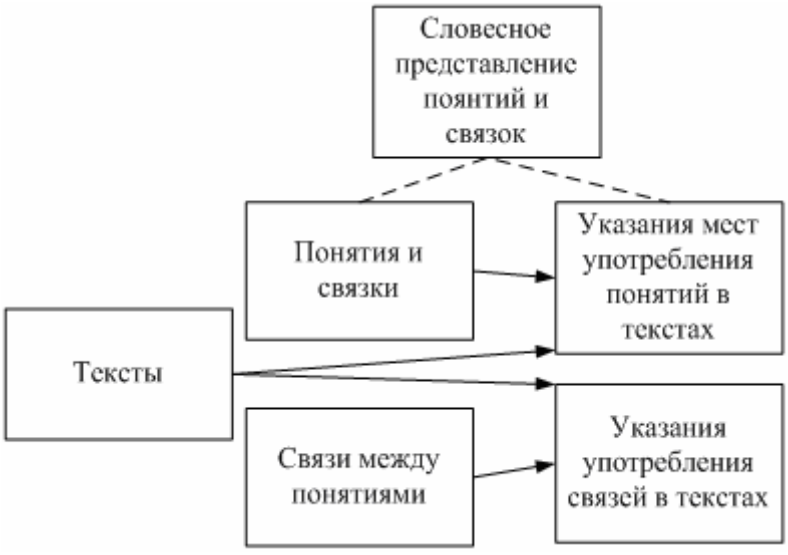


Рис 1. Структура БД с точки зрения технологии ее заполнения

- выбор нового (не обработанного предложения);
- автоматический поиск употребления понятий и связок в предложении на основе существующего их словесного представления в базе;
- проверка экспертом полноты и качества автоматического поиска с исправлением ошибок (каждому слову в предложении может быть поставлено в соответствие понятие или связка, в то же время одному понятию может соответствовать группа слов);
- добавление недостающих для полного разбора предложения понятий и связок, а также их словесного представления;
- на основе найденных употреблений понятий выявляются связи между ними, которые записываются экспертом в базу (привязывая эти связи к разбираемому предложению в его ори-

гинальной записи);

- отметка предложения как обработанного и переход к следующему.

Из изложенного можно сделать вывод, что, в общем, на данном этапе, есть два существенно разнящиеся направления работы:

- добавление понятий и связей между ними;
- указание привязок понятий и связей к тексту.

Также стоит отметить, что для усовершенствования базы данных необходимо будет осуществлять повторные проходы с выявлением новых связей после расширения круга интересующих нас понятий.

3. Выводы и перспективы

Работа любого юриста, занимающегося правотворческой, правоприменительной, консультационной или иной деятельностью — это всегда работа с информацией, с юридическими документами.

В результате проведенных исследований в направлении реализации онтологических принципов построения знание-ориентированной обучающе-консультационной системы сформированы структура базы данных, которая реализует базу знаний, принципы построения программного комплекса, спроектированы интерфейсные формы и разработаны программные модули подсистем эксперта и пользователя.

В настоящее время нарабатывается опыт эксплуатации системы и выдвигаются требования относительно дальнейшей разработки новых возможностей. Перспективными направлениями считаются: сравнение онтологий для оценки полноты и непротиворечивости информации в базе, которая создана различными пользователями; использование системы в юридической клинике для предоставления консультационных услуг через интернет-портал без участия эксперта.

Список использованных источников

1. Гаврилова Т.А., Хорошевский В.Ф. Базы знаний интеллектуальных систем / Учебник для вузов. – СПб.: Изд-во “Питер”, 2000. - 334 с.

2. Литвин В.В. Метод оцінювання подібності документів, доповнених контекстом з онтології // Вісник Національного університету «Львівська політехніка» «Інформаційні системи та мережі», №610, 2008. с.191 – 196.

3. Tatsyi, V. Семантическая сеть знаний в правоведении = Semantic network of knowledge in science of law / V. Tatsyi, A.Getman,, S. Ivanov, V. Karasiuk, O. Lugoviy, O. Sokolov // Автоматика, управление и информационные технологи: Труды IASTED Международной конференции = Automation, Control, and Information Technology (ACIT 2010): Proceedings of the IASTED International Conference on Automation, Control, and Information Technology, held June 15 – 18 2010 in Novosibirsk, Russia / The International Association of Science and Technology for Development. – Anaheim, USA, Calgary, Canada, Zurich, Switzerland: ACTA Press 2010. p. 218 – 222.

Белокурський Ю.П., **Лишенко В.В.**, **Щербіна О.О**.

ДОСЛІДЖЕННЯ ІМПРОВІЗОВАНИХ ДІАГРАМОУТВОРЮВАЮЧИХ ПРИСТРОЇВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

У доповіді наведено результати моделювання і вимірювання імпровізованих антен і екранів. Показані характеристики пристроїв і можливості застосування для захисту інформації в інтересах ВВ МВС України

Засоби обробки інформації, електронні носії інформації схильні до поразки від впливів статичних розрядів, НВЧ випромінювання при експлуатації, зберіганні, транспортуванні. Навіть тимчасова втрата інформації може призвести до зриву термінів прийняття рішення і виконання завдання. Слід вказати, що носії типу «флеш» можуть бути уражені ви-

промінюванням джаммерів стільникового зв'язку або засобами контролю типу «нелінійний локатор».

Сучасні матеріали і технології дозволяють створювати легкі екрани, діаграмоутворюваючі пристрої стаціонарного та мобільного (одноразового) застосування для радіомаскування, захисту від витоку та навмисного силового впливу. Такі пристрої можуть мати форму прямокутних (циліндричних) замкнутих і охоплюючих екранів, кутових і циліндричних відбивачів на дротяних каркасах. Можлива реалізація пневматичних конструкцій з гнучких матеріалів. Такі пристої надають можливість підсилювати захисні можливості інформаційного обладнання, існує необхідність визначення їх характеристик.

Наведено результати моделювання і вимірювання діаграм спрямованості імпровізованіх діаграмоутворюваючіх прістроїв у наближенні прямокутних і конічних рупорних антен, кутових і параболічних екранів (відбивачів) в діапазонах частот витоку і ураження. Моделювалися діаграми в залежності від розмірів імпровізованих пристроїв і відхилення від ідеальної форми (прямокутної, конічної, параболічного циліндра). Виміри проводилися методом вільного простору. Обговорюються також результати та методика випробувань захисних властивостей екранів з металізованої лавсанової плівки від статичних розрядів. Випробування проводились для контактного і повітряного розряду з енергією розряду W = 0,01-0,2 Дж. Середньоквадратична похибка визначення енергії в межах 10%.

Руженцев І.В., Федцова А.С., **Широковська А.С.**

ВИКОРИСТАННЯ НОВИХ МАТЕРІАЛІВ І ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Представлений огляд характеристик сучасних матеріалів і технологій для забезпечення захисту інформації та ресурсів від витоку і навмисних зовнішніх впливів. Розглянуто результати моделювання дефектів сполук матеріалів та вимірювання коеффіцієнтів екранування.

Для пасивного захисту від несанкціонованого доступу до інформації по різних каналах витоку останні роки застосовуються фольга і фольговані матеріали, поглинаючи і металізовані тканини. Для комплексного екрану-вання приміщень також застосовують фольговані тепло і звукоізоляційні матеріали. Матеріали з'єднуються склеюванням, зшиванням, використо-вується скотч-фольга та фальцеві з'єднання. У доповіді представлено огляд характеристик сучасних матеріалів і технологій захисту інформації, ресур-сів від витоку і навмисних зовнішніх впливів. Деякі виробники вказують типові амплітудно-частотні характеристики матеріалів, отримані за резуль-татами вимірювань у закритому коаксіальному осередку. Для проектуван-ня необхідні кількісні характеристики матеріалів і дефектів швів, отримані методами вільного простору при різних поляризаціях падаючої хвилі. Для екранованного приміщеннями "слабкими місцями" є дверний і віконний прорізи. Застосування екрануючих штор на дверному і віконному прорізах не дозволяють отримати необхідний рівень захисту. Штори з непрозорих металізованих тканин або ламінованих фольгових матеріалів потрібно поєднувати з екраном. Розглянуто кріплення “під фальцевий” шов. Наведено результати моделювання і вимірювання дефектів фальцевих сполук ламінованих фольгових матеріалів з одинарним і подвійним стоячим фальцем. Виміри проводилися методом вільного простору на моделі віконного прорізу зменшених розмірів. За ступенем ослаблення електромагнітної енергії модель екранованого приміщення належить до 3 класу (30-60дБ). Макет-модель екранованого приміщення перевірялась на наявність резонансів для типа хвилі H_{10} .В основу методики калібрування вимірювальної антени, вибору схеми вимірювання та обладнання покладені загальноприйняті рекомендації. Невизначеність вимірів оцінюється значенням 5-7д.

УДК 621.396

Альошин Г. В., Бойко Д. О.

ОЦІНКА ВПЛИВУ ПОХИБКИ ФАЗОВОЇ СИНХРОНІЗАЦІЇ НА ЯКІСТЬ ФАПЧ

Одна з кращих структур фазового автопідстроювання частоти (ФАПЧ) [1] (рис.1), що містить попередній підсилювач проміжної частоти (ППЧ) і синхронний детектор, має свої переваги у завадостійкості за рахунок використання синхронного детектору і ППЧ. Проте ця структура характеризується погіршенням стійкості за рахунок використання ППЧ, а також через вплив нестабільності фази ФАПЧ на нестабільність амплітуди, що у свою чергу впливає на нестабільність фази.

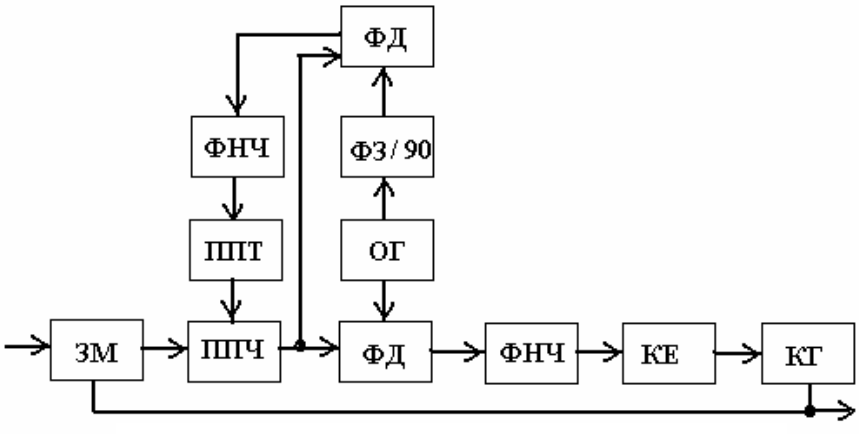


Рис. 1. ФАПЧ з підсилювачем та схемою АРП

На рис.1 позначено: ЗМ – змішувач, ППЧ – підсилювач проміжної частоти, ФД - фазовий детектор, ФНЧ – фільтр низької частоти, КЕ – керуючий елемент, КГ – керований генератор, ОГ – опорний генератор, ФЗ - фазозсувач, ППТ – підсилювач постійного току.

Відомо, що когерентність сигналу доцільно використовувати у всіх випадках для боротьби з ортогональною складовою (по відношенню до фази сигналу) вузькосмугової завади. За рахунок цього можна збільшити відношення сигнал/шум. Але у випадку використання синхронного детектору для АРП ППЧ системи ФАПЧ це може сприяти зменшенню стабільності роботи ФАПЧ.

При оцінюванні впливу похибки синхронізації в системі ФАПЧ на середню амплітуду синхронного детектору допустимо, що похибка ФАПЧ невелика, тоді детекторну характеристику синхронного детектору навколо точної настройки ФАПЧ за фазою можна розкласти у ряд Тейлора з точністю 10%

$$u(\varphi)=U\cos\varphi \approx U(1-\varphi^2/2+\varphi^4/4!-...) \approx U(1-\varphi^2/2) \approx U\exp(-\frac{\varphi^2}{2}), \quad (1)$$

де U – максимальне значення напруги, φ - різниця фаз прийнятого та опорного сигналів.

Похибка ФАПЧ при відношенні потужностей сигналу до шуму більше 5 (q > 5) згідно [1] має практично нормальний розподіл ймовірності, що обумовлено вузькою смугою утримання та дією декількох рівномірних факторів.

У режимі автосупроводження сигналу за фазою природно, що дисперсія флуктуацій повинна бути менше π, що відповідає півперіоду сигналу. Для цього випадку в межах максимуму доброю апроксимацією характеристики синхронного детектору, тобто, з тією ж точністю, може бути закон:

$$G = \frac{u(\varphi)}{U} = \exp(-\frac{\varphi^2}{2}), \quad (2)$$

оскільки справедлива рівність (1) у першому наближенні.

Цей ефект з точністю до позначень співпадає з ефектом нормальних флуктуацій діаграми спрямованості антени з майже гаусовою діаграмою спрямованості [2], а щільність розподілу ймовірності відносного рівня сигналу можна визначити за допомогою виразу:

$$p(G) = \sqrt{\alpha/\pi}\,\frac{G^{\alpha-1}}{\sqrt{\ln\frac{1}{G}}}, \quad (3)$$

де $\alpha = 1/D_x$.; D_x – дисперсія шумової складової похибки ФАПЧ.

Сімейство $\rho(\alpha, G)$ представлене на рис.2,а. Звідси математичне сподівання відносного рівня сигналу дорівнює:

$$M[G] = \sqrt{\frac{\alpha}{\alpha + 1}}, \tag{4}$$

а n-й початковий момент:

$$M[G^n] = \sqrt{\frac{\alpha}{\alpha + n}}. \tag{5}$$

Залежності M[G] і $M[G^2]$ представлені на рис.2,б.

Стосовно енергетичних втрат слід зазначити, що принцип синхронного детектування зменшує середній рівень шуму у $\sqrt{2}$ рази, але для цього потрібне синхронне детектування з його нестабільністю фази, що вже зменшує рівень сигналу на виході фазового детектору згідно виразам (4,5) та рис.2,б. При нестабільності 0,5 радіан виграшу може не бути, проте це найгірша робота.

З виразів (4,5), а також з рис.2,б видно, що врахування зменшення відносної амплітуди за рахунок фазової похибки доцільний вже при $\alpha \le 8$, а при $\alpha \approx 1$ він просто необхідний, оскільки при $\alpha = 8$ середні енергетичні втрати складають 10%, а при $\alpha = 1$ - 50%. Очевидно, що

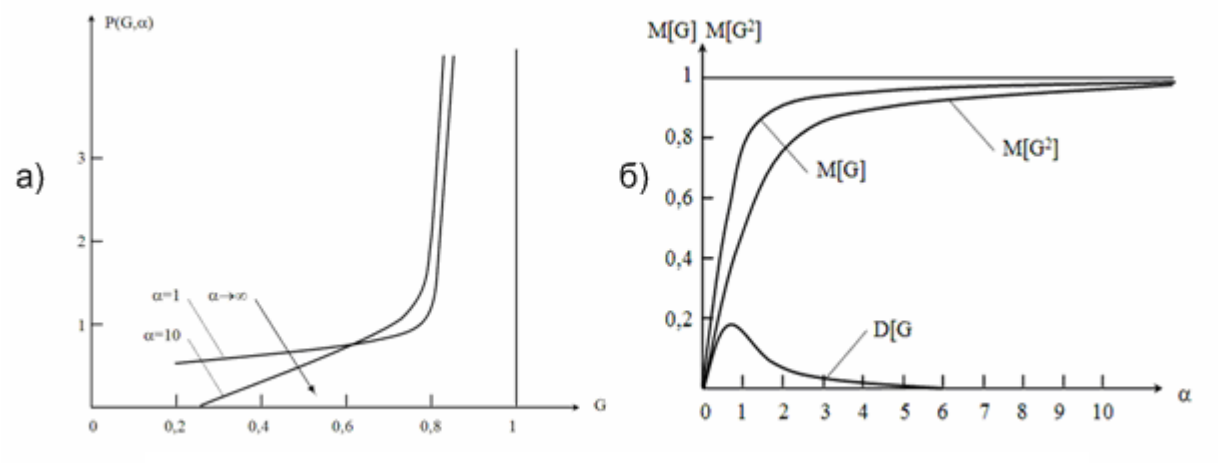


Рис. 2. Графічні залежності: а) щільність розподілу рівня сигналу;
б) математичне сподівання рівнів сигналу

із зменшенням α зростає роль мультиплікативної завади АРП за рахунок флуктуацій фази ФАПЧ, що має розподіл (3), обумовлений формами розподілу флуктуацій фази і характеристики синхронного детектору.

У роботі [2] доведено, що вплив допустимої нестабільності амплітуди сигналу для системи ФАПЧ не повинна перевищувати відношенню шум/сигнал.

$$G = \frac{u}{U} \le \frac{1}{q}. \tag{6}$$

Це умова, за якою похибка системи ФАПЧ, що обумовлена нестабільністю амплітуди, не перевищує флуктуаційну похибку. Якщо нам потрібна високоточна система, то треба відповідно стабілізувати амплітуду сигналу Наприклад, якщо потрібна середня флуктуаційна похибка ФАПЧ у 5^0, то відносна нестабільність повинна бути меншою за 1/36.

Таким чином, виникає ситуація, коли за рахунок завади фаза керованого генератору зменшується. Тоді за рахунок синхронного детектору зменшиться напруга на його виході. Зменшення напруги сигналу на вході фазового детектору призведе до наступного додаткового зменшення фази на його виході. Можливий зрив синхронізму. Тобто, АРП при наявності

синхронного детектору зменшує стійкість ФАПЧ. Потрібен або амплітудний детектор і відказатись від виграшу у боротьбі з завадою, або синхронний детектор і ускладнена боротьба за стійкість ФАПЧ.

Без врахування оцінок нестабільностей амплітуди та флуктуаційної складової фази сигналу керованого генератору і без мір до підвищення стійкості не можна отримати значний виграш у відношенні потужностей сигнал/завада при використанні синхронного детектування в системі ФАПЧ з підсиленням.

Список використаних джерел

1. Тузов Г.И. Выделение и обработка информации в допплеровских системах. «Сов. Радио», 1967.

2. Альошин Г.В. Оцінка якості інформаційно-вимірювальних систем. Х.,УкрДАЗТ, 2008, 288 с.

Захаров В.М., Коваленко О.В., Москалец М.В.

ГЕОІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПЛАНУВАННЯ ЗВ'ЯЗКУ ТА РОЗМІЩЕННЯ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Обговорюються питання використання програми Radio Mobile для оптимізації розміщення засобів зв'язку і РЕБ підрозділів ВВ МВС України в операційному районі.

Вибір позиції для розміщення засобів зв'язку і РЕБ проводиться з урахуванням умов забезпечення максимальних можливостей; по виявленню, пеленгування та придушенню ліній радіозв'язку протиборчої сторони; стійкості зв'язку своїх підрозділів; електромагнітної сумісності (ЕМС) із засобами зв'язку та РЕБ угруповання (підрозділів) внутрішніх військ; забезпечення скритності від засобів розвідки, живучості станції завад в умовах вогневого і діверсійного впливу. При виборі місця розгортання станції завад існують обмеження: на площині радіусом 200-300 м місцевість повинна бути відкритою і, по можливості, рівною ; в радіусі до 100 м місцевість повинна бути вільною від перевиромінювачів (металевих огорож, антен і проводів, споруд і будівель); місце установки повинно бути віддалене від електрифікованих залізниць і високовольтних ліній, магістральних шосе, летовищ, від одноповерхових будівель з металевим дахом і лісових масивів. З метою захисту станції завад від засобів розвідки противника вибір позиції потрібно з ураховувати маскувальні властивості місцевості.

Оптимальність розміщення також вимагає прогнозування (розрахунку) трас і зон доступності. У більшості програмних комплексів реалізовані моделі та методики прогнозування розповсюдження радіохвиль, засновані на рекомендаціях МСЕ: Р.1812 «Метод прогнозування поширення сигналу на конкретній трасі для наземних служб" з пункту в зону "в діапазонах УВЧ і НВЧ»; Р.1546-3 « Метод прогнозування для трас "точка-зона" для наземних служб в діапазоні частот від 30 МГц до 3000 МГц »; Р.526-10 -« Поширення радіохвиль за рахунок дифракції »в частині п.3 «Дифракція над сферичної Землею».

У доповіді розглянуті можливості програми Radio Mobile. Це програма моделювання розповсюдження радіохвиль в діапазоні частот від 20 МГц до 20 ГГц. За основу розрахункової частини програми прийнята модель розповсюдження радіохвиль Лонглі-Райса. Вона надає можливість створювати карти конкретних районів, використовуючи введені в пам'ять дані GOOGLeath, з подальшим додаванням рельєфу місцевості і доріг. Потім у вибраних місцях установливают радіозасоби. Всі радіоканали між станціями можна проаналізувати з точки зору профілю траси і параметрів сигналу. При необхідності для кожної окремої станції можна визначити зону досяжності. Можна визначити Best Sites (найкраще місцерозта-шування), щоб забезпечити зони охоплення для кількох конкретних станцій. Функцією Route Radio Coverage можна відтворити характеристики станції, яка переміщається по певному маршруту на карті. Можна вибрати Best Unit (кращу станцію) з максимальним рівнем сигналу в зада-

ному місці. У версії 8.3.2 з'явилася нова функція - "схема найгірший варіант", на якій відображається найбільш несприятливий рівень для двостороннього сигналу. Ця функція представляє особливий інтерес при аналізі функці-ональних характеристик ретранслятора для малопотужної мобільної станції і побудові комунікаційної області. Якщо типові (бібліотечні) форми діаграм спрямованості антен не відповідають потребам, то є три електрон-ні таблиці, які надають можливість вводити діаграми спрямованості для конкретних антен. Програма Radio Mobile діє з використанням 4 різних систем координат: широта і довгота, завжди використовуються за замовчуванням, радіолокаційних системах Maidenhead або QRA; військова система координат (MGRS); універсальна поперечна проекція Меркатора (UTM). Система MGRS заснована на системі UTM .Программа спочатку за замовчуванням використовує широту і довготу, а також систему QRA (Maidenhead). Загасання сигналу при розповсюдженні радіохвилі між двома пунктами, що знаходяться на лінії прямої видимості, розглядається як «загасання у вільному просторі». Програма використовує наступні параметри для створення карт з відображенням зон впевненого прийому: місце розташування передавача, вихідна потужність передавача, частота, тип антени, діаграмма спрямованості антени, коефіцієнт підсилення, загасання в лінії, включаючи фільтри та багатоканальн ірозгалужувачі.

Дані про місцевість і висотах. Програма використовує дані висот місцевості з баз даних SRTM або DTED, які вільно доступні в Інтернеті. Є також і інші формати даних по висотах, але найчастіше використовуються вище зазначені бази даних. Програма створює кольорову схему зони охоплення однієї або декількох базових станцій з показом передбачуваних рівнів прийнятих сигналів. Рівні сигналів відображаються з використанням одиниць вимірювання, що визначаються користувачем. Існує можливість об'єднувати карту із зображенням зони охоплення з дорожньою або будь-якою іншою географічною картою, створена схема може використовуватися для швидкого визначення можливості комунікацій з конкретних місць розташування. Недоліком є необхідність підключення до Інтернету при використанні Googl ресурсів. При «автономному» обчисленні траси і зони доступності попередньо завантажують дані цифрових карт операційного району. Всі значення параметрів визначаються в метричній системі.

Програма може бути використана для навчального та реального планування роміщення засобів зв'язку і РЕБ при забезпеченні операцій підрозділів ВВ МВС України.

УДК 796.011.3 - 796.8

Хацаюк О.В.

РОЗРОБКА ТА АПРОБАЦІЯ СУЧАСНОЇ ТЕХНОЛОГІЇ УДОСКОНАЛЕННЯ ТЕХНІКИ РУКОПАШНОГО БОЮ ПРАВООХОРОНЦІВ МВС УКРАЇНИ

Аналіз структури професійної діяльності представників правоохоронних органів під час застосування заходів фізичного впливу в процесі СБД свідчить про те, що для кожного співробітника у відповідності до його функціонального стану існує одна оптимальна модель технічних дій рукопашного бою, яка забезпечує максимальну реалізацію рухового потенціалу. Але при втомі, на фоні значних психофізичних навантаженнях навіть у висококваліфікованих правоохоронців, суб’єктивна оцінка виконання технічних дій РБ значно знижується. В свою чергу відсутність універсальної методики, яка своєчасно дозволяє отримувати об’єктивну термінову інформацію про техніку даного єдиноборства, сповільнює процес навчання і удосконалення навичок рукопашного бою.

В ході попереднього педагогічного експерименту, нами були отримані дані про кінематичні параметри техніки рукопашного бою, які дозволили створити уявлення про біомеханічні особливості досліджуваного єдиноборства працівників МВС України різної кваліфікації. Аналіз результатів цих досліджень дозволив нам встановити специфічні закономірності формування технічної майстерності у рукопашному бою та визначити шляхи підвищення рівня

технічної майстерності.

Для підвищення ефективності навчально – тренувального процесу, нами було розроблено технологію удосконалення технічної майстерності курсантів АВВ з рукопашного бою із використанням сучасних засобів термінової інформації яка в себе включала наступні блоки: блок №1 (удосконалення стійки, прийомів самострахування, акробатичних вправ; удосконалення техніки прийомів бою без зброї, прийомів нападу; удосконалення техніки звільнення від захватів, кидкової техніки РБ); блок №2 (удосконалення прийомів бою зі зброєю, спеціальних прийомів РБ; удосконалення техніки рукопашного бою правоохоронців в різних умовах службово – бойової діяльності).

З метою удосконалення ударної техніки рукопашного бою нами використовувався апаратно – програмний комплекс реєстрації ударних зусиль техніки єдиноборств «Katsumoto». Даний комплекс призначений для вимірювання біомеханічних показників техніки ударів рукопашного бою, бойового самбо, універсального бою та інших єдиноборств.

АПК дозволяє швидко, точно і достовірно проводити вимірювання сили удару, швидкості ударних зусиль, швидкості реакції тих, що навчаються правоохоронців, спортсменів на світловий та звуковий подразники.

Основний педагогічний експеримент проводився на базі кафедри фізичної підготовки та спорту Академії ВВ МВС України під час навчально – тренувальних занять зі спеціальної фізичної підготовки упродовж 2006 – 2011 р.р. Досліджувані курсанти Академії ВВ МВС України були розподілені на контрольну (КГ n=90чол.) та експериментальну (ЕГ n=90 чол.) групи.

До початку педагогічного експерименту курсанти – правоохоронці не мали спортивних розрядів та звань з єдиноборств, але володіли елементарними прийомами рукопашного бою в обсязі програми для курсантів та слухачів 1 курсу (РБ – 1). Вік досліджуваних 17 – 26 років.

Всі навчально – тренувальні та контрольні заняття з рукопашного бою проводилися лише після стандартної підготовчої частини заняття зі спеціальної фізичної підготовки. Рівень технічних результатів у КГ та ЕГ перед початком експерименту за критерієм Ст'юдента статистично вірогідно не відрізнявся ($P>0,05$).

Аналіз варіативності провідних параметрів техніки рукопашного бою показав, що на етапі поглибленої спеціалізації настає момент, коли навички техніки вже сформувалися і без подальшого цілеспрямованого удосконалення зростання професійної майстерності значно сповільнюється. Тому, саме на цьому етапі з’являються передумови оптимізації рухових дій РБ із використанням технічних засобів навчання.

Розроблена нами модель удосконалення технічної майстерності правоохоронців МВС України з рукопашного бою із використанням сучасних засобів термінової інформації дозволила вирішити такі навчально-тренувальні завдання: удосконалення техніки виконання прийомів і способів самострахування, ударної техніки, кидкової техніки, техніки захисту від неозброєного противника; удосконалення техніки виконання больових прийомів, прийомів задушення, та техніки захисту від озброєного противника; удосконалення прийомів обшуку, способів зв’язування, одягання наручників та конвоювання. Реалізація зазначених завдань забезпечила досягнення головної мети навчально-тренувального процесу – достовірно збільшити рівень технічної підготовленості з рукопашного бою правоохоронців системи МВС України та підвищити рівень їх бойової готовності.

Оптимізація навиків рукопашного бою у напрямку найбільш ефективного їх застосування в процесі СБД працівників органів внутрішніх справ України свідчила про зростання технічної майстерності у курсантів – правоохоронців ЕГ.

Порівняння показників технічної підготовленості з рукопашного бою у контрольній та експериментальній групах показало високу ефективність розробленої нами моделі. Разом з цим, підвищення рівня функціональних можливостей у спортсменів експериментальної групи свідчило про ефективну реалізацію принципу поєднання удосконалення техніки та розвитку рухових якостей.

Таким чином, акцентоване комплексне застосування СТЗН у процесі удосконалення технічної майстерності правоохоронців МВС України з рукопашного бою дозволяє оптимізувати всі необхідні складові у різних варіативних ситуаціях двоборства, що забезпечило статистично достовірне підвищення рівня професійної майстерності ($P<0,05$).

УДК 621.396
Лаврут О.О., Стрюк О.Ю.

ОПИСАНИЕ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ В ВИДЕ ОДНОПРОДУКТОВОЙ ТЕНЗОРНОЙ МОДЕЛИ

На данном этапе совершенствование методов и способов вооруженной борьбы, оснащение войск связи высокоэффективными образцами техники связи, использующими современные информационные и телекоммуникационные технологии существенно повышают роль систем военной связи и автоматизации при ведении боевых действий на современном поле боя.

Как в мирное время, так и в особый период Вооруженные Силы не могут существовать без надежной системы управления. Строительством и совершенствованием технической основы системы управления Вооруженных Сил Украины занимаются войска связи.

Высокий уровень информационного обеспечения боевых действий становится определяющим фактором достижения превосходства над противником. Этот факт объясняет стремление ведущих мировых держав к достижению именно информационного превосходства над противником, так как очевидным становится и то, что невозможно дальнейшее усиление военной мощи только за счет наращивания войск и вооружения. Все это обуславливает необходимость ведения боевых действий в едином информационном пространстве, что существенно повышает эффективность применения вооруженных сил за счет использования передовых технологий.

Перевод системы связи и автоматизации Вооруженных Сил Украины на современные цифровые технологии и телекоммуникационное оборудование, разработка и внедрение перспективных комплексов средств автоматизации являются актуальными направлениями военного строительства, от решения которых будет зависеть боевая готовность и эффективность применения Вооруженных Сил Украины, а также обороноспособность государства в целом. Учитывая этот факт на данном этапе большое внимание уделяется созданию полевой компоненты системы связи Вооруженных Сил Украины.

Для всестороннего описания полевой компоненты телекоммуникационной системы необходимо применять современные модели и методы. Тензорный анализ, благодаря заложенным в него возможностям, есть логическим способом описания реальных объектов в их многоаспектности и противоречивости. Тензорное представление имеет максимальную целостность, позволяя сконцентрировать основное внимание на самой системе независимо от возможных аспектов ее рассмотрения.

В докладе рассмотрено описание телекоммуникационной системы тактического звена управления в виде однопродуктовой тензорной модели. Данное описание дает возможность осуществлять проектирование любых сложных систем в переходной ситуации, когда вместо старых путей в качестве системы координат выбираются новые пути, ориентированные на устойчивое развитие, согласованное с общими законами природы. Таким образом, применяя тензорный метод для анализа и описания телекоммуникационной системы тактического звена управления, можно одновременно учитывать различные параметры системы в изменяющихся условиях функционирования, сохраняя целостность ее рассмотрения.

УДК 623.618
Малюк В.Г.

ВИЗНАЧЕННЯ ЗАГАЛЬНИХ ВИМОГ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МОБІЛЬНИХ КОМПОНЕНТ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

Розглянуто тенденції розвитку мобільних компонент тактичної ланки управління ВВ Україниии, сформульовані загальні вимоги до лінгвістичного та програмного забезпечення автоматизованих систем управління такими компонентами

Сучасні тенденції розвитку мобільних компонент тактичної ланки управління **(**ТЛУ) ВВ України приводять до необхідності створення системи програмного врахування єдиного поточного часу в усіх ланках для навігації і вирішення задач управління в реальному часі.

АСУ в цілому й всі види її забезпечення повинні бути пристосовані до модернізації, розвитку й нарощуванню в межах вимог, зазначених у ТЗ.

Програмне забезпечення (ПЗ) АСУ повинне бути достатнім для виконання всіх функцій АСУ, реалізованих із застосуванням засобів обчислювальної техніки, а також мати засоби організації всіх необхідних процесів обробки даних, що дозволяють вчасно виконувати усі функції у всіх регламентованих режимах функціонування АСУ.

Необхідними вимогами для ПЗ в цілому є висока надійність, стійкість до відмов, підтримка розподілених баз даних, масштабуємість та підтримка паралельної багатопроцесорної обробки даних.

Програмне забезпечення АСУ повинне мати наступні властивості:

- функціональна достатність (повнота);
- надійність (у тому числі відновлюваємість, наявність засобів виявлення помилок);
- адаптуємість;
- модифіцируємість;
- модульність побудови;
- зручність експлуатації.

Програмне забезпечення АСУ повинне бути переважно побудоване на базі існуючих пакетів прикладних програм і інших програм, запозичених з державних, галузевих і інших фондів алгоритмів і програм, допускати завантаження й перевірку за частинами і дозволяти робити заміну одних програм без корекції інших.

В АСУ повинні бути переважно використані системи управління базами даних (СУБД), зареєстровані у встановленому порядку.

Програмне забезпечення АСУ повинне бути побудоване таким чином, щоб відсутність окремих даних не позначалася на виконанні функцій АСУ, при реалізації яких ці дані не використаються.

Також ПЗ повинне мати засоби діагностики технічних складових АСУ й контролю на вірогідність вхідної інформації.

У програмному забезпеченні АСУ повинні бути реалізовані заходи щодо захисту від помилок при уведенні й обробці інформації, що забезпечують задану якість виконання функцій АСУ.

Загальне програмне забезпечення АСУ повинне дозволяти здійснювати настроювання компонентів спеціального програмного забезпечення й подальший розвиток програмного забезпечення АСУ без переривання процесу її функціонування. Повинне бути забезпечено захист уже згенерованої і завантаженої частини програмного забезпечення від випадкових змін.

Всі програми спеціального ПЗ повинні бути сумісні як між собою, так і з її загальним програмним забезпеченням АСУ.

Експлуатаційна програмна документація на АСУ повинна відповідати стандартам ЕСПД і містити всі відомості, необхідні персоналу АСУ для використання програмного забезпечення, для його первісного завантаження й (або) генерації, завантаження інформації внутрімашиної інформаційної бази, запуску програм АСУ, перевірки їхнього функціонування за допомогою відповідних тестів.

Знову розроблювальні програмні вироби, включені до складу її програмного забезпечення, повинні бути зареєстровані в державному, галузевому або іншому фондах алгоритмів і

програм (по приналежності).

Операційні системи повинні підтримувати:

- мережеве обладнання;
- мережеві протоколи;
- протоколи маршрутизації;
- фільтрацію мережевого трафіку;
- доступ до віддалених ресурсів;
- мережеві протоколи авторизації.

В якості операційних середовищ для підсистем різного рівня можуть використовуватись:

- для робочих місць користувачів, які працюють в розвинутому графічному середовищі - MS Windows XP;
- для серверів загального призначення (файловий, поштовий сервіс та ін.) – операційні системи MS Windows Server 2008 R2 або вище.
- для спеціалізованих серверів (сервери баз даних, комунікаційні сервери, міжмережні екрани) припускається використання різновидів операційної системи Unix.

Системи управління базами даних та програмні засоби взаємодії з ними повинні підтримувати роботу з мовою SQL за стандартом ANSI-ISO X3.135-1992. Базова СУБД визначається на стадії технічного проекту.

В якості базової геоінформаційної системи рекомендується використовувати програмні засоби ESRI ArcInfo/ArcView, а в якості універсального серверу просторових даних - ESRI SDE. Зовнішній обмін геоданими повинен забезпечуватись відповідними мережними програмними засобами лінійки ESRI - ArcExplorer, Internet Map Server (IMS).

При побудові підсистем управління телекомунікаціями необхідно передбачити програмні засоби мережного адміністрування та моніторингу, які відповідають функціональним вимогам до адміністративно-технологічної підсистеми в частині адміністрування локальних обчислювальних мереж та зовнішніх телекомунікацій системи.

В якості засобів розробки прикладних програм можуть використовуватись універсальні засоби програмування - компілятори C та C++ відповідно до операційного середовища так і інструментальні середовища RAD для розробки прикладних програм - Microsoft Visual C/C++ та Visual Basic, Borland Delphi та C++ Builder, Html, Java, Java Bin або інші аналогічні, інструментальні засоби СУБД відповідно до вибраної СУБД, а також можливості інструментальних засобів класу RAD в MSOffice із застосовування серверів автоматизації Access, Excel, Word з використанням технологій Active-X.

Лінгвістичне забезпечення АСУ повинне бути достатнім для спілкування різних категорій користувачів у зручній для них формі із засобами автоматизації АСУ й для здійснення процедур перетворення й машинного подання оброблюваної в АСУ інформації.

У лінгвістичному забезпеченні АСУ повинне бути:

- передбачено язикові засоби для опису будь-якої використовуваної в АСУ інформації;
- уніфіковано використовувані мовні засоби;
- стандартизовано описи однотипних елементів інформації й записи синтаксичних конструкцій;
- забезпечено зручність, однозначність і стійкість спілкування користувачів із засобами автоматизації АСУ;
- передбачено засоби виправлення помилок, що виникають при спілкуванні користувачів з технічними засобами АСУ;
- використання термінологічних словників для контролю інформації, що вводиться (усунення помилок операторів і контролю збоїв обчислювальних засобів);
- формування з загальних словників часткових проблемно-орієнтованих словників.

Лінгвістичне забезпечення АСУ повинне бути відбите в документації (інструкціях, описах) організаційного забезпечення АСУ у вигляді правил спілкування користувачів з технічними засобами АСУ у всіх режимах функціонування системи.

УДК 621.391
Приходько С.И., Волков А.С.

МЕТОД АЛГЕБРАИЧЕСКОГО ДЕКОДИРОВАНИЯ КАСКАДНЫХ СВЕРТОЧНЫХ КОДОВ В ЧАСТОТНОЙ ОБЛАСТИ

Перспективным способом повышения достоверности передаваемых дискретных сообщений в современных телекоммуникационных системах и сетях является использование методов последовательного каскадного сверточного кодирования и декодирования. В качестве компонентных кодов эффективно использовать алгебраические сверточные коды, которые обладают высокой корректирующей способностью, позволяют построение кодов с большими длинами кодового ограничения ($v > 10$) и допускают алгебраические методы декодирования.

Предлагается метод алгебраического декодирования каскадных сверточных кодов в частотной области с использованием быстрого (двумерного) преобразования Фурье Кули-Тьюки в конечном поле на основных этапах декодирования.

Представим разработанный метод декодирования в частотной области в виде последовательности следующих действий.

1. Выделение одной секции кодового слова $s^*(x)$ длины n_0 алгебраического каскадного сверточного кода на внутренней ступени искаженного ошибками $s^*(x) = s^*(x)+e(x)$.

2. Выполнение прямого двумерного преобразования Фурье Кули-Тьюки принятой одной секции кодового слова длины n_0.

3. Формирование многочлена локаторов ошибок $\Lambda(x)$.

4. Рекуррентное продолжение синдрома для нахождения вектора ошибок E, представленного в частотной области.

5. Исправление одной секции кодового слова S^* длины n_0 алгебраического каскадного сверточного кода в частотной области на внутренней ступени искаженного ошибками путем сложения вектора ошибок и принятой секции кодового слова $S=S^*+E$.

Далее процедуру алгебраического декодирования необходимо продолжить аналогичным образом на внешней ступени каскадного сверточного кода с последующим выделением информационных символов.

Отметим, что на втором этапе алгебраического метода декодирования каскадных сверточных кодов в частотной области применяется двумерное преобразование Фурье Кули-Тьюки для каждой ступени кода. В общем случае возможно применение многомерного преобразования Фурье Кули-Тьюки. Для этого необходимо, чтобы длину одной секции кодового слова сверточного кода внешней или внутренней ступени можно было разложить на p делителей. Тогда возможно построение p мерного преобразования Фурье Кули-Тьюки, что позволит еще больше сократить вычислительную сложность (число арифметических операций умножений и сложений).

На третьем этапе декодирования отсутствует необходимость решения ключевого уравнения в полном объеме, что является важным преимуществом при практической реализации данного метода.

Особенности алгебраического метода декодирования в частотной области делают данный метод более предпочтительным по сравнению с алгебраическими методами во временной области. Это связано с высокой вычислительной сложностью существующих методов.

Таким образом, метод алгебраического декодирования каскадных сверточных кодов в частотной области позволяет реализовать декодирование за фиксированное число операций. При этом метод эффективен при использовании компонентных сверточных кодов с большими длинами кодового ограничения на каждой ступени кода, что дает возможность реализовать процедуры декодирования очень длинных кодов ($n > 1000$).

Благодаря применению двумерного преобразования Фурье Кули-Тьюки удается значительно снизить вычислительную сложность метода, что делает данный метод декодировании более привлекательным, чем существующие аналоги.

Зинчук Ю.А.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОПУСКНОЙ СПОСОБНОСТИ СИСТЕМ ПОДВИЖНОЙ СВЯЗИ С CDMA И С OFDMA

Достижение высокой помехоустойчивости и пропускной способности систем подвижной связи(СПС)настоящего и будущих поколений связывается с использованием многоуровневых фазовых (MPSK), амплитудно-фазовых (MQAM),а также с модуляцией вида OFDM. Потенциальные преимущества этих видов модуляции могут быть реализованы на практике только при высокой точности оценки комплексной огибающей принимаемого сигнала. Трудность получения оценки комплексной огибающей в современных системах радиосвязи обусловлена причинами,о которых говорится ниже.

- В СПС каналы распространения сигнала между приёмником и передатчиком являются многолучевыми и нестационарными,что приводит к быстрым изменениям комплексной огибающей компонент многолучевого сигнала. Средняя частота этих изменений определяется скоростью движения мобильного абонента и частотой несущей.Одним из требований к СПС является поддержание связи с абонентами,перемещающимися со скоростью 500км/ч. В этих условиях при частоте несущей 2 ГГц произведение длительности символа на частоту замираний,например в прямом канале системы связи UMTS,может составлять 0.05 и, следовательно,комплексная огибающая сигнала заметно изменяется от символа к символу.

В последнее время для систем радиосвязи активно разрабатываются и внедряются адаптивные антенные решетки,разнесеннаяпередача данных. В связи с этим для обеспечения квазикогерентного приема передаваемый сигнал содержит индивидуальные пилот-сигналы для каждогопользователя системы связи.Для повышения пропускной способности системы связи энергия используемых сигналов должна быть минимизирована.В результате алгоритмы оценки комплексной огибающей должны эффективно функционировать и при низких уровнях пилот-сигнала.

Для повышения емкости системы связи максимально снижают среднее значение отношения сигнал-шум(ОСШ) на информационный символ,при котором обеспечивается требуемое качество приема информации.

Последние достижения в теории и технике связи(применение трубокодирования,исправляющего ошибки,передача данных с перезапросом,многопользовательское детектирование) позволяют снизить среднее ОСШ на кодовый символ до 0÷ 2 Дб. В результате алгоритмы оценки комплексной огибающей,использующие как пилот-сигнал,так и информационный сигнал,должны эффективно функционировать при низких уровнях мощности информационных символов.

В системах радиосвязи,функционирующих в условиях многолучевости,для улучшения качества связи используют многолучевые приемники,которые реализуют разнесенный прием. Также важной характеристикой СПС является пропускная способность канала связи. Далее проведен сравнительный анализ пропускной способности СПС с использованием CDMA и OFDMA.

Полевые испытания, проводившиеся в различных условиях, подтвердили, что при высокой нагрузке пропускная способность систем CDMA в среднем в 15 раз превышает пропускную способность аналоговых систем. Если выражать это в Эрлангах при заданном качестве обслуживания, то преимущества систем CDMA еще более очевидны. При использовании существующих вокодеров, которые работают на половинной скорости передачи, пропускная способность увеличивается еще в 1,7 раза (при том, что для сети CDMA необходимо на 30-40% базовых станций меньше, чем для GSM, и в 2-3 раза меньше, чем для AMPS). Дополнительная секторизация (свыше 3) также увеличивает пропускную способность. Существует возможность выделения требуемой полосы частот по потребности. Кроме того, максимальная дальность связи (в отличии от TDMA-систем) ограничена лишь мощностью и радиовидимостью.

Режим передачи согласно стандарту IEEE 802.16e-2005 основан на концепции наращиваемого (масштабируемого) OFDMA (SOFDMA — Scalable OFDMA) . Он же поддерживает широкий диапазон пропускной способности и гибко приспосабливается к потребностям в различных диапазонах спектра. Наращивание пропускной способности поддерживается регулировкой числа шагов быстрого преобразования Фурье (БПФ — FFT — Fast Fourier Transform). Параметры SOFDMA приведены в таблице 1. Технической рабочей группой WiMAX Forum вначале запланирована разработка документов (профилей) для значений ширины каналов 5 и 10 МГц (выделены в табл.).

Подход OFDM был выбран как многоразовая схема доступа для LTE из-за низкой сложности и преимуществ масштабируемости, что предлагает преимущество над системой CDMA. Выигрыш в пропускной способности WiMAX у OFDMA на равном расстоянии от базовой станции пока не так очевиден. Это связано в первую очередь с тем, что для WiMAX доступно пока не так много частотных диапазонов. Однако если HSDPA, являясь эволюционным шагом в развитии WCDMA, приближается к порогу спектральной эффективности, то у WiMAX возможных путей развития значительно больше — это и новые частотные диапазоны (от 10 до 66 ГГц, и новые модуляционные схемы (а также комбинации с предыдущими), и MIMO (multiple-input-multiple output).

Дальнейшее развитие технологий LTE будет продолжаться в рамках работ над новым стандартом 3GPP Release10(LTE-advanced). На сегодня уже сформулированы основные требования которым должна отвечать система LTE, которые, по сути, в своей совокупности соответствуют стандарту мобильных сетей 4 поколения(4G).

Таблица 1

Параметры	Значение			
Ширина канала (МГц)	1,25	5	10	20
Частота опроса (МГц)	1,4	5,6	11,2	22,4
Размер преобразования Фурье	128	512	1024	2048
Число подканалов	2	8	16	32
Интервал между несущими	10,94кГц			
Длительность полезного символа	91,4мкс			
Защитный интервал	11,4мкс			
Длительность OFDMA-символа	102,9мкс			
Число символов (кадр 5мс)	48			

К ним относятся:

- максимальная скорость передачи данных в нисходящем радиоканале до 1 гигабита за секунду, в восходящем-500 Мбит/с(увелечение средней пропускной способности на одного абонента);
- полоса пропускания в нисходящем канале 70 МГц, в восходящем 40 МГц;
- полная совместимость и легкость взаимодействия с LTE и другими 3GPP системами.

Для решения этих задач предполагается использовать гибридную технологию OFDMA

Іохов О.Ю., Горбов О.М.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЗВ'ЯЗКУ В РАДІОМЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Розглянуто основні наукові підходи до шляхів вирішення проблеми забезпечення радіозв'язку. Запропоновано комплексна система криптографічного захисту зв'язку в радіомережах військового призначення.

Безпека зв'язку – здатність зв'язку зберігати в таємниці зміст переданих повідомлень і протистояти уводу хибної інформації.

Для того щоб звести до мінімуму витік інформації, розробляються відповідні системи інформаційного захисту, які являють собою сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації.

Розглянувши всі стандарти мобільного зв'язку та їх методи забезпечення безпеки зв'язку можна виділити один основний недолік – ні один з проаналізованих стандартів не дає 100 % безпеки зв'язку. Таким чином на даний час використання мобільного зв'язку, як засобу передачі конфіденційної інформації неможливо.

Досвід проведення антитерористичних та стабілізаційних операцій, яки проводили провідні країни світу показав, що зазвичай супротивник володіє останніми досягненнями в галузі радіотехніки це дозволяє йому володіти оперативною інформацією, а також вести радіоперехват та радіоподавлення, розкривати структуру системи управління, нав'язувати хибну інформацію.

В радіомережах силових структур України, відсутні засоби криптографічного захисту інформації. Використання закордонних засобів криптографічного захисту, може призвести до витоку конфіденційної інформації.

Одним з напрямків забезпечення безпеки зв'язку в радіомережах є методи криптографічного захисту інформації.

Криптографічні методи можуть бути класифіковані різним чином, але найбільш часто вони поділяються залежно від кількості ключів, які використовуються у відповідному криптоалгоритмі:

1. Безключовий, в яких не використовуються всі типи ключів.
2. Одноключевий (симетричний) - в них використовується якийсь додатковий ключовий параметр - зазвичай це секретний ключ.
3. Двоключевий (асиметричну), які використовують у своїх обчисленнях два ключі: секретний і відкритий.

Аналіз закордонних засобів захисту інформації показав, що в сучасних засобах криптографічного захисту інформації використовуються блочні симетричні шифри. Використання цих методів шифрування ускладнюється, тим, що у кожного абонента радіомережі повинна бути ключова документація, у разі втрати котрої руйнується система криптографічного захисту.

В свою чергу аналіз стандартних режимів застосування блочних шифрів показав існування у криптоаналітика потенціальної можливості атакувати безпосередньо базові функцію блочного шифрування на основі відомих пар «відкритий-шифрований» в любому з режимів, передбачених міжнародним стандартом. Таким чином, виникає протиріччя між можливостями сучасних методів блочного шифрування протидіяти атакам криптоаналітика, та необхідністю створення системи гарантованої стійкості в радіомережах військового призначення. Вирішення даного протиріччя, можливе за рахунок рішення науково-технічного завдання, яке полягає в створенні організаційно-технічної системи криптографічного захисту, на основі використання методу прямого криптографічного перетворення.

УДК 621. 32

Орлов М. М.

НАПРЯМКИ АВТОМАТИЗАЦІЇ ОПРАЦЮВАННЯ ІНФОРМАЦІЇ В СИСТЕМІ УПРАВЛІННЯ ВНУТРІШНІМИ ВІЙСЬКАМИ

Визначені напрямки автоматизації опрацювання інформації, що циркулює в контурі

управління виходячи із службово-бойових завдань внутрішніх військ.

Автоматизація опрацювання інформації в системі управління внутрішніми військами (ВВ) обумовлена певними *чинниками*, до яких слід віднести: 1) необхідність отримання інформації, що циркулює в контурі управління ВВ, в режимі ON-LINE (розвідувальної інформації у відеографічній формі, формалізованої командної інформації і інформації стану); 2) необхідність зменшення обсягу паперової інформації та "людського фактору" в разі оброблення її і під час безпосереднього управління ВВ; 3) зростаючі вимоги щодо обсягу і організації заходів при ускладненні обстановки в кризових ситуаціях; 4) підвищення вимог керівництва держави щодо готовності ВВ за призначенням і вимог оперативності, своєчасності, стійкості і прихованості управління ними; 5) ускладнення процесу взаємодії ВВ з іншими силовими структурами в середині держави та сусідніх держав в разі вирішення загальних службово-бойових завдань (СБЗ) (бойових завдань).

На теперішній час існують певні недоліки щодо автоматизації інформації в процесі управління ВВ (рис. 1).

ВВ, можуть бути: 1) автоматизація інформації, яка циркулює всередині органу управління (пункту управління) частини ВВ; 2) автоматизація інформації, яка циркулює між органами управління (пунктами управління) територіального командування (ТрК) ВВ; 3) автоматизація інформації, яка циркулює між органом управління Головного управління і управління ТрК та частинами ВВ безпосереднього підпорядкування.

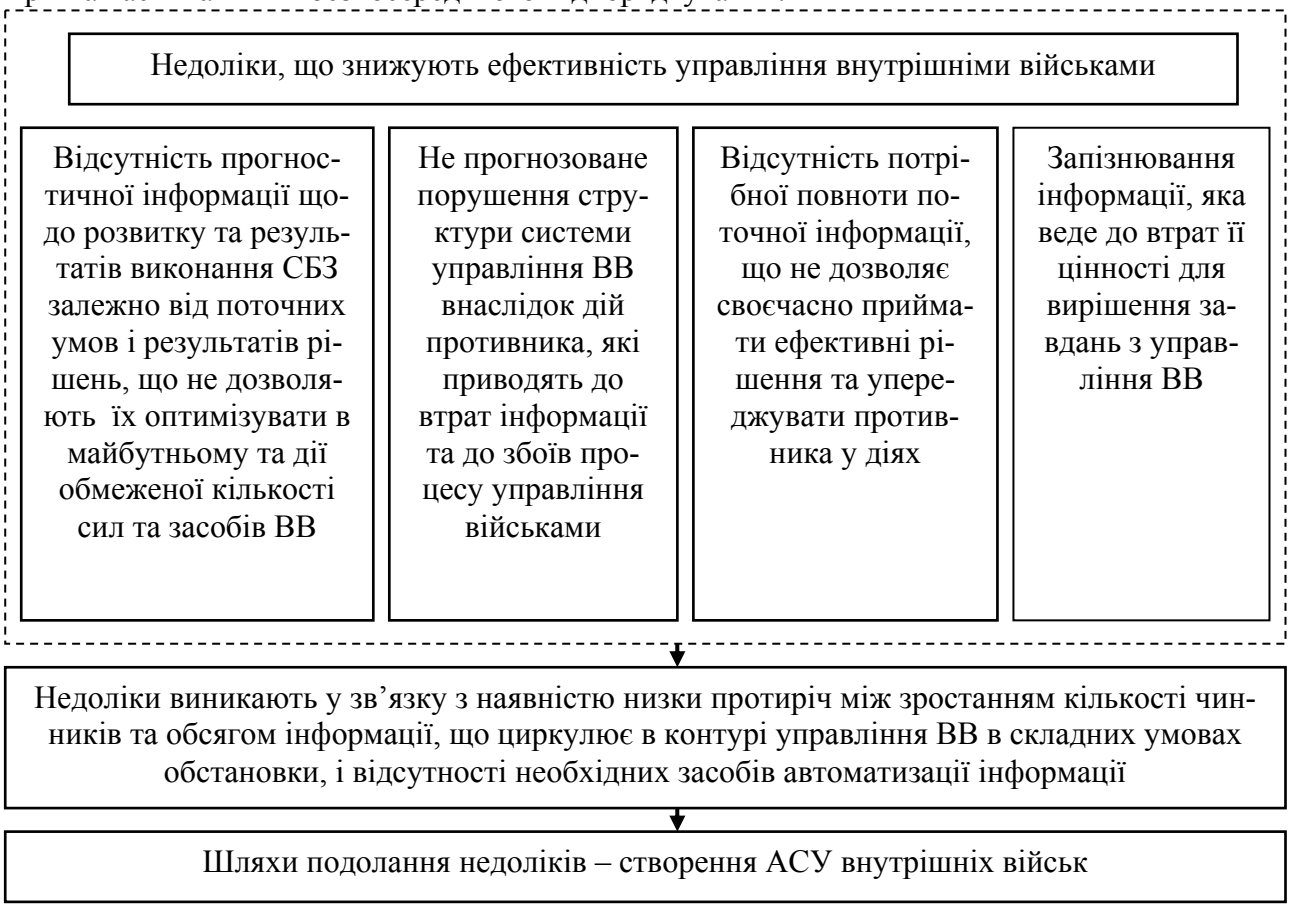


Рис. 1. Недоліки існуючого автоматизованого інформаційного забезпечення управління ВВ

Основними напрямками автоматизації інформації, що циркулює в контурі управління.

В разі створення автоматизована система управління ВВ повинна забезпечити оперативне, своєчасне, стійке і приховане управління при виконанні військами усього переліку СБЗ (табл. 1).

Таблиця 1

Напрямки автоматизації управління внутрішніх військ

(згідно завдань, викладених у Концепції розвитку внутрішніх військ МВС України на період до 2015 р., скорчений варіант)

Перелік завдань, які війська виконують самостійно	Напрямки автоматизації (підходи щодо реалізації див. нижче)
здійснення спеціальної охорони; охорона та оборона центральних баз матеріально-технічного забезпечення Міністерства внутрішніх справ України	*В межах військової частини з охорони ОВДО:* 1. Загальний і вибірковий контроль стану зони охорони і режимних приміщень. 2. Поточний облік особового складу задіяного на службу, резерв і його розподілення згідно бойового розрахунку. 3. Поточний облік та стан озброєння і військової техніки, спеціальних засобів, засобів зв'язку. *В межах внутрішніх військ (на рівні ГУВВ):* 1. Стан системи охорони ОВДО, які охороняють внутрішні війська: режим № 1 – *нема порушень на об'єкті*; режим № 2 – *є порушення на об'єкті.* 2. Поточний облік особового складу задіяного на службу, резерв і його розподілення за кожний об'єкт, згідно бойового розрахунку. 3. Поточний облік і стан озброєння і військової техніки за кожний об'єкт (за кожну військову частину).
конвоювання осіб, узятих під варту, підсудних, осіб, засуджених до позбавлення волі, до апеляційних судів, військових місцевих судів, Касаційного суду та Верховного Суду України і охорона їх під час судового засідання	*В межах військової частини з конвоювання:* 1. Кількість варт з забезпечення судових процесів, їх чисельність і місце виконання завдання. 2. Кількість рухомих варт по супроводженню підсудних і заарештованих, їх чисельність, маршрут пересування, поточний стан на маршруті виконання завдання. *В межах внутрішніх військ (на рівні ТРК):* 1. Кількість варт з забезпечення судових процесів, їх чисельність і місце виконання завдання. 2. Кількість рухомих варт по супроводженню підсудних і заарештованих, їх чисельність, маршрут пересування, поточний стан на маршруті виконання завдання. 3. План і результати перевірки варт на маршрутах руху. *В межах внутрішніх військ (на рівні ГУВВ):* 1. Кількість варт з забезпечення судових процесів, їх чисельність і місце виконання завдання. 2. Кількість рухомих варт по супроводженню підсудних і заарештованих, їх чисельність, маршрут пересування, поточний стан на маршруті виконання завдання. 3. План і результати перевірки варт на маршрутах руху.
переслідування і затримання осіб, узятих під варту, підсудних і осіб, засуджених до позбавлення волі або арешту, які втекли з-під варти	*В межах військової частини ВВ:* 1. Кількість груп переслідування, маршрути їх руху. 2. Поточна інформація про стан справ кожної групи переслідування. *В межах внутрішніх військ (на рівні ТРК):* 1. Кількість груп переслідування, маршрути їх руху. 2. Поточна інформація про стан справ кожної групи переслідування. *В межах внутрішніх військ (на рівні ГУВВ):* 1. Кількість груп переслідування, маршрути їх руху. 2. Поточна інформація про стан справ кожної групи переслідування.

забезпечення охорони учасників кримінального судочинства та охорони місцевих, військових судів, апеляційних судів, Касаційного суду України	*В межах військової частини ВВ:* 1. Кількість варт, склад і місце виконання завдання. 2. Поточна інформація про стан справ кожної варти. *В межах внутрішніх військ (на рівні ТРК):* 1. Кількість варт, склад і місце виконання завдання. 2. Поточна інформація про стан справ кожної варти. *В межах внутрішніх військ (на рівні ГУВВ):* 1. Кількість варт, склад і місце виконання завдання. 2. Поточна інформація про стан справ кожної варти.
охорона дипломатичних представництв, консульських установ іноземних держав і представництв міжнародних організацій в Україні	*В межах військової частини ВВ:* 1. Кількість варт (військовослужбовців), склад і місце виконання завдання. 2. Поточна інформація про стан справ кожної варти. *В межах внутрішніх військ (на рівні ТРК):* 1. Кількість варт (військовослужбовців), склад і місце виконання завдання. 2. Поточна інформація про стан справ кожної варти. *В межах внутрішніх військ (на рівні ГУ ВВ):* 1. Кількість варт (військовослужбовців), склад і місце виконання завдання. 2. Поточна інформація про стан справ кожної варти.

Існуючий стан автоматизації системи управління ВВ можна оцінити через рівень технічного оснащення пунктів управління (ПУ) засобами автоматизації, їх програмним забезпеченням, рівень готовності посадових осіб (ПО) органів управління користуватися засобами автоматизації, рівень оснащеності вузлів зв'язку ПУ, їх пропускної спроможності та кількості і глибини оперативно-тактичних завдань (задач), які система дозволяє вирішувати в автоматичному або автоматизованому режимах.

У подальшому дослідження можуть бути за напрямками: 1) визначення першочергових завдань, які необхідно забезпечити інформацією в автоматизованому режимі; 2) шляхи технічної реалізації процесу автоматизації; 3) поетапне впровадження автоматизації у військах; 4) розроблення типового автоматизованого пункту управління для частини ВВ і управління територіального командування (ТРК) внутрішніх військ.

УДК 681. 3.07

Дорохін І.С., Поштаренко В.М.

ОПТИМІЗАЦІЯ ТРАНСПОРТНИХ МЕРЕЖ NGSDH НА ОСНОВІ ІМІТАЦІЙНОГО МОДЕЛЮВАНИЯ

Розроблена імітаційна модель магістральної мережі NGSDH із використанням математичної моделі за допомогою багаторівневої декомпозиції та проведене імітаційне моделювання та порівняння даної системи у спеціалізованому середовищі Network Simulator.

Постановка проблеми. Розвиток технології Ethernet привів до появи нового транспорту - PoS (Pocket over SDH), або NewGen SDH (NG SDH). По суті, це симбіоз двох добре знайомих технологій - Ethernet й SDH. Така технологія має всі переваги системи передачі SDH, що характеризується найвищою надійністю й керованістю, і мережі IP, що дозволяє надавати всі необхідні послуги передачі пакетного трафіка. Архітектура сучасних мультиплексорів NGSDH з роздільними шинами TDM і шиною даних припускає використання двох незалежних матриць комутації для обробки трафіка SDH і пакетного трафіка. Такий підхід дозволяє не відображати трафік даних у віртуальні контейнери VC й є наступним кроком на шляху до

шляху до міграції транспортних мереж від передачі традиційного голосового трафіка до повністю пакетної передачі даних у майбутньому. Будучи, по суті, гібридною платформою, обладнання NGSDH дозволяє при збереженні інвестицій в існуюче встаткування й прибутків від послуг TDM одержувати додаткові джерела доходів.

Підвищення складності сучасних телекомунікаційних технологій створює проблеми у застосуванні аналітичних методів для оцінки характеристик проектованих систем і мереж, і здійснюється широким застосуванням імітаційного моделювання.

Поява альтернативних операторів зв'язку й будівництво ними власних мереж привелася до переоцінки важливості критеріїв стосовно до мереж SDH й у перспективі до мереж наступного покоління (типу NGN). У цей час мережі SDH експлуатуються багатьма операторами зв'язку. При цьому треба відзначити, що в 95% випадків мережі SDH побудовані із застосуванням кільцевої структури. З розвитком технології мережі SDH можуть бути розвинені до рівня мереж NGN заміною встаткування на вузлах, що спричинить істотне збільшення пропускної здатності мереж, а також дасть можливість реконфігурувати логічну структуру таких мереж при зміні навантаження для максимальної відповідності поточним потребам у передачі інформації. Але при цьому перехід від мереж SDH до мереж NGN ставить задачу керування проведенням такої реконфігурації логічної структури.

Для операторів зв'язку й проектних організацій різного рівня представляється необхідним мати інструмент для побудови структури мереж SDH при розгортанні нових і модернізації вже існуючих мереж. Задача полягає в тім**,** щоб за існуючою схемою розташування вузлів і матриці, що визначає необхідність у передачі навантаження між парами вузлів (далі умовно називаною матрицею досяжності), визначити матрицю суміжності, що визначає фізичний зв'язок між парами вузлів.

Задача визначення всіх можливих маршрутів між кожною парою вершин графа має комбінаторну складність

$$O = C_N^2 \sum_{i=1}^{N-2} \frac{(N-2)!}{(N-2-i)!}.$$

У зв'язку із цим потрібна декомпозиція задачі, у якості якої пропонується розбивка множини вузлів мережі на підмножини.

При рішенні загальної задачі, що полягає в переборі всіх можливих 2exp(N*N-N)/2 варіантів матриці суміжності й визначення всіх можливих варіантів маршрутів, що зв'язують кожну пару вузлів, для кожної матриці необхідно знайти всі можливі маршрути між кожною парою вузлів.

Необхідно одержати схему фізичних зв'язків усередині підмножин, тобто, сполучних ліній між вузлами. Відповідно до існуючих правил для мереж SDH ці зв'язки повинні утворити кільцеву структуру, тобто потрібна розбивка підмножин на кільця.

У світлі необхідності на початковому етапі проектування мережі багаторазового визначення (розрахунку) структури мережі, більші тимчасові витрати прямого рішення не прийнятні на етапі первісного проектування й в умовах динамічно-змінюваних умов функціонування мережі, тобто в умовах зміни матриці досяжності. При введенні деяких обмежень, що враховують умови задачі, можна спростити рішення шляхом декомпозиції задачі на підзадачі з визначенням цільової функції.

Використання мультиплексорів, максимально відповідним рівням системи в створених кільцях, забезпечує мінімально можливі витрати на встаткування. Мінімізація витрат на встаткування й кабелі приводить до зменшення їх кількісних і потужностних параметрів, а це, у свою чергу, приводить до збільшення середнього відсотка завантаження.

Метою статті є розробка імітаційної моделі мереж NGSDH, що виконує оптимізацію за критерієм мінімальних капітальних витрат на побудову або модернізацію мережі SDH на основі алгоритму багаторівневої декомпозиції.

Імітаційна модель розроблена у середовищі Network Simulator. Мережа складається з 6 підмереж T1-T6 і магістральної мережі, утвореної 14 мультиплексорами MUX_1-MUX_14.

Для оцінки ефективності алгоритму за встановленими критеріями введемо наступні оцінні

параметри: середнє завантаження мережі: $V_{ср}$ – середній відсоток завантаження мережі, в %; кількість мультиплексорів; довжина використаного кабелю.

Зазначені вище параметри рішення, отриманого за допомогою запропонованого алгоритму, рівняються зі значеннями цих же параметрів,але без застосування алгоритму.

У даній роботі запропонований простий спосіб оцінки характеристик моделі на основі аналізу файлу траси за допомогою командних файлів ОС Unix, не потребуючого використання спеціальних класів системи NS.

Виконано імітаційне моделювання процесів у зазначеному фрагменті магістралі Інтернет для різної інтенсивності потоків, генеруємих термінальними мережами. Оцінювалися пропускна здатність магістралі, середній час доставки пакета й відсоток доставлених пакетів для різної інтенсивності потоків по трасі моделювання за допомогою спеціальних скріптів.

Поводження мережі досліджувалося при пікових навантаженнях. Інтенсивність джерел трафіка до 150 Kbps відповідає нормальному навантаженню мережі із часток загублених пакетів не перевищуючої 2-3% і часом доставки пакета 0.05-0,15 с.; при цьому пропускна здатність всієї мережі приблизно рівняється сумарному сгенерованому трафіку. Подальший ріст інтенсивності трафіка приводить до зниження пропускної здатності через зюільшення черг і втрати пакетів і значному збільшенню часу доставки пакета (до 0.4 с).

Результатами моделювання є оцінка продуктивності NGSDH в таких випадках: без застосування запропонованого методу і в результаті роботи алгоритму. Виконано аналіз особливостей проектування транспортних мереж, обгрунтовано необхідність та основи впровадження NGSDH.

Таким чином, при оптимізації мережі з використанням розробленого алгоритму отриманий більший відсоток завантаження мережі, що дозволяє обійтися меншими ресурсами мережі на 15-20% і забезпечує зменшення капітальних витрат на створення мережі.

Висновки. Отримані при застосуванні алгоритму результати підтверджують наступне: застосування алгоритму й методики дозволяє одержувати раціональну схему організації кільцевої структури мережі SDH за критеріями мінімальних капітальних витрат; пропонований підхід до побудови транспортних мереж NGSDH за певних умов є близьким до оптимального й дозволить операторові досягти бажаних технічних і фінансових результатів за рахунок поетапної реконструкції інфраструктури.

УДК 623.618

Іохов О.Ю., Кузминич І.В.

ПІДВИЩЕННЯ СКРИТНОСТІ УПРАВЛІННЯ В РАДІОМЕРЕЖАХ ВВ МВС УКРАЇНИ

Шляхи захисту радіомереж ВВ МВС України при виконання завдань за призначенням. Аналіз технологій забезпечення скритності радіозв'язку.

Розвиток високоточної зброї та засобів радіоелектронної боротьби провідних країн світу, можливість вільного придбання цих засобів, говорить про те, що основним чинником, який впливає на ефективність функціонування системи управління військами під час виконання службово-бойових завдань є забезпечення безпеки зв'язку.

Досвід проведення антитерористичних та стабілізаційних операцій силовими структурами провідних країн світу показав, що зазвичай супротивник володіє останніми досягненнями радіотехніки. Це дозволяє не тільки володіти оперативною інформацією, а також утручатися в радіо мережі, розкривати структуру радіомереж та порушувати радіозв'язок. Радіозасоби, які знаходяться на озброєнні ВВ МВС України є морально застарілими та повністю не відповідають сучасним вимогам. Це приводить до висновку, що розробка новітніх зразків радіозв'язку є основним завданням на теперішній час, і потребує особливої уваги з боку керівництва країни. При розробки радіозасобів требо враховувати необхідність дотримання підвищених вимог до таких характеристик, які достовірності та скритності радіозв'язку.

Аналіз засобів зв'язку силових структур провідних країн світу показав, що всі сучасні зразки використовують широкосмугові системи множинного доступу, які здатні забезпечити задану достовірність, скритність зв'язку та велику пропуску спроможність.

В сучасних засобах радіозв'язку провідних країн світу вже використовується один із методів формування широкосмугових сигналів – метод частотного розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing – OFDM). Основними перевагами даної технології є висока стійкість щодо частотно-селективних завмирань та висока спектральна ефективність.

Суттєвим недоліком, що обмежує застосування ортогональної частотної модуляції у системах радіозв'язку є нестійка робота в умовах впливу навмисних завад. Спектральна щільність потужності найпростіших шумових завад, навіть зосереджених по спектру, на прийомі після прямого перетворення Фур'є розмивається практично по всіх частотних підканалах, що або ускладнює, або й зовсім унеможливлює прийом OFDM-сигналу.

Одним з шляхів вирішення цього недоліку та значного підвищення енергетичної та структурної прихованості зв'язку стає можливим при розширенні спектру OFDM-сигналу псевдовипадковими послідовностями, адже спектральна щільність потужності широкосмугового сигналу значно менша у порівнянні з простими сигналами.

Таке поєднання використовується в стандарті MC-CDMA (multi carrier CDMA – багаточастотне кодове розділення каналів) і дозволяє значно зменшити вплив навмисних завад. MC-CDMA система має всі переваги CDMA і OFDM систем, тобто дозволяє боротися із багатопроменевістю й частотно-селективними завмираннями, однак платою за це є істотне зменшення швидкості передачі даних.

Однак для застосування MC-CDMA у для систем радіозв'язку ВВ МВС України необхідно одночасне виконання підвищених вимог, що на даний час неможливо.

Виникає протиріччя між зростанням вимог до достовірності та скритності зв'язку та неможливістю сучасних методів, у повному обсязі, забезпечення виконання цих вимог. Розв'язати це протиріччя дозволяє вирішення наукової задачі, яка полягає у побудові збалансованої системи множинного доступу на основі методів формування кодових послідовностей з підвищеними кореляційними властивостями.

УДК 681.3.06

Халимов Г.З.

АСИМПТОТИЧЕСКИЕ ОЦЕНКИ МАКСИМАЛЬНЫХ КРИВЫХ ДЛЯ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ

Представлены основные асимптотические оценки отношения числа точек алгебраических кривых к роду для целей универсального хеширования.

Универсальное хеширование реализуется на вычислениях в функциональном поле алгебраических кривых. Фундаментальная теорема Римана-Роха связывает свойства пространства рациональных функций с проективным многообразием точек кривой. Коллизионные границы определяются отношением значения полюса рациональных функций базисного пространства к числу точек алгебраической кривой. Наилучший результат достигается на максимальных кривых. Проблематикой универсального хеширования на функциональном поле $F_q(C)$ алгебраической кривой C над конечным полем F_q является определение оценок отношения числа точек алгебраических кривых к роду. Целью данной работы является асимптотическая оценка основных параметров максимальных кривых.

1. Определение максимальных кривых

Под кривой будем рассматривать проективную, геометрически неразложимую и несингулярную алгебраическую кривую определенную над конечным полем F_q с q элементами.

Точка P кривой C называется несингулярной, если существует касательная линия к кри-

вой в точке P. Например, если $P=(a,b)\in F_q\times F_q$ является точкой плоской кривой ассоциированной с полиномом $f(X,Y)\in F_q[X,Y]$, тогда точка P называется несингулярной если

$$f_X(a,b)\neq 0 \text{ или } f_Y(a,b)\neq 0,$$

где f_X и f_Y частные производные. Кривая C называется несингулярной, если каждая точка $P\in C$ является несингулярной.

Кривая $\widetilde{C}$ является проективной моделью аффинной кривой C ассоциированной с полиномом $f(X,Y)$ степени $d:=\deg f(X,Y)$ имеет представление

$$F(X,Y,Z)=Z^d f(X/Z,Y/Z) \text{ и } \widetilde{C}:=\left\{(a:b:c)\in P^2(F_q)\middle| F(a,b,c)=0\right\}.$$

Если проективная плоская кривая является несингулярной, тогда для рода кривой справедлива оценка **[**11**]**

$$g(\widetilde{C})\le (d-1)(d-2)/2.$$

Точка $(a:b:c)$ кривой $\widetilde{C}$ является рациональной точкой, если $a,b,c\in F_q$. Точка $(a:b:c)$ кривой $\widetilde{C}$ является точкой бесконечности P_∞, если $c=0$.

Пусть $F_q(C)$ есть поле рациональных функций на кривой C над F_q. В каждой точке $P\in C$ можно вычислить оценку ϑ_P для рациональных функций $x\in F_q(C)$, которая определяет порядок нуля или полюса функции x в этой точке, тогда $div(x)$ обозначает дивизор функции x, соответственно $div_\infty(x)$ значение полюса дивизора.

Пусть N_0 есть множество неотрицательных целых. Подгруппа Вейерштрасса точек не разрыва $H(P)$ ассоциированная с точкой $P\in C$ определяется как множество

$$H(P)=\left\{\alpha\in N_0:\exists x\in F_q(C)\middle| div_\infty(x)=\alpha P\right\}.$$

Соответственно подгруппа Вейерштрасса точек разрыва $G(P)$ определяется как

$$G(P)=N_0\setminus H(P),$$

и $|G(P)|=g$.

Пусть $N_q(g)$ обозначает максимальное число F_q рациональных точек, которое кривая рода g может иметь. Кривая C рода g является оптимальной над F_q если её число F_q рациональных точек $\#C(F_q)$ равно $N_q(g)$. Главный результат для теории определяется теоремой Хассе-Вейля.

Теорема 1. [1] Пусть C есть проективная и несингулярная, абсолютно неразложимая кривая определенная над конечным полем F_q с q элементами. Тогда число F_q рациональных точек кривой определяется неравенством

$$N_q(g)\le 1+q+2\sqrt{q}g(C)$$

Максимальные кривые над F_q это кривые, число F_q рациональных точек которой удовлетворяет границе Хассе-Вейля (*). Существуют три замечательных семейства таких кривых, которые связываются с Дэлигнэ-Лустига (Deligne-Lusztig) многообразием размерности $\dim=1$. Кривая Дэлигнэ-Лустига ассоциируется с проективной специальной линейной группой (кривые Эрмита), с группой Сузуки (Suzuki) $Sz(q)$ (кривые Сузуки) и Ри (Ree) группой $R(q)$ [1]. Важный результат по максимальным кривым определяется следующим предложением.

Предложение 1. [2] Пусть X_1 и X_2 неприводимые алгебраические кривые, определенные в проективном пространстве над полем F_q. Предположим, что существует морфизм $f:\mathrm{X}_1\to\mathrm{X}_2$ над полем F_q. Тогда если X_1 является максимальной кривой, тогда максимальной кривой является X_2.

Основной результат предложения 1 состоит в том, что позволяет расширить поиск других

семейств максимальных кривых.

2. Асимптотики для кривых над конечным полем

Для максимальных кривых над конечным полем достигается максимальное отношение числа точек кривой к роду. Основные асимптотические результаты для кривых следующие.

Пусть $N_q(g) = \max\limits_{C} \#C(F_q)$ есть число точек кривой C над F_q, где C пробегает все кривые рода $g(C) = g$. Асимптотическая оценка имеет вид

$$A(q) = \lim \sup\limits_{g\to\infty} N_q(g)/g .$$

Используя верхнюю границу для $N_q(g) \le q+1+\frac{1}{2}\sqrt{(8q+1)g+4(q^2-q)g}-g$, граница для $A(q)$ впервые была получена Ihara Y. [3]

$$A(q) \le \frac{1}{2}(\sqrt{8q+1}-1) .$$

Отметим, что из границы Хассе-Вейля прямо следует

$$A(q) \le 2\sqrt{q} .$$

Если $g > \sqrt{q}(\sqrt{q}-1)/2$, $N_q(g)$ лежит ниже границы Хассе-Вейля.

Основываясь на идее Ihara Y., Дринфельд и Влэдуц показали [4], что

$$A(q) \le \sqrt{q}-1$$

и в случае $q = l^2$ на модулярных кривых следует равенство $A(l^2) = l-1$.

Известна также нижняя граница Цинка для оценки $A(q^3) \ge \frac{2(q^2-1)}{q+2}$ [5].

Замечание 1. Для криптографических применений интерес представляют алгебраические кривые, определенные над конечным полем F_q с как можно большим отношением числа точек кривой к её роду.

В табл. 1 представлены максимальные кривые в квадратичном поле.

Таблица 1

Максимальные кривые над квадратичным полем F_{l^2}.

Значение рода кривой	Уравнение кривой $C(F_{l^2})$	Ограничения на коэффициенты кривой	Значение подгруппы Вейерштрасса
$g_1 = l(l-1)/2$	$y^l + y = x^{l+1}$		$\langle l, l+1\rangle$
$g_2 = (l-1)^2/4$	$y^l + y = x^{(l+1)/2}$	l нечетное	$\langle (l+1)/2, l\rangle$
$g'_2 = l(l-2)/4$	$\sum\limits_{i=1}^{t} y^{l/2^i} = x^{l+1}$	$l = 2^t$	$\langle l/2, l+1\rangle$
$g'_3 = (l^2-3l+2)/6$	$y^l + y = x^{(l+1)/3}$	$l \equiv 2 (\mathrm{mod}\, 3)$	$\langle (l+1)/3, l\rangle$
$g''_3 = l(l-3)/6$	$\sum\limits_{i=0}^{t-1} y^{3^i} = \omega x^{l+1}$	$l = 3^t$, $\omega \in F_{l^2}$ $\omega^{l-1} = -1$	$\langle l/3, l+1\rangle$
$g_3 = (l^2-l+4)/6$	$x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0$	$l \equiv 2 (\mathrm{mod}\, 3)$	$\langle 2(l+1)/3, l, l+1\rangle$
$g'''_3 = l(l-1)/6$	$\omega x^{(l-1)/3} - y x^{2(l-1)/3} + y^l = 0$	$l \equiv 1 (\mathrm{mod}\, 3)$ $\omega \in F_{l^2}$, $\omega^{l-1} = -1$	$\langle (2l-1)/3, l, l+1\rangle$
$g'''_3 = l(l-1)/6$	$y^l + y = \left(\sum_i^t x^{l/3^i}\right)^2$	$l = 3^t$	$\langle 2l/3, l, l+1\rangle$

$g_3 = \left(l^2 - l + 4\right)/6$	$x^{2(l+1)/3} y^{(l+1)/3} + y^{2(l+1)/3} + x^{(l+1)/3} = 0$	$l \equiv 2 (\mathrm{mod}\, 3)$	$\langle (2l+1)/3, l, l+1 \rangle$

Выводы. Максимальные плоские кривые представлены только в квадратичном поле F_q, $q = l^2$. Не существует максимальных кривых рода $g > \sqrt{q}(\sqrt{q} - 1)/2$. Кривой максимального рода является кривая Эрмита.

Список использованных источников

1. Weil A. Courbes algebriques et varietes abeliennes / Weil A.// Hermann, Paris, -1971.
2. Lachaud G. Sommes d'Eisenstein et nombre de points de certaines courbes algebriques sur les corps finis / Lachaud G. //C.R. Academy Science, Paris. - 1987, Vol.305, Series 1, - P.729-732.
3. Ihara Y. Some remarks on the number of rational points of algebraic curves over finite fields / Ihara Y.// J. Fac. Science, Tokio. – 1981, Vol. 28, -P.721–724.
4. Vladut S.G. Number of points of an algebraic curve / Vladut S.G., Drinfeld V.G. // Function Analyse. – 1983, - Vol.17(1), - P.68–69.
5. Giulietti M. A new family of Fq2 -maximal curves / Giulietti M., Korchmaros G. // prep., 2007.

УДК 681.3.06

Халимов Г.З., Котух Е.В.

ФУНКЦИОНАЛЬНОЕ ПОЛЕ КРИВОЙ СУЗУКИ ДЛЯ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ

Рассматривается универсальное хеширование на функциональном поле кривой Сузуки. Обобщены основные результаты по максимальным кривым ассоциированным с группой Сузуки и группой Ри.

Максимальные кривые ассоциированные с группой Сузуки и группой Ри имеют максимально возможное значение рода и соответственно число точек. Проблематикой универсального хеширования на функциональном поле $F_q(C)$ алгебраической кривой C над конечным полем F_q является определение проективного многообразия точек кривой, поля рациональных функций и оценка параметров семейства хеш функций. Целью данной работы является оценка основных параметров кривой Сузуки, определение рациональных функций базисного пространства ассоциированного с точками кривой.

1. Определение и свойства кривой Сузуки

Кривые Сузуки S являются F_q изоморфными плоской кривой

$$y^q - y = x^{q_0}(x^q - x),$$

где $q = 2q_0^2$ и $q_0 = 2^s$. Род кривой $g = q_0(q-1)$ и число F_q рациональных точек равно $q^2 + 1$.

Главный результат по кривым Дэлигнэ-Лустига второго типа ассоциированных с $Sz(q)$ определяется следующей теоремой.

Теорема 2. [1] Для положительного целого s заданы $q = 2q_0^2$ и $q_0 = 2^s$. Пусть X кривая над F_q рода g и удовлетворяются следующие условия

1. $g = q_0(q-1)$;
2. $\# X(F_q) = q^2 + 1$.

Тогда X является F_q изоморфной кривой Дэлигнэ-Лустига ассоциированной с группой Сузуки $Sz(q)$.

Кривая Дэлигнэ-Лустига ассоциированная с группой Сузуки определяется полной линейной серией $D=\left|(q+2q_0+1)P_0\right|$ размерности $\dim=4$ и степени $q+2q_0+1$, которая выводится из энумератора Зета функции [2]. Отображение кривой Сузуки на проективное пространство P^4 и подгруппа Вейерштрасса $H(P)$, $P\in X(F_q)$ рассмотрены в работах [1,2-4].

2. Функциональное поле кривой Сузуки

Основные результаты обобщены в утверждении 1.

Утверждение 1. F_q рациональный морфизм кривой Сузуки в P^4 есть отображение

$$\pi := (1:x:y:v:w),$$

где x,y,v,w определяются уравнениями [2]

$$y^q - y = x^{q_0}(x^q - x),$$

$$v := x^{2q_0+1} + y^{2q_0},$$

$$w := xy^{2q_0} + x^{2q+2q_0} + y^{2q},$$

и порядки полюсов равны

$div_\infty(x) = qP_0$, $div_\infty(y) = (q+q_0)P_0$, $div_\infty(v) = (q+2q_0)P_0$, $div_\infty(w) = (q+2q_0+1)P_0$.

Кривая Сузуки может быть представлена в P^4 множеством точек вида

$$P_{(a,b)} := (1:a:b:f(a,b):af(a,b)+b^2)\cup\pi(P_0) = (0:0:0:0:1),$$

где $a,b\in F_q$ и $f(a,b) := a^{2q_0+1} + b^{2q_0}$ [3,4].

Подгруппа Вейерштрасса $H(P)$, $P\in C(F_q)$ функционального поля кривой содержит подгруппу [2]

$$H(P) = \langle q, q+q_0, q+2q_0, q+2q_0+1\rangle.$$

Доказательство. Покажем подгруппу Вейерштрасса. Для этого запишем уравнение кривой в проективных координатах

$$Y^qZ^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1}Z^{q+q_0-1}. \quad (1)$$

На кривой C существуют особая точка на бесконечности $P_0=(0:1:0)$ кратности q_0 и рациональные точки $P_{\alpha,0}=(\alpha:0:1)$ $P_{0,\beta}=(0:\beta:1)$, где $\alpha,\beta\in F_q$.

Пусть $\aleph$ является линией с уравнением $X=0$. Тогда $\aleph$ пересекает кривую в точках $P_{0,\beta}$ и P_0. Число точек $P_{0,\beta}$ равно q. Линия $\aleph$ имеет только однократные пересечения в точках $P_{0,\beta}$, так как $X=0$ не является касательной в этих точках. По теореме Безу кратность пересечения линии $\aleph$ с кривой C равна $q+q_0$. Отсюда следует, что $\aleph\cdot C = \sum_{\beta\in F_q} P_{0,\beta} + q_0P_0$.

Рассмотрим линию $\Re$ с уравнением $Y=0$. $\Re$ пересекает кривую C в точках $P_{\alpha,0}$ и в точке $P_{0,0}=(0:0:1)$ является касательной кратности пересечения q_0+1, следовательно $\Re\cdot C = \sum_{\alpha\in F_q,\alpha\neq 0} P_{\alpha,0} + (q_0+1)P_{0,0}$. Для линии $\Im$ с уравнением $Z=0$ имеем пересечение с кривой только в одной точке $P_0=(0:1:0)$ и $\Im\cdot C = (q+q_0)P_0$.

Для рациональных функций $x=X/Z$ и $y=Y/Z$ получим следующие дивизоры

$$div(x) = \sum_{\beta\in F_q} P_{0,\beta} + qP_0,\ div(y) = \sum_{\alpha\in F_q,\alpha\neq 0} P_{\alpha,0} + (q_0+1)P_{0,0} - (q+q_0)P_0$$

соответственно $div_\infty(x) = qP_0$ и $div_\infty(y) = (q+q_0)P_0$ значение полюса дивизоров.

Рассмотрим уравнение $v := x^{2q_0+1} + y^{2q_0}$. Имеем

$$y = (v - x^{2q_0+1})^{1/2q_0}.$$

Подставим в $y^q - y = x^{q_0}(x^q - x)$ и после преобразований получим

$$v^q - v = x^{2q_0}(x^q - x).$$

Запишем уравнение в проективных координатах

$$V^q Z^{2q_0} - VZ^{q+2q_0-1} = X^{q+2q_0} - X^{2q_0+1} Z^{q-1}. \qquad (2)$$

Уравнение (2) также как и уравнение кривой (1) имеет q^2+1 число решений в F_q.

Рассмотрим линию Ψ с уравнением $V=0$. Ψ пересекает кривую C в точках $P_{\alpha,\beta}$, $\alpha^{2q_0+1} + \beta^{2q_0} = 0$ и в точке $P_{0,0} = (0:0:1)$ является касательной кратности пересечения $2q_0+1$, следовательно $\Re \cdot C = \sum_{\alpha,\beta \in F_q, \alpha^{2q_0+1}+\beta^{2q_0}=0} P_{\alpha,\beta} + (2q_0+1)P_{0,0}$. Для линии $\Im$ с уравнением $Z=0$ имеем пересечение с кривой $V^q Z^{2q_0} - VZ^{q+2q_0-1} = X^{q+2q_0} - X^{2q_0+1} Z^{q-1}$ только в одной точке $P_0 = (0:1:0)$ и $\Im \cdot C = (q+2q_0)P_0$. Для рациональной функций $v = V/Z$ получим дивизор

$$div(y) = \sum_{\alpha \in F_q, \alpha \neq 0} P_{\alpha,0} + (2q_0+1)P_{0,0} - (q+2q_0)P_0$$

и $div_\infty(y) = (q+2q_0)P_0$ значение полюса дивизора.

Определим $w := y^{2q_0} x + v^{2q_0}$. Уравнение от переменных w, y, x имеет вид

$$w^q - w = y^{2q \cdot q_0} x^q + v^{2q \cdot q_0} - y^{2q_0} x - v^{2q_0} = y^{2q_0}(x^q - x)$$

Порядок полюса функции w в точке P_0 получим с использованием следующих свойств дискретной оценки ϑ_P для рациональных функций:

a) $\vartheta_{P_0}(xy) = \vartheta_{P_0}(x) + \vartheta_{P_0}(y)$ (см. определение I.1.9 стр. 4, [5]);

b) оценка ϑ_P рациональных функций x, y в уравнении $y^q + \mu y = f(x)$ над $F_q, q = p^s$ определяется выражением (см. VI.4.1 стр. 200, [5]) $q\,\vartheta_{P_0}(y) = \vartheta_{P_0}(y^q + \mu y) = \vartheta_{P_0}(f(x))$.

Вычислим оценку ϑ_P для $w^q - w$

$$\vartheta_{P_0}(w^q - w) = \vartheta_{P_0}(y^{2q_0}(x^q - x)) = \vartheta_{P_0}(y^{2q_0}) + \vartheta_{P_0}(x^q - x).$$

Так как $\vartheta_{P_0}(x) = div_\infty(x) = q$ и $\vartheta_{P_0}(y) = div_\infty(y) = q + q_0$ получим

$$q\,\vartheta_{P_0}(w) = (q+q_0)2q_0 + q \cdot q = q(q+2q_0+1)$$

и значение полюса дивизора $div_\infty(w) = q + 2q_0 + 1$.

Отсюда следует, что подгруппа Вейерштрасса $H(P)$, $P \in C(F_q)$ функционального поля кривой содержит подгруппу $H(P) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle$. Число точек разрыва определяет род кривой $|G(P_0)| = \#(N \setminus H) = q_0(q-1)$ [2]. Линейная серия $q, q+q_0, q+2q_0, q+2q_0+1$ является полной, размерности $\dim = 4$ и определяется рациональными функциями $x, y, v, w \in F_q(C)$.

Рассмотрим представление точек кривой Сузуки. Для $P \in C(F_q) \setminus P_0$ пусть $a := x(P), b := y(P)$ и $f(a,b) := v(a,b) = a^{2q_0+1} + b^{2q_0}$. Уравнение для $w := y^{2q_0} x + v^{2q_0}$ приводится к виду $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$. Тогда $w(a,b) := af(a,b) + b^2$.

Список использованных источников

1. Torres F. The Deligne-Lusztig curve associated to the Suzuki group / Torres F. // arXiv:alg-geom/9706012v1 26Jun. - 1997

2. Hansen J.P. Group codes on certain algebraic curves with many rational points / Hansen J.P.; Stichtenoth H.// AAECC 1. – 1990. - P.67–77.

3. Tits J. Ovoıdes et groupes de Suzuki / Tits J. // Arch. Math. – 1962. Vol.13, - P.187–198.
4. Penttila, T. Ovoids of parabolic spaces / Penttila, T., Williams, B. //preprint. - 1997.
5. Stichtenoth H. Algebraic function fields and codes / Stichtenoth H. // Springer-Verlag, Berlin. - 1993.

УДК 681.3.06
Халимов Г.З., Иохов А.Ю.

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО РАЦИОНАЛЬНЫМ ФУНКЦИЯМ КРИВОЙ ЭРМИТА

Рассматривается универсальное хеширование по кривым Эрмита. Представлены оценки вероятности коллизии и алгоритм вычисления хеш кодов.

Не существует плоских максимальных кривых рода $g \ge q$ над полем F_q [1]. По классификации максимальных плоских кривых кривая Эрмита является кривой первого рода $g = g_1 < q$. Универсальное хеширование реализуется вычислениями в функциональном поле алгебраических кривых. Наилучший результат достигается на кривой Эрмита [2,3]. Проблематикой универсального хеширования на функциональном поле $F_q(C)$ алгебраической кривой C над конечным полем F_q является определение функции хеширования, алгоритма вычисления хеш кода и оценка параметров. Целью данной работы является построение универсального хеширования на функциональном поле кривой Эрмита, оценка основных параметров хеширования и построение практического алгоритма вычислений.

1. Определение универсального хеширования по кривой Эрмита

Известные результаты.

- Кривая Эрмита над конечным полем F_{q^2} является несингулярной, определяется уравнением в проективном пространстве P^2

$$F(X,Y,Z) = Y^q Z + YZ^q - X^{q+1},$$

и аффинном пространстве

$$y^q + y = x^{q+1}.$$

- Кривая имеет $(q^3+1)F_{q^2}$ рациональных точек, род $g = q(q-1)/2$ и достигает границы Хассе-Вейля.
- Точками кривой являются $P_\infty = (0:1:0)$ и $P_{a,b} = (a:b:1)$, где $a \in F_{q^2}$ и $b^q + b = a^{q+1}$.
- Подгруппа Вейерштрасса $H(P_\infty)$ в точке P_∞ образуется порядками полюсов $div_\infty(x) = qP_\infty$ и $div_\infty(y) = (q+1)P_\infty$, и $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < ...\}$.
- Базис пространства $L(mP_\infty) = L(\rho_\ell P_\infty)$, $\rho_\ell \le m \le \rho_{\ell+1}$ задается функциями вида $\{x^i \cdot y^j : iq + j(q+1) \le m\}$, это также следует из подгруппы Вейерштрасса $H(P_\infty)$ представленной порядками полюсов функций $x = X/Z$ и $y = Y/Z$.

Определение 1. Хеш функция $h_{x,y}(m) \in F_{q^2}$ для сообщения m по рациональным функциям в точке x, y кривой Эрмита определяется выражением

$$h_{x,y}(m) = \sum_{i \ge 0, 0 \le j \le q-1, i \cdot q + j \cdot (q+1) \le \rho_k} m_{i,j} \cdot x^i \cdot y^j, \qquad (1)$$

где ρ_k полюс подгруппы Вейерштрасса $H(P_\infty)$, $m_{i,j} \in F_{q^2}$ -слова сообщения m.

Замечание 1.

1. Определение хеш функции следует из базиса пространства $L(\rho_\ell P_\infty)$ рациональных функций Эрмитовой кривой.

2. Для теоретической оценки вероятности коллизии необходимо связать значение k с показателями i, j степеней рациональных функций $x^i \cdot y^j$.

Лемма 1. Пусть $k < q(q-1)/2$, тогда $j = k - s(s-1)/2$, $i = s - j$ и $s = \left\lceil (2k+1/4)^{1/2} - 1/2 \right\rceil$, где $\lceil \cdot \rceil$ округление к большему целому числу.

Замечание 2.

1. В случае $k = q(q-1)/2$ решение уравнения (4) будет $s = q-1$. Отсюда следует $j = 0$ и $i = q-1$.

2. Пусть $k > q(q-1)/2$. В этом случае $j = \overline{0, q-1}$ и $j = 0$, если $k = q(q-1)/2$. Просто показать, что $j = (k - q(q-1)/2) \bmod q$ и $i = q - 1 + (k - q(q-1)/2 - j)/q$.

Утверждение 1. Хеширование по рациональным функциям кривой Эрмита над полем F_{q^2} определяет универсальный хеш класс $\varepsilon - U(q^3, q^{2k}, q^2)$, где q^3 - число хеш функций (объём ключевого пространства), q^{2k} - объём пространства сообщений, q^2 - объём пространства хеш кодов. Вероятность коллизии ε определяется соотношениями

$$\varepsilon = k/q^3 + s/q^2 - s(s-1)/(2q^3), \text{ если } k < q(q-1)/2, \quad (2)$$

$$\varepsilon = k/q^3 + 1/(2q) - 1/(2q^2), \text{ если } k \geq q(q-1)/2, \quad (3)$$

где $s = \left\lceil (2k+1/4)^{1/2} - 1/2 \right\rceil$ есть округление значения до наибольшего целого.

Замечание 3.

1. Выражения для вероятности коллизии для универсального хеширования по рациональным функциям кривой Эрмита являются точными.

2. Утверждение 1 впервые представлено в [4]. Соотношения (2),(3) здесь изложены в другой интерпретации.

Следствие 1. Асимптотика вероятности коллизии универсального хеширования по кривым Эрмита, когда, при больших значениях размерности поля $q \to \infty$ имеет вид

$$\varepsilon_{q\to\infty} = k^{1/2}/q^2, \text{ если } k < q(q-1)/2 \quad (4)$$

$$\varepsilon_{q\to\infty} = 1/q + k'/q^3 - 1/q^2, \text{ если } k \geq q(q-1)/2, \quad (5)$$

где $k' = k - q(q-1)/2$.

Замечание 4.

1. Для универсального хеширования по проективной линии в квадратичном поле оценка для вероятности коллизии равна $\varepsilon = \frac{k}{q^2}$. Асимптотика вероятности коллизии универсального хеширования по кривым Эрмита при малых значениях k определяется отношением корня квадратного длины данных к размерности поля, что $\sqrt{k}$ лучше, по сравнению с хешированием по проективной линии. Хеширование по проективной линии является результативным только до $k = q^2$.

2. Вероятность коллизии универсального хеширования по кривым Эрмита при больших значениях $k \geq q(q-1)/2$ имеет нижнюю границу $\varepsilon = 1/q$ и допускает хеширование до $k = q^3 - q(q-1)/2 \approx q^3$, что в корень квадратный от размерности поля больше по сравнению с хешированием по проективной линии.

2. Практический алгоритм вычисления хеш кодов

Порядок назначения точек кривой Эрмита и практический алгоритм вычисления хеш кода определяется предложениями 1 и 2.

Предложение 1. Пусть кривая Эрмита над конечным полем F_{q^2} задана уравнением $y^q + y = x^{q+1}$. Тогда точки кривой $P_{a,b} = (a:b:1)$ определяются выражениями

$$b = \alpha^{i\cdot(q-1)+j}, \; a = \alpha^{s+t(q-1)}, \quad \textbf{(6)}$$

где $i = \overline{0,q}$, $j = \overline{0,q-2}$, $t = \overline{0,q}$, $\alpha^{s\cdot(q+1)} = tr(b)$, $\alpha \in F_{q^2}$.

Предложение 2. Алгоритм универсального хеширования по кривым Эрмита в F_{q^2} определяется схемой Горнера вида

$$h_{x,y}(m) = \sum_{j=0}^{s} y^j \cdot \sum_{i=0}^{s-j} m_{i,j} \cdot x^i \ , \tag{7}$$

со сложностью

$$N_{опер} = k + s \text{, если } k < q(q-1)/2 \text{,} \tag{8}$$

$$N_{опер} = k + q \text{, если } k \geq q(q-1)/2 \text{,} \tag{9}$$

где $s = \left| (2k + 1/4)^{1/2} - 1/2 \right|$.

Замечание 5.

1. Соотношения (6) для определения точек кривой Эрмита являются новыми.

2. Применение схемы Горнера для хеширования по кривой Эрмита и оценки сложности вычислений (8), (9) впервые представлены в [4]. Доказательство предложения 2 является простым.

3. Асимптотика оценки сложности универсального хеширования по кривым Эрмита при $k < q(q-1)/2$ определяется $N_{опер}(HC) = k + k^{1/2}$, так как $s = \left| (2k + 1/4)^{1/2} - 1/2 \right|$.

В алгеброгеометрической интерпретации универсальное хеширование по проективной линии для сообщения $m = (m_0, m_1, ..., m_k)$, $m_i \in F_{q^2}$ определяется выражением

$$h_x(m) = \sum_{i=0}^{k-1} m_i \cdot x^i \ , \tag{14}$$

где x точки проективной прямой.

Сложность вычислений (7) по схеме Горнера равна $N_{опер}(PS) = k$. Хеширование по кривой Эрмита по сравнению с хешированием по проективной прямой сложнее на $N_{опер}(HC) - N_{опер}(PS) = k^{1/2}$ операций. Относительное увеличение сложности вычислений является несущественным $N_{опер}(HC) / N_{опер}(PS) = 1 + k^{-1/2}$.

Список использованных источников

1. Cossidente A. Curves of large genus covered by the Hermitian curve / Cossidente A., Korchmaros G. and Torres F. // Comm. Algebra. – 2000. -Vol. 28(10). P.4707–4728.

2. Халимов Г.З. Каскадное универсальное хеширование с использованием АГК кодов /Халимов Г.З., Иохов А.Ю.// Восточно-европейский журнал передовых технологий. – Х., 2005. – Вып. 2/2(14). – С. 111–119.

3. Халимов Г.З. Аутентификация с применением алгеброгеометрических кодов. / Халимов Г.З.,.Кузнецов А.А. //Радиотехника. Всеукр. межвед. науч.-техн. сб.- 2001.- Вып. 120.- С. 103-109.

4. Халимов Г.З. Аутентификация с применением Эрмитовых кодов. /Халимов Г.З., Иохов А.Ю. // Вестник ХПИ. – Х., -2005. НТУ „ХПИ”. –Вып. 9. –С. 26-32.

УДК 623.618

Іохов О.Ю., Руденко А.Л.

НАПРЯМКИ РОЗВИТКУ ЗАСОБІВ РАДІОЗВ’ЯЗКУ В ТАКТИЧНІЙ ЛАНЦІ УПРАВЛІННЯ ВНУТРІШНІХ ВІЙСЬК МВС УКРАЇНИ

Аналіз сучасних систем та засобів радіозв’язку провідних фірм-виробників. Можливі шляхи розвитку системи зв’язку внутрішніх військ МВС України

Сучасний рівень розвитку внутрішніх військ (ВВ) МВС України, якісні зміни у способах і засобах ведення операцій поставили питання щодо вдосконалення системи управління в число найважливіших. Технічною основою системи управління ВВ, її невід'ємною складовою частиною є система зв'язку та автоматизації. Вона значною мірою визначає ступінь реалізації бойового потенціалу ВВ.

У перспективних комплексах радіозв'язку необхідно використовувати схеми зв'язку, що забезпечують багатостанційний доступ чи повно доступне підключення великої кількості абонентів до обмеженого числа каналів зв'язку Такі системи можуть застосовуватися для організації групового зв'язку рухомих абонентів, а також індивідуальних переговорів. У такій радіосистемі кожному абоненту для зв'язку може бути наданий будь-який із вільних каналів. Усі канали об'єднані загальною системою управління, яка слідкує за каналами, що звільняються, й відразу надає їх наступним абонентам.

Аналіз сучасних систем та засобів радіозв'язку провідних фірм-виробників (Harris – США, Tadiran – Ізраїль, Codan – Австралія, ВАТ„ Концерн Сузір'я"– Росія та ін.) свідчить про те, що при створенні вітчизняних радіозасобів повинні виконуватись наступні вимоги: застосування єдиної базової радіостанції; локальне та дистанційне управління радіозасобами; сучасна елементна база з експлуатаційними характеристиками, що відповідають світовим військовим стандартам; єдині способи аналого-цифрового та цифро-аналогового перетворення мови; засекречування інформації; підвищення пропускної спроможності систем і засобів радіозв'язку; можливість створення автоматизованих (автоматичних) радіоцентрів; підвищення надійності засобів і комплексів радіозв'язку; використання вдосконалених алгоритмів управління, інформаційного і програмного забезпечення; реалізація нових завадо- і розвідзахищених алгоритмів роботи засобів і комплексів радіозв'язку; створення уніфікованих перепрограмованих засобів радіозв'язку, в тому числі для взаємодії радіоцентрів ВВ МВС України та з іншими зацікавленими відомствами; застосування компенсаторів завад і коригуючих кодів; сполучення з опорною мережею ВВ МВС України, з мережами загального користування, комп'ютерними мережами; можливість попереднього настроювання не менше ніж на 100 симплексних або напівдуплексних каналів з кроком частот не більшим 10 Гц; режими ППРЧ; функціональна повнота– портативні, переносні та перевізні радіозасоби; автоматизація процесів встановлення, ведення та відновлення зв'язку; пріоритетність обслуговування абонентів; використання панелей управління з мінімальною кількістю органів управління; наявність вмонтованої апаратури навігації (GPS-приймач та ін.); зменшення енергоспоживання, маси та габаритів.

Задовольнити зростаючі вимоги до якості радіозв'язку у внутрішніх військах МВС України в цілому і в тактичній ланці управління зокрема можливо тільки шляхом розробки та реалізації комплексної програми зі створення єдиного інформаційного простору, де система радіозв'язку буде представлена як його мобільний компонент. Очевидно, що для виконання сучасних вимог до радіозв'язку необхідні сучасні засоби і комплекси, які мають бути побудовані на єдиному базовому ряду уніфікованих програмно-технічних комплексів: стаціонарних, мобільних, переносних, портативних та ін., призначених для оснащення командних пунктів рівнів з'єднання, частина, підрозділ, командирські машини (командирів рот, взводів, відділень), окремих військовослужбовців.

УДК 681

Закора О.В., **Селеенко Е.Е., Фещенко А.Б.**

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПРОЦЕДУР СИТУАЦИОННОГО УПРАВЛЕНИЯ

Обычно понятие ситуационного управления применяется к тем аспектам управления, которые связаны большей частью с решением вопросов выхода объектов из кризиса, который уже произошел, т.е. с ликвидацией последствий чрезвычайной ситуации (ЧС).

В штатных ситуациях технологии управления объектами сосредотачиваются на выполне-

нии задач штатного регламента функционирования и одновременно на недопущении нарушений, которые приведут к невозможности функционирования объектов управления по назначению. Кризисные ситуации требуют от органа управления принятия решений относительно стратегии выхода из кризиса и проектирования новой, временной системы для ее реализации.

Таким образом, критическим для системы управления является сам период, когда возникает кризис и надо переходить от технологий штатного управления к технологиям ликвидации последствий кризиса.

С точки зрения обеспечения управления объектом в любой ситуации, технология ситуационного управления не должна отделяться от штатной системы управления, а должна создавать целостную систему, которая поддерживает органы управления в вопросах предупреждения кризиса в штатных ситуациях, в вопросах перехода от штатного к кризисному управлению и в кризисном управлении.

В этой связи, наиболее важным вопросом является дополнение технологии штатного управления системой онлайнового анализа ситуации на объекте.

Четкое определение момента начала ЧС на объекте управления дает возможность органу управления обеспечить своевременный переход от технологии штатного к технологии кризисного управления и создает реальные условия для предотвращения ЧС, поскольку между следствиями нарушений, которые приводят к ЧС, и их причиной существует определенный промежуток времени, которым можно воспользоваться для предупреждения ЧС или уменьшения масштаба ее последствий.

Дерев'янко О.А., **Закора О.В.**, **Селеєнко Е.Е.**, **Фещенко А.Б.**

ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА ГАРАНТОВАНОЇ ДОСТАВКИ ІНФОРМАЦІЇ ДО ЦЕНТРІВ ОБРОБКИ ЕКСТРЕНИХ ВИКЛИКІВ СИСТЕМИ 112

Приведено обґрунтування варіанту побудови системи екстреної допомоги населенню за єдиним телефонним номером 112 при розгортанні спеціального оператора телекомунікацій

В рамках реалізації Державної цільової програми підготовки та проведення в Україні фінальної частини чемпіонату Європи 2012 року з футболу затвердженої Постановою КМУ від 14.04.2010 №357 актуальним є завдання зі створення та впровадження системи екстреної допомоги населенню за єдиним телефонним номером 112.

Основний зміст "Системи 112" полягає в тому, щоб людина, яка опинилась в надзвичайній ситуації не роздумуючи знала, куди звернутися по допомогу, і міг оперативно її одержати. Держава вже веде роботу зі створення в країні Служби 112, яка повинна забезпечити виклик усіх екстрених служб по єдиному номеру, де показник оперативності реагування є основним.

Головне, що для цього потрібно - побудувати інформаційну систему, здатну скоординувати дії всіх оперативних служб, організувати обмін інформацією між ними, а також успішно використовувати досвід, накопичений у колишніх надзвичайних ситуаціях (НС).

Черговий диспетчер служби 112 буде приймати сигнали про надзвичайні ситуації незалежно від їхнього виду - будь те пожежа, техногенна катастрофа або терористичний акт і направляти їх у відповідні оперативні служби. Він також буде координувати дії служб під час рятувальних операцій і консультувати людей, яки опинились в надзвичайній ситуації, як правильно поводитися в умовах, що створилися. Таким чином, і одержання громадянами необхідної допомоги й керування діями рятувальних служб буде здійснюватися з єдиного центру, що підвищить результативність проведення рятувальних операцій і знизить рівень людських і матеріальних втрат.

Ефективність дій рятувальників буде забезпечувати потужна інформаційна система підтримки прийняття рішень. Система буде "видавати" план дій екстрених оперативних служби для даного типу надзвичайної ситуації й контролювати хід його виконання. Це завдання вимагає від системи здатності працювати з величезною кількістю інформації, щоб з великого

обсягу даних добувати потрібні й робити це в найкоротший термін.

Існуюча телекомунікаційна система доставки екстрених викликів (101,102,103,104) організована через спецвузли Укртелекому, яки на даний час вже перезавантажені, мають обмежену пропускну спроможність, та швидкість передачі інформації. В перспективі не ясна ситуація з приватизацією державного підприємства Укртелеком.

Самі великі проблеми, які можна й потрібно вирішувати в першу чергу засобами інформаційних технологій – це перевантаженість диспетчерських служб, телефонних мереж загального користування (ТМЗК) особливо в часи “пік” або святкові дні потоком одночасних викликів від громадян. За цим іде - людські помилки операторів, які позбавлені оперативної інформації, неможливість вчасного надання допомоги потерпілим, та загибель людей, колосальні матеріальні збитки під час НС. Крім того існує нормативна та законодавча невизначеність з доставкою аварійних сигналів від Систем пожежної та техногенної автоматики до Системи 112.

Потрібна концентрація та маршрутизація усіх можливих технічних форм та способів екстрених викликів від осіб з фізичними вадами. (SMS, I-mail, факс, прямі кнопки, аварійні GPS системи безпеки автомобіля та інші). З метою підвищення надійності роботи та гарантованості доставки інформації до центрів обробки екстрених викликів системи 112 потрібне забезпечення резервування доставки викликів (сигналів) на дублюючі регіональні Центри Системи 112. у випадку відмови, перевантаження основного.

Для вирішення зазначених проблем на основі європейського досвіду пропонується на базі ресурсу ТМЗК створити Спеціальний оператор телекомунікацій (СОТ), який буде складовим елементом системи екстрених телекомунікацій. СОТ уявляє собою вузол концентрації та подальшої маршрутизації екстрених мультимедійних викликів від абонента (автоматики) через виділену мережу оператора телекомунікацій до оператора Системи 112. При цьому оператори телекомунікацій ТМЗК створюють власну виділену мережу екстрених телекомунікацій.

Основними завданнями та функціями СОТ повинні бути:

- забезпечення гарантованої доставки голосового екстреного виклику за номерами 101,102,103, 112 від абонента телефонної мережі загального користування до оператора Системи 112;
- забезпечення гарантованої доставки сигналів телеметрії від систем автоматичної пожежної сигналізації та інших систем раннього виявлення надзвичайної ситуації (НС) до оператора Системи 112;
- забезпечення резервування доставки екстрених викликів до дублюючих регіональних Центрів 112 та організація пріоритетних міжнародних зв'язків у період НС відповідно до плану нумерації;
- спільно з операторами телекомунікацій побудова виділеної (накладеної) мережі екстрених телекомунікацій;
- організація Call центра для надання населенню інформаційних послуг.

Техніко економічне обґрунтування свідчить, що СОТ в сучасних умовах доцільно створювати підприємством, яке займається комерційною діяльністю. Для розгортання підприємства необхідно придбати та змонтувати телекомунікаційне обладнання із розрахунку 2 млн. грн. на кожен обласний центр, тобто необхідно інвестицій орієнтовно 60-65 млн.

Основним джерелом надходжень для утримання СОТ є між операторські розрахунки за гарантовану доставку аварійних сигналів від систем пожежної та техногенної автоматики до Системи 112 на підставі укладених угод з власниками пультів пожежного та техногенного спостерігання.

Закора О.В., Селеенко Е.Е., Фещенко А.Б.

ПРОГНОЗИРОВАНИЕ ДАЛЬНОСТИ РАДИОСВЯЗИ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ СИЛ ОХРАНЫ ПРАВОПОРЯДКА

Одной из важных задач, решаемых в процессе организации радиосвязи в системе опове-

щения сил охраны правопорядка, является определение потенциальной дальности УКВ-радиосвязи между подразделениями в тех или иных. Решение данной задачи требует учета множества факторов, влияющих на дальность распространения ультракоротких волн (УКВ), таких как влияние местных предметов и рельефа местности, затухание радиоволн в процессе распространения и поглощения в атмосфере и др.

В наш час известно множество отечественных и зарубежных исследований и методик в данной области, позволяющих решить задачу прогнозирования потерь распространения радиоволн (РРВ) с той или иной степенью достоверности. Однако наибольший, по-видимому, интерес в данной области представляют соответствующие наработки авторитетного международных органа - Международного союза электросвязи (МСЭ - специализированного учреждения ООН, англ. International Telecommunication Union, ITU), который обеспечивает координацию между разными странами вопросов совместного использования радиочастотного ресурса. По состоянию на сентябрь 2010 года в МСЭ входит 192 страны, в том числе и Украина. Разрабатываемые МСЭ стандарты в области радиосвязи (по терминологии МСЭ - "рекомендации") не являются обязательными для стран-участниц, но широко поддерживаются, так как позволяют облегчить решение вопросов взаимодействие между сетями связи по всему миру.

Применительно к диапазонам, используемым МВД для организации радиосвязи, представляет интерес рекомендация ITU-R P.1546 "Метод прогнозирований передач для наземных служб в диапазоне частот от 30 до 3000 МГц" (далее – Рекомендация).

Рекомендация обеспечивает учёт энергетических параметров и характеристик приемопередающих устройств и позволяет прогнозировать величину напряжённости электромагнитного поля (ЭМП), создаваемой передатчиком мощностью 1 кВт эквивалентной излучаемой мощности (э.и.м.) в районе приёмной антенны. В основе прогнозирования лежат графики (кривые), учитывающие зависимость напряжённости поля от факторов, определяющих характер РРВ. Графики основаны на статистическом анализе экспериментальных данных и учитывают результаты многолетних наблюдений закономерностей РРВ в различных регионах земного шара. Кривые отражают результаты измерений, большей частью относящихся к климатическим условиям умеренных регионов, содержащих холодные и теплые моря. Кривые для сухопутных трасс были подготовлены по данным, полученным большей частью в климатических условиях Европы и Северной Америки. МСЭ периодически обновляет эти данные с введением необходимых поправок и корректировок.

Кривые дают статистические оценки значений напряженности поля на средних частотах 100, 600 и 2000 МГц (рис.1), действительные для диапазонов частот (30 – 300), (300 – 1000) и (1000 – 3000) МГц соответственно. Кривые изображают значения напряженность поля для сухопутных и морских трасс РРВ в зависимости от дистанции связи при определенных условиях:

- обеспечивается превышение прогнозируемого значения напряженности в 50% мест в пределах области 200 на 200 м в течение 1, 10 или 50% времени;

- для заданной эффективной высоты передающей/базовой антенны h_1, которая определяется как высота антенны над средней высотой местности на интервале дальностей от 3 до 15 км в направлении на приемную/мобильную антенну. Напряженности поля даны для значений h_1 от 10 до 1200 м;

- для заданной высоты приемной/мобильной антенны h_2, которая приравнивается "характерному" значению средней высоты поверхности земли в районе расположения приёмной антенны. Минимальное значение характерной высоты - 10 м.

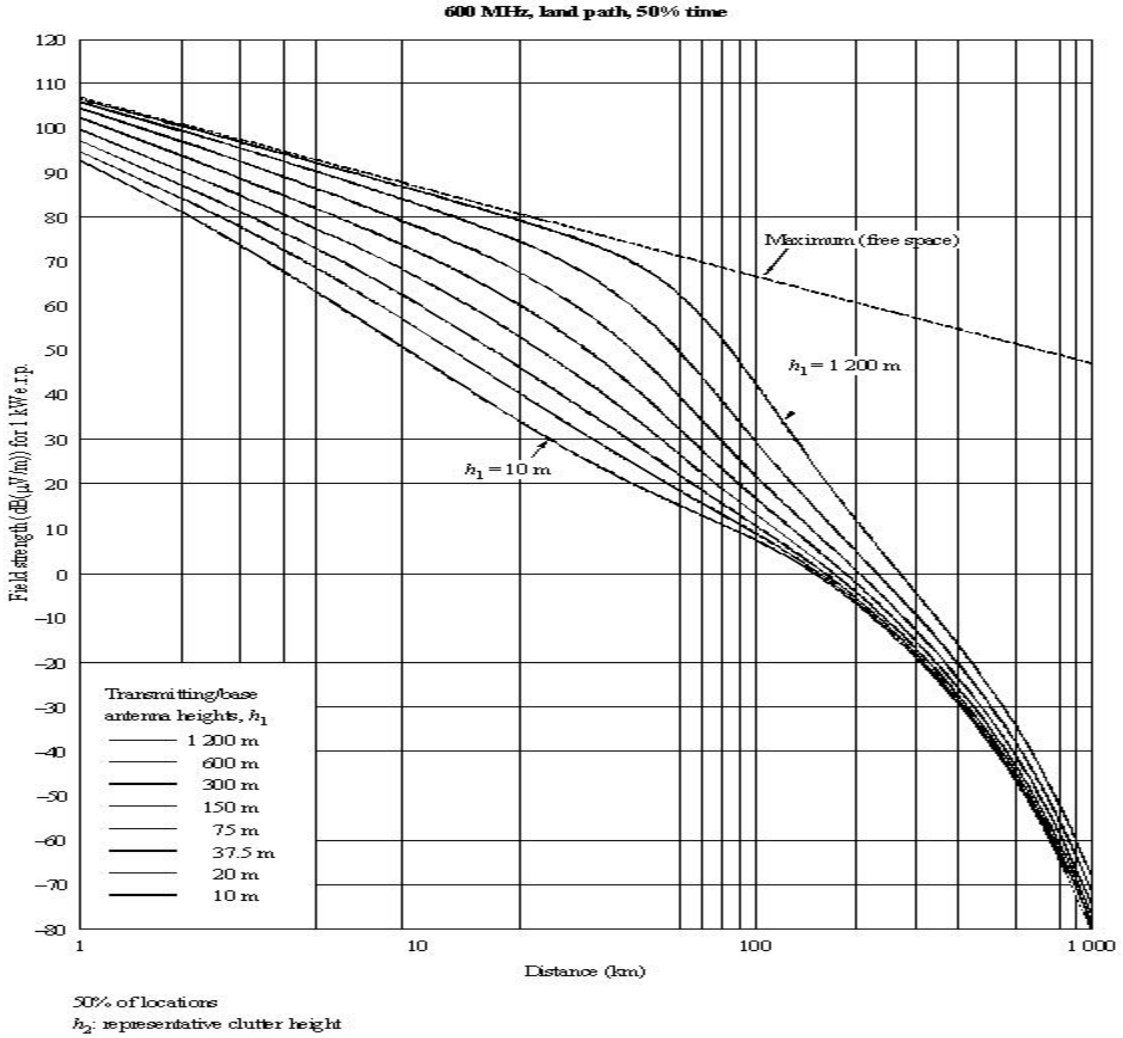


Рис. 1. Прогноз напряженности поля для частоты 600 МГц

Конечно, параметры данных кривых охватывают не все практические случаи проведения расчётов. Для уточнения результатов прогнозирования в зависимости от тех или иных факторов Рекомендацией предусмотрен ряд поправок:

- интерполяция или экстраполяция значения напряженности поля, как функции частоты (для частот, отличных от 100, 600 и 2000 МГц);
- интерполяция значения напряженности поля, как функции процента времени;
- интерполяция значения напряженности поля, как функции процента расположения;
- интерполяции или экстраполяция значения напряженности поля, как функции значений высоты h_1 (для значений h_1, отличных от заданных значений);
- коррекция значения напряженности поля, соответствующая значениям высоты приемной/мобильной антенны, отличным от характерного значения средней высоты антенны над землей h_2;
- повышение точности прогнозирования напряженности поля за счёт учета угла закрытия местности (поправка на угол закрытия) и др.

Следует отметить, что представленные выше графики не учитывают ряд существенных параметров приёмо-передатчиков, влияющих на дальность радиосвязи, таких, как реальное ослабление сигналов в фидерных трактах и усиление сигналов антеннами. Учёт этих факторов производится отдельно в процессе расчёта дальности.

Расчёт дальности, в свою очередь, может быть осуществлён на основе известного в радиотехнике соотношения для действующего значения напряжённости поля в районе приёмной антенны. Задаваясь пороговой величиной напряжённости поля $E_{min\_Д,дБ/мкВ/м}$, обеспечи-

вающей нормальное функционирование радиоприёмника, получим выражение для расчёта условного значения напряжённости для соответствующих условий обеспечения радиосвязи:

$$E_{ГрАдБ/мкВ/м} = E_{min\_ДдБ/мкВ/м} - B_{MдБ} + B_{ослдБ} + \eta_{TдБ} + \eta_{RдБ} - G_{TдБ} - G_{RдБ} + 3. \quad (1)$$

где $E_{ГрА,дБ/мкВ/м}$ - напряжённость поля, создаваемого передатчиком с э.и.м. 1000 Вт (30 дБ/Вт) на удалении D от антенны передатчика, дБ/мкВ/м; амплитудное значение; определяется по графику (рис. 1);

$B_{M,дБ}$ - коэффициент, который показывает, на сколько дБ мощность передатчика превышает "эталонное" значение э.и.м. 30 дБ/Вт;

$B_{осл,дБ} > 0$ - коэффициент ослабления напряжённости рельефом местности, дБ;

$\eta_{T,дБ} > 0, \eta_{R,дБ} > 0$ - соответственно коэффициенты ослабления (потерь) сигнала в фидерах передатчика (трансивера) и приёмника по напряжению, дБ;

$G_{T,дБ} > 0, G_{R,дБ} > 0$ - коэффициенты усиления по напряжению диаграмм направленности антенн передатчика и приёмника соответственно, дБ.

Методика определения дальности включает два этапа:

- на первом, на основании исходных данных – параметров приёмо-передатчиков и трассы РРВ из выражения (3) рассчитывается условное значение напряжённости поля для соответствующих условий обеспечения радиосвязи;
- на втором, по графикам (рис1) для соответствующего диапазона частот и высот антенн определяется максимальная дистанция радиосвязи. Выбор нужного графика из соответствующего семейства производится по эффективной высоте антенны передатчика.

Дополнительное повышение точности оценок дальности может быть достигнуто при использовании перечисленных выше поправок и корректировок.

Таким образом, данная методика расчёта дальности УКВ радиосвязи учитывает рекомендации МСЭ по расчёту затухания сигналов на трассе РРВ. Данная методика может быть использована как при проведении ручных расчётов, так и для программной автоматизации (на основе ПЭВМ) процессов, требующих расчёта дальности радиосвязи между подразделениями сил охраны правопорядка.

Сергєєв О.Ю.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОРГАНІЗАЦІЇ ОЦІНЮВАННЯ ЯКОСТІ НАВЧАЛЬНИХ ЗАНЯТЬ

Реформа освіти, що відбувається, вимагає використовування принципово нових педагогічних технологій. Успіх діяльності в умовах ринку визначається умінням ухвалювати нестандартні рішення, рішучістю, енергійністю, заповзятливістю. Ці якості важко сформувати без індивідуалізації і диференціації навчання, без урахування інтересів, схильностей і здібностей студентів. Рішення даних задач викликає необхідність пошуку засобів розкриття індивідуальності особи. Досвід західної системи освіти примушує звернутися до практики тестування, яка набула широке поширення в учбово-виховному процесі

Тест принципово відрізняється від звичного контролю знань тим, що до його безпосереднього застосування необхідно заздалегідь приготувати еталонні відповіді, з якими порівнюють відповіді студента. Еталон необхідний для точного визначення ступеня засвоєння студентом змісту навчання, яка характеризується коефіцієнтом засвоєння, який може бути розрахований по формулі:

$$K = \frac{e}{p},$$

де e - число операцій тесту, виконаних студентом правильно,

p – загальне число операцій в тесті.

АСТКЗ розгорнута на базі існуючої локальної (LAN) обчислювальної мережі та дозволяє викладачеві централізовано завантажувати тестові завдання та контролювати хід та результати їх виконання.

Апаратне забезпечення системи включає :

- Робоче місце викладача – ПЕОМ архітектури IBM PC з комунікаційним обладнанням;
- Робочі місця тих хто тестується – ПЕОМ архітектури IBM PC з комунікаційним обладнанням;
- LAN або WAN;

Програмне забезпечення включає :

- Операційну систему Windows 2000/XP з налаштованими мережними підключеннями;
- Модуль управління (серверна частина) який встановлений на робочому місці викладача;
- Модуль тестування (клієнтська частина) який встановлений на робочих місцях тих хто тестується;
- Обмін даними між компонентами системи забезпечується за допомогою протоколу TCP/IP.

Модуль управління АСТКЗ забезпечує:

1. Створення, редагування та зберігання у вигляді файлу тестових завдань;
2. Завантаження тестових завдань ;
3. Встановлення режиму одноразового або багаторазового проходження тесту ;
4. Встановлення режиму перемішування тестових завдань на робочих місцях;
5. Корегування часу на проходження тесту;
6. Здійснення постійного контролю за ходом тестування ;
7. Зберігання результатів тестування у вигляді файлу.

Тестові завдання уявляють собою звичайний текстовий файл з розширенням «**. tsm**» який містить в собі тексти питань та варіанті відповідей розташованих за визначеними правилами.

Під час роботи викладач має можливість контролювати зі свого робочого місця хід тестування. Після закінчення тестування результати (оцінки) тестування зберігаються та можуть бути роздруковані з метою проведення аналізу. Питання, на яки студенти не надали вірну відповідь відображаються на екранах ПК та доповнюються вірними відповідями, що сприяє більш якісному засвоєнню студентами навчального матеріалу.

Щербіна О.О., **Семенов М. І.**

ВИБІР АНТЕН ЗАСОБІВ ЗАХИСТУ РЕСУРСІВ ТА ІНФОРМАЦІЙНИХ ПОТОКІВ ВІД ВИТОКУ

У доповіді представлено короткий аналіз типів антен. Запропоновано використовувати антену витікаючої хвилі, яка відповідає вимогам комплексної системи активного захисту інформації і ресурсів. Представлені результати моделювання і вимірювань

Інформації (ресурсам) необхідний захист від руйнування, підміни, несанкціонованого доступу дистанційного і фізичного. В автономній системі захисту повинні бути засоби придушення каналів витоку, силового впливу, виявлення фізичного вторгнення. Засоби повинні відповідати санітарним нормам і вимогам електромагнітної сумісності (ЕМС). За наявності декількох випромінюючих систем, що працюють в різних діапазонах, є необхідність використовувати одну антену. Для вибору типу антен обмежимо призначення систем захисту і діапазони частот: придушення стільникових телефонів і виявлення вторгнення, діапазони GSM900/1800, 3G, LPD.

Одним з перспективних принципів виявлення фізичного вторгнення визнається активний

радіохвильовий. Способи формування поля в зоні охорони можуть бути різними, одним з них є застосування випромінюючих коаксіальних кабелів – антен витікаючої хвилі. Кабелі можуть розміщуватися в товщі стіни, під зовнішньою обробкою стін приміщень або периметрових загороджень, чим гарантується їх візуальне маскування. Зміна конструктивних параметрів розміщення кабелів дозволяє варіювати не тільки форму, але нахил, ширину і висоту зони виявлення.

Положення зон випромінювання охоронної системи (рис.1) відповідає вимогам до зон придушення. Для заданих цілей можна обрати антену витікаючої хвилі.

У доповіді надані результати моделювання кабельної антени з кутовим екраном і результати вимірювань діаграми спрямованості і захисного відношення у зазначених діапазонах частот. Кутовий екран виконувався з харчової фольги, антенна з кабелю марки РК50-11-14 .

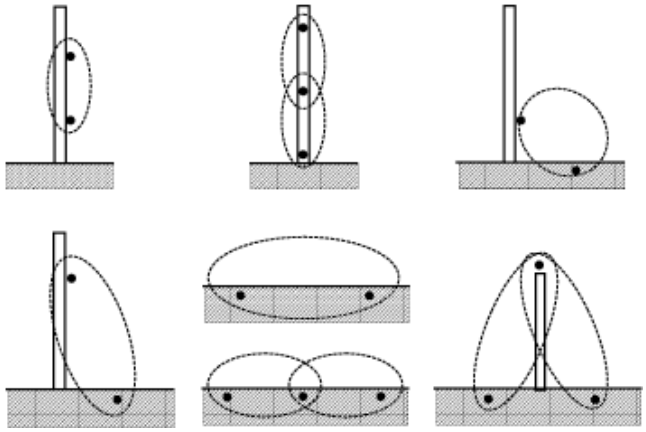


Рис. 1. Варіанти розміщення кабелів антен витікаючої хвилі на периметрі охорони й перетину зони виявлення.

Новикова О.О.

ЗАХИСТ ІНФОРМАЦІЇ ПРИ РОБОТІ З БАЗАМИ ДАНИХ ТА СУБД

Сучасні інформаційні системи дозволяють безлічі користувачів оперувати великими обсягами даних. Для забезпечення швидкої і коректної обробки цих даних до програмного забезпечення, зокрема до СУБД, висуваються наступні вимоги:

1) збереження великих обсягів інтегрованої інформації з різних тематичних напрямків, призначеної для різних користувачів;
2) простота звертань користувачів до БД;
3) можливість модифікації, сортування, фільтрації і пошуку даних за різними критеріями;
4) робота з даними в багатокористувальницькому режимі;
5) модифікованість, тобто можливість розширення і реорганізації даних у БД при змінах у предметній області;
6) мобільність, тобто можливість переносу прикладної системи на нові платформи без яких-небудь змін;
7) достатня продуктивність.

При роботі з БД і СУБД необхідно враховувати такі особливості:

- БД можуть бути фізично розподілені по різних пристроях і вузлах обчислювальної мережі;
- СУБД можуть забезпечувати одночасний доступ багатьох користувачів (клієнтів) до БД за допомогою мережних протоколів, при цьому запити користувача до БД обробляються на сервері і результати обробки направляються користувачам (клієнтам);
- БД можуть включати інформацію різного рівня конфіденційності;
- БД є корпоративним ресурсом, і її необхідно надійно захистити від порушень цілісності даних і несанкціонованого доступу (НСД).

Остання особливість є однією з пріоритетних задач при проектуванні БД.

Під захистом БД в обчислювальних мережах розуміють:

- захист самих даних і їхнє контрольоване використання клієнтами мережі;

- захист будь-якої інформації, що витягається чи генерується з цих даних.

Тому можна виділити наступні об'єкти доступу в СУБД:

1) табличні структури (реальні - таблиці, у яких зберігаються дані, і віртуальні - результати запитів-вибірок і представлення);
2) поля і записи табличних структур, а також окремі значення даних;
3) домени і збережені процедури (розширення стандарту SQL2).

Комплексний підхід до захисту БД полягає в застосуванні організаційних мір і використанні технічних засобів захисту.

До організаційних мір відносяться інвентаризація об'єктів доступу, встановлення їхніх власників, категоризація об'єктів доступу, підбір і підготовка кадрів, оформлення нормативно-розпорядницької документації і т.п.

Класичний комплекс технічних засобів по захисту інформації від НСД включає наступні обов'язкові процедури:

1) забезпечення вірогідності даних (логічна цілісність даних);
2) забезпечення безпеки даних (фізична цілісність даних);
3) забезпечення конфіденційності даних (керування доступом).

Забезпечення вірогідності даних - це система гарантованої схоронності інформації в БД при внесенні ненавмисних помилок і їхнього запобігання. Воно досягається за рахунок перевірки обмежень цілісності - умов, яким повинні задовольняти значення даних при їхньому введенні і модифікації. Реалізація обмежень цілісності виконується СУБД або спеціальними програмними модулями. Відповідно до стандарту SQL2 існують наступні типи обмежень:

1) обов'язкова наявність даних у полі (NULL / NOT NULL);
2) умови на значення стовпця і домена при створенні таблиці і домена (CHECK);
3) унікальність значення первинного ключа (PRIMARY KEY);
4) унікальність стовпців (UNIQUE);
5) обмеження посилальної цілісності на зовнішні ключі (FOREIGN KEY);
6) обмеження на ділові правила і відновлення даних (триггери);
7) обмеження на паралельне виконання операцій (транзакції) і перевірка обмежень цілісності після закінчення внесення взаємозалежних змін.

Забезпечення безпеки даних - це система гарантованої схоронності інформації в БД при програмних чи апаратних збоях. Забезпечення безпеки є внутрішньою задачею СУБД, тому що зв'язано з її нормальним функціонуванням, і тому виконується на рівні СУБД.

Найбільш типовими збоями при роботі з БД є:

1) збій пропозиції;
2) збій користувальницького процесу;
3) збій процесу сервера;
4) збій носія (диска);
5) помилка користувача.

При збоях 1-3 типу СУБД може відновити БД автоматично, а у випадку виникнення збоїв 4-5 типу в процесі відновлення БД задіється людина.

Класичними засобами фізичного захисту даних є резервне копіювання і журнали транзакций.

Резервне копіювання означає періодичне збереження файлів БД на окремому зовнішньому запам'ятовуючому пристрої. Воно виконується тоді, коли стан файлів БД є несуперечливим. У випадку збою БД відновлюється на основі останньої копії. Резервні копії можуть бути:

- повними (всі файли БД);
- частковими (частина БД, визначена користувачем);
- інкрементними (блоки, які змінилися з моменту останнього резервного копіювання).

Створення часткової й інкрементної резервної копії виконується засобами СУБД, а створення повної - засобами СУБД чи ОС (наприклад, за допомогою команди copy).

Періодичність резервного копіювання визначається адміністратором БД і залежить від багатьох факторів: обсяг БД, інтенсивність запитів до БД, інтенсивність відновлення даних та

ін. Як правило, повне копіювання здійснюється раз у тиждень (день, місяць), а часткове чи інкрементне копіювання - раз у день (годину, тиждень).

Основним призначенням журналу транзакций є протоколювання всіх транзакцій і зроблених ними змін. Журнал транзакцій створюється при створенні БД і використовується для її відновлення при виникненні збою.

Журнал транзакцій містить зведення тільки про поточну транзакцію. Після завершення транзакції інформація про неї може бути перезаписана. Для того щоб у випадку збою забезпечити можливість повного відновлення БД, необхідно вести архів журналу транзакцій, тобто зберігати копії файлів журналу транзакцій разом з резервною копією бази даних. Для підвищення продуктивності сервера БД необхідно розміщати журнал транзакцій на окремому фізичному диску.

Якщо відновлення БД після збою не можна виконати автоматично, воно виконується в два етапи:

1) перенос на робочий диск резервної копії бази даних (чи ушкодженої її частини);
2) перезапуск сервера БД із повторним проведенням усіх транзакцій, зафіксованих після створення резервної копії і до моменту виникнення збою.

Якщо в системі є архів транзакцій, то повторне проведення транзакцій може проходити автоматично чи під керуванням користувача.

Забезпечення конфіденційності даних означає захист даних від навмисного перекручування і/чи доступу користувачів чи сторонніх осіб. Для цього вся інформація БД поділяється на загальнодоступні дані і конфіденційні. Санкціонування доступу до даних виконує адміністратор БД. При реєстрації користувача система створює його "паспорт": ідентифікатор (ім'я) користувача, ім'я процедури підтвердження дійсності і список привілеїв (прав доступу).

Відомі два способи захисту даних у мережних базах:

- заборона доступу до даних тим користувачам мережі, що не мають права доступу до них. Подібне керування запобігає випадковому чи навмисному виявленню, зміні чи знищенню записів і наборів даних;
- забезпечення гарантійного доступу до усіх необхідних даних тим користувачам мережі, що правильно використовують можливості і права доступу.

У СУБД на етапі підключення до БД традиційно виконується парольна ідентифікація користувача - запит на введення імені користувача і пароля для підтвердження того, що це ім'я ввів його власник. Пароль повинен містити не менш 6 символів (букв, цифр, спеціальних знаків) без пробілів і часто мінятися. Для контролю виконання цих вимог використовуються спеціальні програми. Також ідентифікацію й аутентифікацию користувача можна проводити за допомогою ключової дискети, електронного ключа й інших способів.

Керування доступом до даних виконується через СУБД, що і забезпечує захист даних. Але поза СУБД дані стають загальнодоступними: якщо відомий формат БД, то можна здійснити до неї доступ за допомогою інших програм. Тому для підвищення захисту особливо конфіденційних даних використовуються криптографічні методи, спрямовані на запобігання витоку інформації по каналах зв'язку, на захист інформації від НСД і дій по її знищенню чи блокуванню.

Захист конфіденційної інформації може виконуватися методом прозорого шифрування за допомогою технології роботи з віртуальним логічним диском. Дані на фізичному диску завжди зашифровані: при записі на диск здійснюється їхнє шифрування «на лету» за допомогою стійких алгоритмів шифрування, а при читанні з диска - їхня розшифровка.

Надання прав доступу на конкретні об'єкти доступу в СУБД, що підтримують стандарт SQL2, виконується за допомогою інструкцій GRANT і REVOKE. Крім привілеїв на доступ до об'єктів (SELECT, INSERT, DELETE, UPDATE) СУБД ще може підтримувати системні привілеї: це права користувача на створення / зміну / видалення об'єктів різних типів.

У більшості мережних СУБД встановлена відповідальність кожного користувача за керування доступом до створеному їм об'єкту. Користувач може надати право доступу до об'єктів

і операцій іншому користувачу.

Отже, для більш повного захисту необхідна наявність наступних рівнів:

1) Реєстрація й аутентифікація користувачів, ведення системного журналу. У системному журналі реєструються будь-які спроби входу в систему і всі дії користувача в системі.

2) Визначення прав доступу до інформації БД для конкретного користувача (авторизація користувача) при звертанні до СУБД. Усі дії користувача протоколюються в системному журналі. На цьому рівні відбувається конфігурація БД під повноваження конкретного користувача. У цьому випадку користувач працює з віртуальною "особистою" БД.

3) Безпосередній доступ до БД. На цьому рівні для підвищення захищеності системи в цілому доцільно використовувати шифрування окремих об'єктів БД. Ключі для шифрування можна визначати, виходячи з "паспорта"користувача.

УДК 355.422.21: 519.172.3

Побережний А.А., Горєлишев С.А.

ГЕОІНФОРМАЦІЙНА СИСТЕМА ЯК ЕЛЕМЕНТ СИСТЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ ВНУТРІШНІХ ВІЙСЬК

Розглянуто місце геоінформаційної системи в системі інформаційно-аналітичного забезпечення внутрішніх військ. Сформовано вимоги до геоінформаційної системи внутрішніх військ МВС України

Посилення боротьби зі злочинністю, забезпечення громадської безпеки у державі потребують швидкого, якісного й об’єктивного аналізу реального стану оперативної обстановки та прийняття відповідних управлінських рішень. В цих умовах від точності її оцінки, прийняття обґрунтованих рішень і своєчасності їх доведення залежатиме виконання завдань, поставлених внутрішнім військам, ефективність їх діяльності.

Сьогодення вимагає проводити дослідження щодо вибору пріоритетних інформаційних технологій, адаптації їх до нових умов виконання службово-бойових завдань, запровадження цих технологій у перспективні інформаційно-аналітичні системи, призначені для державного і військового управління [1].

Створення інформаційно-аналітичної системи завжди направлене на вирішення завдань управління у всіх його аспектах. Тому, в остаточному підсумку, віддача від впровадження інформаційно-аналітичної системи буде полягати в різкому підвищенні ефективності управління. Ефективність управління досягається, у тому числі, і за рахунок істотного зростання обґрунтованості ухвалених рішень на основі великих вибірок точних даних і великого аналітичного апарату.

Варто підкреслити, що інформаційно-аналітична система - це не готовий продукт. Успіх реалізації інформаційно-аналітичної системи залежить від правильного вибору й максимально тісної інтеграції компонентів системи [2-3].

Однією з головних особливостей інформаційно-аналітичної системи внутрішніх військ МВС України є те що кожне рішення командира будь-якого рівня пов’язане із просторовим баченням місцевості виконання службово-бойових завдань. Таким чином, джерелом даних можуть служити спеціалізовані комп’ютерні системи, побудовані за сучасною технологією, які дозволяють ефективно працювати з просторово-розподіленою інформацією для картографування та аналізу об’єктів реального миру, подій та явищ, що прогнозуються або відбуваються – геоінформаційні системи.

Найважливішим компонентом ГІС, як електронних аналогів паперових карт, є цифрові моделі місцевості, які забезпечують адекватну передачу геометричних, топологічних властивостей об’єктів.

Крім того, програмні засоби ГІС внутрішніх військ (ВВ) повинні задовольняти таким вимогам як

1. глобальна, єдина (можливо розподілена) база даних обстановки;
2. синхронізація даних з декількох джерел, можливість колективної роботи, а також можливість автономної роботи з наступною синхронізацією локальних даних із централізованими сховищами даних;
3. можливість ведення карти відповідно до вимог, прийнятих у ВВ та можливість аналізу місцевості й обстановки;
4. надійність – система повинна забезпечувати збереження даних у критичних ситуаціях;
5. оперативність – у режимі реального часу повинна видати повну й актуальну інформацію про наявну обстановку;
6. робота з даними великого об'єму в реальному масштабі часу;
7. простота й зручність інтерфейсу, його інтуїтивна зрозумілість;
8. розмежування доступу до даних;
9. можливість доробки ГІС під нові потреби внутрішніх військ.

Список використаних джерел

1. Довбня В. В.Особливості інформаційного забезпечення у внутрішніх військах МВС України / В. В. Довбня // Честь і закон. – 2009. – № 4. – С. 4–12.
2. Inmon W. H. Building the Data Warehouse. New York: John Wiley & Sons, Inc.
3. E. F. Codd, S.B.Codd. Providing OLAP. On-line Analytical Processing to User-Analists: An IT Mandate. C. T. Salley, E. F. Codd & Associates, 19

Сорока Л.С., Кузнецов А.А., Исаев С.А.

ИССЛЕДОВАНИЕ ЛИНЕЙНЫХ СВОЙСТВ МИНИ-ВЕРСИЙ БЛОЧНО-СИММЕТРИЧНЫХ ШИФРОВ

Рассматриваются блочно-симметричные шифры, поданные на открытый конкурс по отбору кандидатов на национальный стандарт блочного симметричного шифрования Украины. Исследуется эффективность мини-версий, поданных на конкурс шифров относительно линейного криптоанализа как в зависимости от числа раундов преобразования, так и в зависимости от числа операций и требуемых затрат памяти. Оценивается влияние свойств применяемых нелинейных узлов замен на линейные характеристики блочно-симметричных шифров.

В настоящее время в Украине проходит открытый конкурс по отбору кандидатов на национальный стандарт блочного симметричного шифрования. В качестве шифров-кандидатов на конкурс были поданы следующие криптоалгоритмы: Калина, Мухомор, Лабиринт, RSB-32 и ADE.

С развитием информационных технологий повышается значение надежной защиты информации от нежелательного влияния, поэтому все более жесткими становятся предъявляемые требования к современным шифрам. Основным требованием, предъявленным к алгоритмам-кандидатам, выдвинута высокая стойкость к известным методам криптоанализа, при этом учитывался опыт прошедших конкурсов по отбору криптоалгоритмов AES и NESSIE. В соответствии с Положением про проведение открытого конкурса криптографических алгоритмов одним из основных требований, выдвинутым к современным алгоритмам БСШ является требование длины блока открытого текста и ключа не меньше, чем 128 бит [1]. Такие большие размеры блоков и ключей гарантируют высокую вычислительную сложность для атак типа «грубой силы», потому что требуют выполнения по 2128, 2256 и 2512 операций шифрования или расшифрования соответственно для каждого из возможных 2128, 2256 или 2512 блоков данных.Очевидно, что современные вычислительные возможности не позволяют осуществить соответствующие расчеты в приемлемые сроки. Сейчас отсутствуют также и возможности для хранения всего необхимого объема данных. Но, в то же время, это также усложняет процесс верификации существующих криптоалгоритмов, полного исследования

их свойств и характеристик безопасности. Поэтому, как один из подходов к решению криптологических задач по изучению и анализу алгоритмов БСШ может быть использован метод построения их уменьшенных моделей.

Под уменьшенной моделью мы понимаем такой шифр, который имеет меньшие, чем шифр-оригинал длины блоков данных и ключей [2-4]. В то же время должна быть как можно лучше сохранена математическая структура шифра, т.е. должны быть использованы криптографические преобразования, максимально похожие по свойствам на оригинальные. Это достигается пропорциональным уменьшением соответствующих длин блоков данных и ключей с 128 бит до, например, 16 бит.

По мнению некоторых отечественных и зарубежных криптографов, повышение показателей стойкости шифра к известным методам криптоанализа может быть достигнуто путем введения в шифрующие преобразования блоков замен, которые обладают повышенными показателями стойкости по нелинейности и автокорреляции, при этом сохраняя сложность алгоритма и скорость преобразований.

Первая часть наших исследований состояла в оценке влияния используемых S-боксов на линейные свойства шифров. Исследования состояли в построении линейных таблиц, оценке максимальных значений отклонений и сравнении их с асимптотическим показателем среднего значения максимума линейных аппроксимаций для мини-версий шифров с использованием двух различных типов S-боксов. Один тип S-боксов обладал заведомо лучшими свойствами по нелинейности и автокорреляции, чем другой. Целью данных исследований было, во-первых, сравнение эффективности рассматриваемых шифров, т.е. сравнение по количеству циклов, требуемых для выхода на асимптотику для максимальных значений отклонений, а, во-вторых, исследование влияния используемых S-боксов на эффективность шифров.

Вторая часть наших исследований как раз и заключалась в оценке эффективности шифров к линейным атакам по требуемым вычислительным затратам, т.е. в зависимости получаемых показателей максимумов линейных таблиц от количества операций и памяти.

Работа является логическим продолжением предыдущей нашей работы, посвященной исследованию дифференциальных свойств мини-шифров БСШ, поданных на укранский конкурс [5].

В результате проведенных исследований получены следующие важные в прикладном значении результаты:

- по устойчивости к линейному криптоанализу в зависимости от числа раундов преобразования, исследуемые шифры идут в следующем порядке: 1) Калина, 2) Лабиринт, 3) AES и ADE;
- по устойчивости к линейному криптоанализу в зависимости от числа операций преобразований, исследуемые шифры идут в следующем порядке: 1) AES и ADE, 2) Калина, 3) Лабиринт;
- по совокупности частных показателей наиболее рациональным решением следует, очевидно, считать шифр AES.

Полученные результаты хорошо согласуются с полученными ранее результатами аналогичных исследований, проведенных для дифференциального криптоанализа [5].

Наиболее примечателен последний вывод. Очевидно, что обеспечение требуемой стойкости к линейному криптоанализу при меньшем числе раундов не всегда является рациональным. При выборе криптоалгоритма следует ориентироваться, прежде всего, на вычислительные затраты, которые требуется внести в качестве «платы» за реализацию шифра, обеспечивающего требуемые показатели стойкости.

Полученные результаты показали, что использование узлов замен с улучшенными свойствами позволяет усилить линейные свойства шифров, и в некоторых случаях выйти к асимптотическому показателю максимумов таблиц линейных аппроксимаций раньше, чем с использованием S-боксов с худшими свойствами.

Перспективным направлением дальнейших исследований представляется теоретическое и экспериментальное обоснование адекватности предлагаемой методики исследований, осно-

ванной на использовании мини-версий шифров.

Список использованных источников

1. Положення про проведення відкритого конкурсу криптографічних алгоритмів. http://dstszi.gov.ua

2. A Description of Baby Rijndael, ISU CprE/Math 533; NTU ST765-U, February 19, 2003

3. Raphael Chung-Wei Phan, "Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students", Cryptologia, XXVI(4), October 2002, pp 283-306.

4. Raphael Chung-Wei Phan, “Impossible Differential Cryptanalysis of Mini-AES", Cryptologia, Vol. XXVII, No. 4, October 2003.

5. Сорока Л.С. Исследование дифференциальных свойств блочно-симметричных шифров/ Л.С. Сорока, А.А. Кузнецов, И.В. Московченко, С.А. Исаев// Системи обробки інформації, вип. 6(87), 2010. – с. 286 – 294.

УДК 681.3.06

Кузнецов А.А., Король О.Г., Босько В.В.

МОДЕЛЬ ФОРМИРОВАНИЯ КОДОВ АУТЕНТИФИКАЦИИ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ УНИВЕРСАЛЬНЫХ ХЕШИРУЮЩИХ ФУНКЦИЙ

Исследуются методы и модели формирования кодов аутентификации сообщений с использованием универсальных хеширующих функций (UMAC - Message Authentication Code using Universal Hashing). Посредством масштабирования применяемых преобразований разрабатывается уменьшенная модель UMAC (mini-UMAC), которая позволяет исследовать коллизионные свойства кодов аутентификации сообщений и вырабатывать практические рекомендации по построению эффективных механизмов обеспечения аутентичности и целостности данных.

Одна из первых версий алгоритма формирования кодов подлинности сообщений с использованием универсального хеширования (UMAC – Message Authentication Code using Universal Hashing) была представлена в работе [1]. В дальнейшем, после некоторой доработки [2-4], алгоритм UMAC был представлен в финальном отчете европейского конкурса NESSIE - New European Schemes for Signatures, Integrity, and Encryption (новые европейские схемы для подписей, целостности, и шифрования) [5]. Одна из последних электронных версий алгоритма UMAC доступна в [6]. Наиболее подробно отдельные компоненты UMAC изложены в диссертационной работе [7].

Код подлинности сообщений (обозначим его Tag) по спецификации алгоритма UMAC формируется посредством вычисления следующей функции:

$$Tag = UMAC(K, M, Nonce, Taglen) = Y \oplus Pad,$$

где: K - секретный ключ, длина которого $Keylen$ равна стандартной длине секретного ключа используемого блочного симметричного шифра (спецификацией UMAC рекомендуется использовать алгоритм шифрования AES (FIPS-197), в этом случае длина секретного ключа $Keylen$ принадлежит множеству допустимых значений $\{16, 24, 32\}$ байт); M - информационное сообщение, подлежащее аутентификации, представленное в виде массива-строки, размерностью от одного до 2^{67} бит (2^{64} байт); $Nonce$ - неповторяющееся (для всех вводимых информационных сообщений M) восьмибайтное число; $Taglen$ - целое число из множества допустимых значений $\{4, 8, 12, 16\}$, задающее длину кода подлинности сообщений Tag в байтах; $Hash(K, M, Taglen)$ - функция ключевого универсального хеширования информационного сообщения M с использованием секретного ключа K; $PDF(K, Nonce, Taglen)$ - функция формирования псевдослучайной подложки (Pad) по введенному значению $Nonce$ и секретному ключу K; «$\oplus$» - побитовое сложение (XOR) ре-

зультата ключевого хеширования сообщения $Y = Hash(K, M, Taglen)$ и сформированной подложки $Pad = PDF(K, Nonce, Taglen)$, т.е.

$$Tag = Hash(K, M, Taglen) \oplus PDF(K, Nonce, Taglen).$$

Длина хеш-кода Y, подложки Pad и кода Tag принадлежат множеству допустимых значений $\{32, 64, 96, 128\}$ бит. Эти фиксированные значения $Taglen$ соответствуют случаю формированию кодов подлинности сообщений UMAC – 32, UMAC – 64, UMAC – 96 или UMAC – 128, соответственно.

Вычисление значения функции $Hash(K, M, Taglen)$ выполняется в три этапа (используется три уровня (слоя) ключевого хеширования) $Hash_{L1}$, $Hash_{L2}$ и $Hash_{L3}$, соответственно. Второй уровень хеширования $Hash_{L2}$ выполняется только если длина хешируемого сообщения M превосходит 1024 байт.

Длина хеш-кода Y кратна 32 битам, его значение $Y = Hash(K, M, Taglen)$ для любой длины $Taglen$ формируется посредством объединения (конкатенации) нескольких (от одной до четырех) последовательностей Y_{L3_i}: $Y = Hash(K, M, Taglen) = Y_{L3_1} \| Y_{L3_2} \| ... \| Y_{L3_{It}}$, $It = Taglen / 4$, где Y_{L3_i} - результат многоуровневого хеширования сообщения M на i-ой итерации с использованием соответствующих ключей, $i = 1,2,..., It$.

Специальная функция $KDF(K, Index, Numbyte)$ предназначена для формирования последовательностей псевдослучайных бит данных, которые используются на различных уровнях формирования кодов подлинности сообщений как ключевые данные соответствующих функций хеширования. В качестве исходных данных функции $KDF(K, Index, Numbyte)$ используется секретных ключ K длины $Keylen$ байт и два положительных целых числа $Index$ и $Numbyte$, значение которых не превосходит 2^{64}.

Для формирования псевдослучайных ключевых последовательностей используется блочный симметричный шифр. Обозначим процедуру шифрования блока данных T длины $Blocklen$ байт с использованием секретного ключа K длины $Keylen$ байт в виде некоторой функции $Enchiper(K, T)$. Тогда процедуру формирования псевдослучайной ключевой последовательности $K' = KDF(K, Index, Numbyte)$ можно представить в виде следующего итеративного (для всех $i = 1,2,..., n$) преобразования:

$$T_i = Index \| i,\ K'_i = Enchiper(K, T_i),\ K' = K'_1 \| K'_2 \| ... \| K'_n,$$

где $n = \left\lceil \frac{Numbyte}{Blocklen} \right\rceil$, $\lceil x \rceil$ - целая часть числа x, $a \| b$ - конкатенация строк a и b.

Функция $PDF(K, Nonce, Taglen)$ предназначена для формирования псевдослучайной подложки Pad, используемой на заключительном этапе формирования кода подлинности сообщения. В качестве исходных данных используется секретных ключ K длины $Keylen$ байт и неповторяющееся (для всех вводимых информационных сообщений M) восьмибайтное число $Nonce$, а также целое число $Taglen$, задающее размер (длину в байтах) формируемого кода подлинности Tag.

Процедура $Pad = PDF(K, Nonce, Taglen)$ состоит в формировании подключа $K' = KDF(K, Index, Numbyte)$, $Index = 0$, $Numbyte = Keylen$, с использованием процедуры $KDF(K, Index, Numbyte)$ и шифрования значения $Nonce$ на сформированном подключе K', т.е.: $Pad = Enchiper(KDF(K, 0, Keylen), Nonce)$.

Процедура PDF построена так, что результирующее значение Pad имеет длину $Taglen$ байт вне зависимости от значений $Blocklen$ и $Nonce$.

Таким образом, схема UMAC использует многоуровневую конструкцию

$Hash(K, M, Taglen)$ и процедуру формирования псевдослучайной подложки Pad. Применение универсального хеширования позволяет обеспечить равновероятность формирования хеш-образов для всего множества используемых ключевых данных, формирование псевдослучайной подложки криптографически стойким алгоритмом (например, с использованием блочного симметричного шифра AES) обеспечивает высокую криптостойкость алгоритма UMAC. В тоже время на сегодняшний день не исследованы коллизионные свойства алгоритма UMAC после применения завершающей процедуры наложения на формируемые хеш-коды $Y = Hash(K, M, Taglen)$ псевдослучайных подложек $Pad = PDF(K, Nonce, Taglen)$.

В основе предлагаемой методики исследования коллизионных свойств UMAC лежит использование уменьшенных моделей отдельных слоев используемых преобразований и оценка распределения коллизий (столкновений) формируемых образов (кодов).

Применение уменьшенных моделей используемых слоев преобразований позволяет, сохранив алгебраическую структуру криптоалгоритма, проводить исследования основных показателей его эффективности. Этот поход широко используется на сегодняшний день при исследовании криптографических свойств блочных симметричных шифров. Так, например, в работах [8-10] разработаны уменьшенные модели некоторых криптоалгоритмов, что позволило экспериментально исследовать дифференциальные и линейные характеристики, оценить устойчивость к соответствующим методам криптоанализа. В настоящей работе предлагается дальнейшее развитие данного направления, состоящее в использовании уменьшенных моделей отдельных слоев преобразований для оценки коллизионных свойств формируемых кодов аутентификации сообщений. Разработанная уменьшенная модель UMAC (mini-UMAC) включает соответствующие слои преобразования с сохранением их алгебраической структуры. Практическое использование разработанной модели позволяет экспериментально исследовать коллизионные свойства кодов аутентификации сообщений mini-UMAC и вырабатывать практические рекомендации по построению эффективных механизмов обеспечения аутентичности и целостности данных на основе полной версии UMAC.

Перспективным направлением дальнейших исследований является экспериментальная оценка коллизионных свойств mini-UMAC с использованием разработанной уменьшенной модели и методики статистического тестирования, обоснование на основе опытных данных конкретных предложений по совершенствованию механизмов обеспечения аутентичности и целостности информации.

Список использованных источников

1. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and provably secure message authentication", Advances in Cryptology - CRYPTO '99, LNCS vol. 1666, pp. 216-233, Springer-Verlag, 1999.

2. T. Krovetz, and P. Rogaway. Fast universal hashing with small keys and no preprocessing", work in progress, 2000. To be available from http://www.cs.ucdavis.edu/~rogaway/umac

3. T. Krovetz, J. Black, S. Halevi, A. Hevia, H. Krawczyk, and P. Rogaway. UMAC -Message authentication code using universal hashing. IETF Internet Draft, draft-krovetz-umac-00.txt, www.cs.ucdavis.edu/~rogaway/umac, 2000.

4. T. Krovetz. UMAC -Message authentication code using universal hashing. IETF Internet Draft, draft-krovetz-umac-02.txt, www.cs.ucdavis.edu/~rogaway/umac, 2004.

5. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 - Version 0.15 (beta), Springer-Verlag.

6. T. Krovetz. UMAC - Message authentication code using universal hashing, 2006. To be available from http://www.cs.ucdavis.edu/~rogaway/umac

7. T. Krovetz. Software-Optimized Universal Hashing and Message Authentication. Dissertation submitted in partial satisfaction of the requirements for the degree of doctor of philosophy. University Of California Davis. September 2000. – 269p.

8. A Description of Baby Rijndael // ISU CprE/Math 533; NTU ST765-U. – 2003.

9. Долгов В.И. Исследование дифференциальных свойств мини-шифров Baby-ADE и

Baby-AES / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. – Х.: ХНУРЭ, 2009. – Т. 8, № 3. – С. 252-257.

10. Долгов В.И. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / В.И. Долгов, А.А. Кузнецов, И.В. Лисицкая, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. – Х.: ХНУРЭ. – 2009. – Т.8, № 3. – С. 268 – 277.

Павленко М.А.

АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ ПРИ МОДЕЛИРОВАНИЕ ПРОЦЕССА МАРШРУТИЗАЦИИ

Развитие телекоммуникационных систем в настоящее время связано с широким внедрением новых технологических решений в их построение и использование. В соответствии с общемировыми тенденциями развития систем телекоммуникаций основной задачей отрасли связи является создание единой интегральной мультисервисной широкополосной сети связи, отвечающей всевозрастающим запросам пользователей к качеству обслуживания. Ее успешное решение тесно сопряжено с необходимостью обобщения уже накопленного опыта в сфере телекоммуникаций и всецело зависит от степени технологического внедрения передовых принципов и методов управления, передачи и обработки информации.

Существующие алгоритмы решают данные задачи с заданной периодичностью. Однако при изменениях топологии сети или характеристик каналов передачи данных расчет новых маршрутов не всегда реализуется в заданные интервалы обновления маршрутных таблиц. Это, в свою очередь, приводит к значительным задержкам в передачи информации, снижении качества передачи данных и потере данных. Таким образом, необходимо проводить дополнительные исследования, связанные с поиском альтернативных методов решения задач маршрутизации, которые позволят решать данные задачи в реальном масштабе времени без снижения качества их решения. Одним из подходов к решению задачи маршрутизации является использование аппарата искусственных нейронных сетей.

В работе предлагается исследовать возможность использования искусственных нейронных сетей для решения задачи маршрутизации. В качестве объектов анализа рассмотрим следующие нейронные сети: многослойный персептрон, сеть RBF и сеть Хопфилда.

Павленко М.А., Руденко В.М., Бердник П.Г., Першин О.В.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ ПРИЙНЯТТЯ РІШЕНЬ ОПЕРАТОРАМИ ПЕРСПЕКТИВНИХ АСУ

Аналіз інформаційних моделей на пунктах управління може займати дуже багато часу та істотно впливати на час прийняття рішень. Тому склад системи інформаційного забезпечення, склад інформаційних моделей та їх наповнення інформаційними елементами будуть впливати на час їх аналізу та переробку у концептуальні моделі.

Скоротити час на аналіз інформаційних моделей можливо наступним чином, по-перше це проведення аналізу інформаційної моделі групою осіб, але це може забрати більше часу ніж аналіз однією особою. Інший шлях, це розробка системи оперативного супроводження процесу аналізу інформаційних моделей голосовими підказками, які дозволять розробити систему фокусування уваги оператора на «конфліктних» ділянках інформаційних моделей. Наступний шлях це розробка інформаційних моделей у відповідності до інтелектуального характеру діяльності оператора та вирішуваних ним задач.

Це, в свою чергу, зумовлює необхідність вирішення задач аналізу та синтезу повідомлень обмеженої природної мови, а також системи ситуаційного управління природо мовними повідомленнями, а також нових інформаційних елементів для системі інформаційних моделей в АСУ.

УДК 004.72(045)
Хоптинський Р. П.

АНАЛІЗ ХАРАКТЕРИСТИК ПРОДУКТИВНОСТІ МЕРЕЖІ З ПАКЕТНОЮ ПЕРЕДАЧЕЮ ДАНИХ ПРИ ЗАБЕЗПЕЧЕНІ ЯКІСНОГО ОБСЛУГОВУВАННЯ

У тезах розглядаються основні характеристиками продуктивності мережевого з'єднання з пакетною передачею даних, які впливають на якість обслуговування в телекомунікаційній мережі.

Одним з основних аспектів, який повинен братися до уваги при аналізі телекомунікаційної мережі є забезпечення якості обслуговування. В свою чергу якість обслуговування (QualityofService, QoS) – це узагальнений (інтегральний) корисний ефект від обслуговування, який визначається степенем задоволення користувача, як від послуг, які він отримує так і від самої системи обслуговування [1]. В сьогоденні широкого розповсюдження отримали пакетні мережі передачі даних. Специфіка пакетних мереж полягає в тому, що на відміну від мереж з комутацією каналів, в одному і тому ж інформаційному потоці може передаватися різнорідний трафік, який характеризується низкою критичних і некритичних параметрів.

На даний час існує ряд варіантів реалізації якості обслуговування які передбачають з сторони мережі з'єднання з певними обмеженнями по продуктивності. Основними характеристиками продуктивності мережевого з'єднанняєсмуга пропускання, затримка, тремтіння та рівень втрат пакетів [2].

Смуга пропускання (bandwidth) використовується для опису номінальної пропускної здатності середовища передачі інформації, протоколу або з'єднання. Як правило кожне з'єднання, що потребує гарантованої якості обслуговування, вимагає від мережі резервування мінімальної смуги пропускання. Прикладом може програми, які орієнтовані на передачу відцифрованої мови створюють потік інформації інтенсивністю 64 Кбіт/с. Ефективне використання таких додатків стає практично неможливим внаслідок зниження смуги пропускання нижче 64 Кбіт/с на якій-небудь з ділянок з'єднання.

Затримка між кінцевими пристроями характеризує загальний час проходження даних або потоку даних до віддаленої точки. Затримка при передачі пакета (packetdelay) або латентність (latency) на кожному переході складається з затримки серіалізації, затримки розповсюдження і затримки комутації.

Затримка серіалізації (serializationdelay) це час, який потрібно пристрою на передачу пакета при заданій ширині смуги пропускання. Затримка серіалізації залежить як від ширини смуги пропускання каналу передачі інформації, так і від розміру переданого пакета.

Затримка розповсюдження (propagationdelay) – це час, який потрібно переданому біту інформації для досягнення пристрою на іншому кінці каналу. Ця величина є досить суттєвою, оскільки в найкращому випадку швидкість передачі інформації порівнянна зі швидкістю світла. Затримка поширення залежать від відстані і від середовища передачі інформації, яке використовується, а не від смуги пропускання.

Затримка комутації (switchingdelay) - час, який потрібно пристрою, який отримав пакет, для початку його передачі наступного пристрою. Як правило, це значення менше 10 нс.

Зазвичай кожен з пакетів, що належить одному і тому ж потоку трафіку, передається з різним значенням затримки. Затримка при передачі пакетів змінюється в залежності від стану проміжних мереж. Якщо мережа не відчуває перевантаження (стан мережевих вузлів, коли мережа не може гарантувати задану якість обслуговування, як для встановлених з'єднань так і для тихз'єднань, що встановлюються [3]), то пакети не ставляться в чергу в маршрутизаторах, а загальний час затримки при передачі пакета складається з суми затримки серіалізації та затримки поширення на кожному проміжному переході. У цьому випадку можна говорити про мінімально можливу затримку при передачі пакетів через задану мережу. Слід зазначити, що затримка серіалізації стає незначною порівняно з затримкою поширення при передачі пакета по каналу з великою пропускною здатністю.

Якщо ж мережа перевантажена, затримки при організації черг в маршрутизаторах починають впливати на загальну затримку при передачі пакетів, та призводять до виникнення різниці у затримці при передачі різних пакетів одного і того ж потоку. Коливання затримки при передачі пакетів отримало назву джиттер-пакетів (packetjitter). Даний параметр має велику важливість, оскільки саме він визначає максимальну затримку при прийомі пакетів у кінцевому пункті призначення. Приймаюча сторона, в залежності від типу використовуваного додатка, може спробувати компенсувати тремтіння пакетів за рахунок організації прийомного буфера для зберігання прийнятих пакетів на час, менше або рівне верхній межі тремтіння. До цієї категорії відносяться програми, орієнтовані на передачу і прийом безперервних потоків даних, наприклад IP-телефонія або додатки, що забезпечують проведення відеоконференцій.

При обслуговувані трафіку коли пропускної здатності недостатньо для обробки вхідних пакетів виникають черги. При цьому затримка при очікувані є основною складовою сумарної затримки пакетів. Що стосується втрати пакетів, то якщо відкинути перекручування при передачі переповнення черг через перезавантаження є єдиним істотним джерелом втрат. Втрати пакетів які передаються в пакетній мережі характеризуються рівнем втрати пакетів (packetloss), який визначає кількість пакетів, які відкидаються мережею під час передачі [4]. Найчастіше відкидання відбувається в місцях перевантаження комутаційних вузлів, де число вхідних пакетів набагато перевищує верхню межу розміру вихідний черги. Крім того, відкидання пакетів може бути викликано недостатнім розміром вхідного буфера комутаційного вузла. Як правило, рівень втрати виражається як частка відкинутих пакетів за певний інтервал часу

Виходячи з вище сказаного слід розуміти, що сукупність контрольованих параметрів продуктивності мережевого з'єднання інформаційного потоку гарантує відповідність між реальними параметрами продуктивності мережевого з'єднання та заданими.

На даний час існує ряд варіантів, що ведуть до зменшення (а при ідеальному використані і нейтралізації) негативного впливу перерахованих вище характеристикпродуктивності мережевого з'єднання на якість обслуговування, а саме [2]:

- класифікація і маркування пакетів;
- управління інтенсивністю трафіку;
- розподіл ресурсів;
- попередження перевантажень та політика відкидання пакетів;
- маршрутизація та інші.

В свою чергу механізми якості обслуговування (QoS) полягають у забезпеченні гарантованого і диференційованого обслуговування мережевого трафіку шляхом передачі контролю за використанням ресурсів і завантаженістю мережі, проте кожен з механізмів має ряд недоліків. Тому постає природнє бажання, щодо створення системи управління потокамина основі існуючих механізмівQoS та з урахуванням всіх характеристик, які впливають на процес передачі даних.

Список використаних джерел

1. Конахин Г.Ф., Чуприн В.М. Сети передачипакетныхданных. – К.: "МК-Пресс", 2006 – 272 с.

2. Шринивас-Вегешна.Качествообслуживания в сетях IP. - М.: Вильямс, 2003. - 368 с.

3. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет. - СПб.:Наука и Техника, 2004. – 336 с.

4. Ирвин Дж., Харль Д. Передача данных в сетях: инжинерный подход: Пер. с англ. –СПб.: БХВ-Петербург, 2003. – 448с.

УДК 004.056.57:656.2

Приходько С.І., Цимбал Г.С.

МЕТОД ОТРИМАННЯ НЕЛІНІЙНИХ ФУНКЦІЙ ДЛЯ АЛГОРИТМІВ ПОТОКОВОГО ШИФРУВАННЯ ДАНИХ

У роботі розглянуті вимоги до функцій, що формують нелінійні блоки замін алгоритмів потокового шифрування, надан метод отримання нелінійних функцій, що формують нелінійні блоки замін для алгоритмів потокового шифрування.

Дослідження в області нелінійних блоків замін [1-2] показують, що необхідна розробка нових методів побудови нелінійних блоків замін (S-блоків).

Аналіз вимог, що висуваються до нелінійних функцій [1], показує, що еластичні нелінійні функції є найбільш доцільними для застосування.

Отримання еластичних нелінійних функцій з заданими параметрами є актуальною задачею. Аналіз методів побудови еластичних функцій [3-6] дозволяє зробити висновок, що найкращими показниками криптостійкості буде володіти така функція, що отримується із згорткового коду. Також, слід зазначити, що, так як, згорткові коди є нескінченними, а отже використання матричного способу отримання еластичних функцій не є можливим, для побудови еластичних функцій треба використовувати алгебраїчні згорткові коди.

Метод, що пропонується, базується на теорії взаємозв'язку між лінійними кодами та еластичними функціями. Використовуючи кодові слова згорткового коду, ми отримуємо компонентні функції еластичної функції, так як кодові слова згорткового коду володіють усіма властивостями самого коду, тож функція, що отримана таким чином буде наслідувати характеристики коду. Така функція буде показувати кращі характеристики криптостійкості ніж функції отримані з звичайних лінійних кодів.

Таким чином, метод, що пропонується дає можливість за той самий час, що потребується на побудову еластичних функцій з звичайних лінійних кодів, отримати еластичні функції з покращеними показниками криптостійкості.

Список використаних джерел

1. Кузнецов А.А., Московченко И.В. Разработка предложений по совершенствованию симметричных средств защиты информации перспективной системы критического применения // Радіоелектронні і комп'ютерні системи. – 2008. – №2 (29). – С. 94-100.
2. Потий А.В., Избенко Ю.А. Исследование методов криптоанализа поточных шифров // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – ДСТСЗІ СБУ, НТУ «КПІ». – 2003. - №6. – С. 34-49.
3. Pascale Charpin, Enes Pasalic. Highly Nonlinear Resilient Functions Through Disjoint Codes in Projective Spaces // Design, Codes and Cryptography. – 2005. - № 37. – pp. 319-346.
4. D.R. Stinson, J.L. Massey. An finite calss of counterexamples to a conjecture concerning non-linear resilient functions. // http://www.cacr.math.uwaterloo.ca/~dstinson/papers/respk.ps.
5. Xian-Mo Zhang , Yuliang Zheng. Cryptographically Resilient Functions // http://pscit-www.fcit.monash.edu.au/~yuliang/pubs/ie3it-resi.ps.
6. Paul Camion, Anne Canteaut. Correlation-Immune and Resilient Functions Over a Finite Alphabet and Their Applications in Cryptography /http://portal.acm.org/citation.cfm?id=309154.

Усачов О.М., Дробот О.А., Дрозд О.А.

МЕТОД РІШЕННЯ БАГАТОКРИТЕРІАЛЬНИХ ЗАДАЧ В УМОВАХ НЕЧІТКОЇ ІНФОРМАЦІЇ

При ухваленні рішення в умовах нечіткої інформації може бути висунуто кілька альтернатив. Для виключення послідовного їхнього перебору використається система переваг і оцінка наслідків ухваленого рішення. Ці дві операції при ухваленні рішення людиною виконуються практично разом. Інтелектуальна система ухвалення рішення буде виконувати їх послідовно.

Для оцінки переваг і наслідків ухвалення рішення в умовах нечіткої інформації необхідні відповідні методи. Методи оцінки переваг визначаються як відмінністю альтернатив між собою, так мірою чіткості інформації, наявністю резерву сил і засобів зарезервованих при ухваленні рішення, можливістю поповнення цих сил і засобів і т.д.

Вдосконалений метод вибору переваги дозволяє вирішувати багатокритеріальні задачі, які часто виникають при управлінні телекомунікаційною мережею спеціального призначення. Ухвалення рішення в умовах нечіткої інформації пропонується здійснювати з кількісною оцінкою висунутих переваг. Особливістю даного методу є можливість вибору шляхів визначення значення вагових коефіцієнтів при визначенні функції корисності, що дає можливість звести багатокритеріальну задачу до однокритериальної. Такий підхід надає можливість вирішити завдання залежності якості рішення задачі ухвалення рішення від кваліфікації особи приймаючого рішення, у випадку недостатнього особистого його досвіду та обмеженої інтуїції.

УДК 681.5.015

Авраменко В.П., **Парамонов А.К.**, **Чибирев А.Д.**

ФОРМИРОВАНИЕ РАСТРОВЫХ ИЗОБРАЖЕНИЙ КОМПЬЮТЕРНОЙ ГРАФИКИ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛОВ

Исследованы методы и конструктивные средства создания растровых изображений компьютерной графики, каждая точка которого в свою очередь формируется с использованием фрактальных функций.

Важным направлением компьютеризации современного общества является компьютерная графика, которая охватывает все виды и формы представления изображений, доступных для восприятия человеком на экране монитора или в виде копии на внешнем носителе.

Визуализация данных находит применение в различных сферах человеческой деятельности – в медицине (компьютерная томография), в правоведении (компьютерное распознавание образов), в издательской деятельности (компьютерный способ отображения информации).

В зависимости от способа формирования изображений компьютерную графику принято подразделять на растровую, векторную и фрактальную. Для растровыж изображений, состоящих из точек, особую важность имеет понятие разрешение, которое выражается количеством точек, приходящимся на единицу длины.

Растровые изображения получают, как правило, в результате сканирования оригиналов (схем, рисунков) или фотографирования объектов цифровыми фотоаппаратами. Растровое изображение состоит из матрицы малых графических элементов – пикселей. Каждому пикселю как наименьшему элементу изображения можно задать размер, цвет, глубину цвета, интенсивность тона, плложение и другие характеристики.

Чем большее количество точек приходится на один дюйм, тем выше качество растровой графики, которое выражается разрешающей способностью или разрешением. Размер точки растрового изображения (растра) зависит от примененного метода и параметров рвстрирования. Растрирование является основой изготовления печатных форм для любых способов печати: офсетной, глубокой, флексографской, цифровой и многих других.

При растрировании на оригинал как бы накладывается сетка линий, ячейки которой образуют элемент растра. Густота (частота) сетки растра измеряется числом линий на дюйм и называется линеатурой. Размер точки растра зависит от интенсивности тона в данной ячейке. Для управления печатью применяется растровый процессор, осуществляющий растрирование.

Традиционные растры имеют регулярную периодическую структуру. Для передачи градаций оттенков цвета используется амплитудная модуляция размера точки растра. С целью улуч-шения отображения применяются растровые точки различной формы: квадратные, круглые, эллиптические, цепеобразные.

Недостатками периодических растров являются:

– наличие нелинейной зависимости величины растискивания растровой точки от ее номинального относительного размера (% растра);

– визуальная неравномерность градиентных заливок;

– большая вероятность возникновения муара;

– технологические ограничения линиатуры растра;

– заметная розеточная структура изображения;

– пропадание или деформация тонких линий;

– ограничение цветового охвата.

Большинство описанных ограничений снимаются использованием стохастических растров,

особенно для изображений с низкой линиатурой, например, при печати газет или упаковке на немелованном картоне. Однако некоторые ограничения всё жеостаются и у них.

Полутоновой точке оригинала при использовании стохастических растров ставится в соот-ветствие «облако» одинаковых по размеру точек, количество которых определяется уровнем яркости точки на оригинале, а взаимное расположение точек квазислучайно.

Чем темнее точка на оригинале, тем больше число точек в «облаке». Такое формирование изображения позволяет снять влияние растискивания точки, исключить возникновение муара, увеличить цветовой охват. К основным недостаткам стохастического растрирования относятся:

– трудность копирования маленьких точек на печатную форму;

–повышенные требования к печатным краскам и формным материалам;

– повышенные требования к стабильности печатной машины;

– повышенные требования к файлам пиксельной графики;

– размывание тонких штрихов (засечек у букв);

– незначительное визуальное снижение резкости иллюстраций.

Дальнейшее развитие алгоритмов растрирования – это гибридные растры. Они сочетают общие признаки классических и стохастических растров. Каждая вариация гибридной технологии по-своему уникальна, и разработчики не разглашают всех технологических секретов, однако у всех есть общее:

– более высокая линиатура растра;

– частичная частотная модуляция;

– адаптивный подход к разным элементам изображения;

– увеличение цветового охвата.

Поскольку ни одна из существующих на сегодняшний день технологий растрирования не обеспечивает «беспроблемного» полиграфического воспроизведения, то авторами доклада предложено в качестве элементов растра использовать фрактальные функции (фракталы).

Отсутствие регулярной решётки позволяет избежать недостатков периодических растров. Внесение случайностей в процесс построения фрактальных структур приближает их к свойствам стохастического растра, а также привносит элемент оригинальности в сформированное растровое изображение.

Так как фракталы себе подобны, то из любой части фрактального растра можно определить тип и параметры применяемой для растрирования фрактальной структуры. Отсюда следует, что применение фракталов позволяет внести индивидуальность каждому отпечатку, то есть фрактальное растрирование может использоваться как средство защиты печатной продукции.

Кроме самого типа используемого фрактального изображения, дополнительной степенью защиты может быть применение случайных величин в процессе формирования растра. Фиксируя последовательность случайных величин и повторяя её для каждого экземпляра фрактала в растре, получается своеобразный ключ для идентифицировать печатной продукции.

Фрактальная графика, как и векторная, использует математические выражения и позволя-

ет формировать как простейшие графические регулятные структуры, так и сложные иллюстрации.

Последовательность величин, на основе которых модифицируется фрактальный растр, может носить не обязательно случайный характер, а заранее заданный и быть информационно нагруженной. Закодированная таким способом информация встраивается в растр и после печати получается исходное изображение со скрытыми данными.

Принцип предлагаемого фрактального метода растрирования основан на зависимости заполнения поверхности от уровня детализации отображаемого фрактала. С увеличением уровня детализации, увеличивается количество точек, необходимое для его отображения. Если поставить в соответствие каждой точки изображения фрактальную конструкцию с необходимым уровнем заполнения поверхности, то получится его растрированный аналог.

Обобщённый алгоритм формирования фрактального растра содержит следующие блоки: выбор типа фракталов, введение данных в изображение, генерирование модификаторов фракталов, расчет параметров вывода с учетом разрешения и линиатуры, формирование фрактальных структур, растрирование исходного изображения.

УДК 681.5.015

Авраменко В.П., **Чибирев А.Д.**, **Парамонов А.К.**

СТРАТЕГИИ ЗАЩИТЫ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНЫХ ФУНКЦИЙ

Рассмотрены современное состояние и стратегии защиты графической информации. Предложены методы и средства защиты информации на основе фрактальных функций.

При создании систем защиты графической информации возникает необходимость расширять арсенал используемых классических методов защиты за счет применения нечетких множеств, экспертного оценивания, «мозгового штурма», интеллектуальной генерации решений, алгебраических и фрактальных функций.

Для обоснования основных положений защиты графической информации необходимо ввести ключевые понятия стратегии защиты на основе унифицированной концепции защиты информации. Унифицированная концепция должна отражать цепь методологий оценки уязвимости информации, выработки требований по ее защите, определения концептуальных решений по защите, оценке факторов, влияющих на уровень защиты.

На пути эффективной информатизации общества стоит ряд серьезных проблем, важнейшей из которых является надежная защита информации (предупреждение искажения или уничтожения её, несанкционированная модификация, злоумышленное получение и использование её). Особую актуальность эта проблема приобретает в связи с доступом массы пользователей к ресурсам информационно-вычислительных сетей.

Проблемы защиты различного рода информации в системах обработки и хранения возникли практически одновременно с появлением самих систем, однако особенно они обострились, когда средства вычислительной техники стали применяться для обработки закрытой, служебной и конфиденциальной информации.

Понятие «стратегия» в широком смысле представляет собой совокупность сориентированных на перспективу руководящих методических материалов по организации определенного вида деятельности, направленная на обеспечение наиболее важных целей этой деятельности при рациональном расходовании ресурсов.

Стратегия защиты информации представляет собой совокупность организационных и технологических мероприятий по защите информации, которая должна быть такой, чтобы в течение всего времени функционирования системы уровень защиты соответствовал требуемому, а выделяемые ресурсы расходовались наиболее рациональным образом.

Существующая практика защиты информации показывает, что в различных ситуациях требования к защите и условия защиты могут существенно отличаться, поэтому одной стра-

тегией не удастся охватить и содержательно выразить общую направленность защиты для всех систем защиты и всех возможных условий их функционирования.

Для системного решения вопросов защиты на множестве потенциально возможных условий необходимо сформировать такой набор различных стратегий защиты, чтобы каждая из них была сориентирована на некоторую подобласть проблемы защиты. Основой множества стратегий защиты должны служить результаты системного анализа требуемых условий, в которых может осуществляться защита конкретного вида информации.

Организация защиты информации в самом общем виде может быть определена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами.

Выбор конкретной стратегии защиты информации обусловливается важностью и объемами защищаемой информации, условиями ее хранения, обработки и использования. Эти условия определяются предъявляемым качеством защиты, уровнем организации обработки информации, условиями расположения защищаемых компонентов и рядом других параметров [А.А. Малюк].

Размер выделяемых ресурсов на защиту информации может быть ограничен либо конкретным значением, либо определяться условием обязательного достижения требуе-мого уровня защиты. В первом случае защита организуется так, чтобы при выделенных ресурсах обеспечить максимально возможный уровень защиты, а во втором – так, чтобы требуемый уровень защиты обеспечивался при минимальном расходовании ресурсов.

Задачи защиты информации, представленные системами алгебраических равенств и неравенств, можно рассматривать как прямую и обратную задачи моделирования (исследования операций), для решения которых разработаны методы регуляризации некорректно поставленных задач [А.Н. Тихонов, Е.С. Вентцель].

Задачи защиты графической информации также делятся на прямые и обратные, методы решения которых существенно зависят от способа формирования графических изображений. На сегодняшний день для защиты ценных бумаг на стадии создания оригинал-макета применяется растровая и векторная графика, а на ближайшую перспективу намечается применение методов и функций фрактальной графики.

Фракткалы в узком смысле представляют собой множество сложных геометрических объектов, генерируемых с помощью математических выражений [Р. Гонсалес]. Создавать фракталы можно с помощью аналитико-вычислительного итерационно-циклического процесса, причем отдельные части фрактала подобны по форме на весь фрактал.

Прямая задача фрактальной защиты графической информации состоит в том, чтобы в условиях.нечеткого задания исходных данных сгенерировать с заданной точностью графический образ как геометрическую совокупность точек.

Обратная задача фрактальной защиты графической информации предусматривает распознавание графических образов с идентифицикацией аналитических зависимостей в виде фрактальных функций.

Фракталы в широком смысле представляют собой множество точек евклидова пространства, у которых имеется дробная метрическая размерность, строго меньшая топологической размерности [Р.М. Кроневер]. Сложность фрактального изображения при его увеличении не изменяется. Именно это свойство и используется для защиты информации.

Все фрактальные соотношения принято подразделять на детерминированные (алгебраические, геометрические) фракталы и недетерминированные (стохастические) фракталы. Фракталам присущие также следующие свойства: самоподобие, то есть подобие частей фрактала на форму всего фрактала; непродолжительность структуры на всех шкалах; дробнометрическая размерность, которая не превосходит топологическую.

Форма полученного фрактального изображения существенно зависит от заданных параметров аналитического выражения (формулы). Построение фрактала осуществляется с использованием рекурсивной процедуры или системы итеративныхь функций.

Примером фрактала может служить множество Мандельброта, для построения каждой то-

чки которого требуется выполнить цикл итераций согласно формуле

$$z_{k+1} = z_k^2 + z_0, \; k = 0, 1, ..., n.$$

Величины z_k и z_0 – комплексные числа; $z_k = x_k + iy_k$, причем стартовые значения x_0, y_0 – координаты точки изображения. Для каждой точки изображения итерации выполняются ограниченное количество раз (n) или до тех пор, пока модуль комплексного числа z_k не превышает фиксированного значення 2. Цикл итераций для фрактала Мандельброта обычно выбирается в диапазоне x = (–2,2; +1,0), y = (–1,2; +1,2). Для кодирования изображений решается обратная задача [Е.П. Путятин, В.О. Гороховатский].

УДК 355.233.1.005

Калачова В.В., **Алексєєв С.В.**, **Трублін О.А.**

ОСОБЛИВОСТІ МЕТОДИКИ КОМПЛЕКСНОЇ ОЦІНКИ ЕФЕКТИВНОСТІ КУРСУ ДЛЯ СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В роботі доводиться перспективність застосування канонічного підходу в методиці комплексної оцінки ефективності дистанційного навчального курсу системи дистанційного навчання військового призначення щодо забезпечення індивідуального підходу до кожного, хто проходе навчання в її межах і формування в них стійких та якісних знань.

Значні зміни у структурі, технічному і кадровому забезпеченні Збройних Сил (ЗС) України вимагають від військової системи освіти втілення останніх світових досягнень наукової думки та технічного прогресу в навчальний процес ВВНЗ. Ці дії мають сприяти одержанню більш стійких та якісних знань курсантами.

Світова практика показує, що в якості сучасного засобу для надання та підтримки відповідного рівня як цивільної так і військової освіти варто використовувати системи дистанційного навчання (СДН), які реалізують дистанційне навчання на різних рівнях освіти за допомогою дистанційних навчальних курсів.

Дистанційний навчальний курс, є прикладом складної системи. Його складові такі як програма курсу, контент, глосарій, комунікаційні засоби організації процесу навчання можуть розглядатися як незалежні системи зі своїми особливими рисами та кількісними та якісними характеристиками. Але ж тільки їх об’єднання та взаємодія дає можливість казати про реалізацію та досягнення мети дистанційного навчання – формування стійкий та якісних знань як у окремих навчаючихся так і у цілих дистанційних навчальних груп. Оцінка складних систем, в свою чергу, здійснюється за комплексним критерієм.

Під комплексним критерієм розуміється оцінювана характеристика (властивість) системи, яка складається з декількох інших, теж можливо складних характеристик. Таким чином, комплексний критерій може бути представлений як ієрархічна структура (дерево), термінальними вершинами якого є прості показники, які можуть бути оцінені кількісно. Причому ця оцінка може бути одержана об'єктивно, як результат вимірювання деякої характеристики об'єкту або системи, так і від експерта. Згідно з факт-потенціальним методом всі оцінки простих показників нормуються до діапазону [0,1]. Всі нетермінальні вершини розмічаються функціями з класу середніх для отримання агрегованих оцінок і також належать діапазону [0,1].

Дистанційний навчальний курс СДН військового призначення, є складною системою з ієрархічною структурою. Обов'язковими елементами його є: навчальний матеріал (програма, контент, глосарій, посилання на додатковий матеріал та т. ін.), засоби організації зворотного зв’язку для процесу навчання або самонавчання (консультації, семінари, обговорення в групах, тестування, іспити) та оперативна допомога курсанту. Будь-яка компонента такої системи може володіти як характеристикою верхнього рівня, так і більш простими властивостями. Щоб побудувати модель оцінки конкретної системи за комплексним критерієм необхідно приписати компонентам системи властивості з дерева характеристик. При цьому властивості розповсюдяться на інші компоненти за правилами спадкоємства.

При формуванні та описі моделі оцінки системи за комплексним критерієм можливо за-

стосування декількох підходів: канонічний, фрактальний та Case-підхід. Кожна з моделей має свої особливі переваги, але з погляду авторів, канонічна модель є найбільш вдалою з точки зору її подальшої формалізації та автоматизації, тому на цій моделі і була сконцентрована основна увага в роботі щодо комплексної оцінки ефективності курсу для систем дистанційного навчання військового призначення.

Канонічна модель оцінки дистанційного навчального курсу як складної системи за комплексним критерієм будується по поточному стану системи, при цьому повністю визначається структура системи і структура комплексного критерію для оцінки системи і її компонент. Модель відповідно до методики наочно представлена у вигляді двох дерев:

- дерево структури С = $\{c^{i}_{j,k}\}$, де *i* – номер вершини-батька з попереднього рівня, *j* - номер поточного рівня в дереві і *k* - номер поточної вершини в дереві;
- дерево критеріїв і оцінок К=$\{к^{n}_{m,l}\}$ з відповідними індексами.

Множина оцінок О в загальному випадку є відношенням між С і К, тобто О=С*К.

Формування цього відношення зводиться до встановлення зв'язків між вершинами двох дерев С і К

Всі нетермінальні вершини цього дерева слід розмітити агрегуючими функціями, які можуть бути будь-якими з класу середніх, але ми братимемо тільки середньозважені або (вже зовсім у важких випадках) середньоарифметичні.

Критерій може розглядатися, як такий, що має дві сторони: оцінки експерта за змістом та оформленням навчального матеріалу і оцінки курсантів, що закінчили цей курс.

Припускається, що експерт оцінює зміст і оформлення курсу за наступними показниками: повнота навчального матеріалу; структурованість; ясність і чіткість викладу; ступінь наочності; динамічність викладу; стимулювання самостійної роботи курсанта.

Курсанти оцінюють якість курсу і рівень викладання за показниками, розбитими на 5 груп:

1) *рівень викладання*: організованість; стимулювання інтересу до предмету; відповідність рівня спілкування викладача рівню розуміння курсанта; об'єктивність оцінок; корисність зауважень і відгуків; підтримка і допомога; доступність викладача; підтримка активності курсантів; баланс складових курсу (очних занять, Web конференцій, E-mail).

2) *зміст курсу:* інтелектуальна привабливість навчального матеріалу; відповідність формату курсу його змісту; обґрунтованість завантаження курсанта; ясність завдань і їх відповідність завданням курсу; обґрунтованість і ясність вимог.

3) *опис курсу:* ясність цілей і завдань курсу; зрозумілість домашніх завдань; обґрунтованість розкладу; відповідність форм навчального матеріалу навчальному курсу.

4) *формування навичок:* уміння писати, висловлювати матеріал; комп'ютерна письменність; науковий і інформаційний пошук; широта поглядів; критичне мислення.

5) *загальні оцінки:* задоволеність курсом; рекомендація курсу іншим курсантам; рекомендація викладача іншим курсантам.

Курсанти дають свої оцінки за відповідною шкалою. При цьому може бути оцінка 0, що значить "думка відсутня", вона не враховується.

Всі нетермінальні вершини дерева розмічаються агрегуючими функціями, які можуть бути будь-якими з класу середніх, але інтерес представляють тільки середньозважені або (вже зовсім у важких випадках) середньоарифметичні.

Для установки зв'язків між деревами потрібно навісити піддерева критерію на коріння дерева структури курсу

При цьому спадковість може бути різна, по дереву структури властивості по спадку передаються вгору, а якщо компонент курсу володіє якоюсь складною властивістю, то він володіє і всіма складовими цієї властивості, тобто по дереву критерію спадковість передається вниз. Так по критерію експерта оцінюється тільки навчальний матеріал, а курсанти оцінюють курс повністю.

Одержане дерево дозволяє нам обчислювати оцінки як для всього курсу, так і для його складових. При цьому вхідними даними для методики є оцінки курсантів або експерта по те-

рмінальних вершинах. Оцінки можуть бути будь-які, але по методиці вони нормуються, наприклад, можливо зведення їх до значень з інтервалу [0,1]. Потім обчислюються оцінки, послідовно рухаючись вгору по дереву. В деяких випадках, із-за надмірності, оцінки можуть бути обчислені декількома способами, але вони повинні співпадати, інакше модель буде суперечлива.

В роботі одержано безліч оцінок, але зіставні (тобто ті, які є сенс порівнювати), це завжди вершини тільки одного дерева. Наприклад, можна порівнювати активність курсантів в різних конференціях (тобто одна властивість для складових однієї компоненти), або різні властивості одного об'єкту.

Одержані класи зіставних оцінок дозволяють проводити статичний аналіз дистанційного навчального курсу, виявляти його слабкі місця, тобто складові курсу; і слабкі сторони - тобто окремі властивості курсу або його складових.

Методика дозволяє проводити не тільки статичний аналіз системи, наприклад, дистанційного навчального курсу, але і відстежувати динаміку такої системи. Якщо мається ряд оцінок цієї системи (дистанційного навчального курсу) за деякий період часу, є можливість дивитися динаміку всієї системи, або окремих її складових, або окремих її сторін.

З ціллю всебічного врахування індивідуальних особливостей та навчальних можливостей кожного курсанта, що проходе навчання за дистанційною формою у ВВНЗ України, та формування в нього стійких та якісних знань проведено дослідження можливості застосування методики комплексної оцінки ефективності дистанційного навчального курсу з канонічним підходом щодо опису моделі оцінки системи за комплексним критерієм. Дослідження показали, що застосування канонічного варіанту моделі оцінки курсу надає найбільш масштабні перспективи для подальшого процесу формалізації та автоматизації систем дистанційного навчання військового призначення, що базуються на використанні останніх технічних розробок та новітніх інформаційних технологіях.

Рубан И.В., Шитова О.В.

ФОРМИРОВАНИЕ НАБОРА ПРИЗНАКОВ ИНФОРМАТИВНЫХ ОБЛАСТЕЙ ДЛЯ ИХ ЛОКАЛИЗАЦИИ НА ЦВЕТНЫХ ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ В СИСТЕМАХ ТЕХНИЧЕСКОГО ЗРЕНИЯ

Выбор признаков является необходимым шагом для решения задачи локализации информативных областей изображения при обработке изображений в системах технического зрения. Каждое цифровое изображение можно рассматривать как множество числовых признаков, заданных в пространстве, размерность которого определяется количеством пикселов изображения. Признак цифрового изображения определяется как функция от значений, содержащихся в одном или более пикселях, и вычисляется так, что численно выражает его некоторую значимую характеристику. Под признаковым описанием подразумевается минимальный набор признаков, характеризующих искомые области изображения, который позволяет решать задачу обнаружения и локализации областей на изображении с заданной достоверностью за минимальное время.

Для реализации работы предлагаемого метода обработки изображений формирование набора признаков областей изображений осуществлялось в три этапа. На первом этапе производился предварительный выбор признаков методом экспертного анализа, в результате которого были выбраны дешифровочные признаки объектов, так как операции обнаружения и локализации, по сути, близки к операции дешифрирования объектов на аэрофотоснимках. Так как известно, что основными дешифровочными признаками являются тон, размеры и форма объекта, то в качестве первоначального набора признаков было предложено выбрать соответственно, цвет, площадь и параметры формы искомых областей. Признаками цвета изображения, представленного в системе RGB, являются значения его интенсивностей. На втором и третьем этапах проводилась статистическая и экспериментальная оценка признаков формы областей изображения.

Было взято изображение с объектами разных классов. Для каждого объекта между классами и внутри классов были рассчитаны значения признаков формы средствами программного пакета Matlab 7.5.0 (R2007b). После чего были проведены статистические расчеты информативностей признаков формы. Признаки с минимальным колебанием значения внутри класса и наибольшим разбросом значений от класса к классу обладают наибольшей информативностью. Такими признаками являются площадь, эквивалентный диаметр и коэффициент заполнения области.

В результате проведенных исследований набор выбранных признаков имеет вид:

$$(I, S_{obl}, D_{obl}, K_{obl}),$$

где I - конечное множество значений интенсивностей искомой области, S_{obl} - площадь искомой области, D_{obl} - эквивалентный диаметр искомой области, K_{obl} - коэффициент заполнения.

Полученный набор признаков позволяет решать задачу локализации информативных областей изображения с достоверностью 0,91.

УДК 510.12

Турута А. П.

МОДЕЛИРОВАНИЕ СЕТЕВОГО ТРАФИКА С ЗАДАННЫМ ПАРАМЕТРОМ САМОПОДОБИЯ

Для моделирования трафика современных телекоммуникационных систем предлагается использовать самоподобные случайные процессы.

Активное использование сетевой инфраструктуры в человеческой жизни привело к росту трафика в информационных сетях, что в свою очередь, привело к развитию методов управления трафиком (трафик инжиниринг) в информационных сетях. Не всегда удается создать условия для тестирования разработанных методов в реальной сети, поэтому актуальным является разработка методов моделирования сетевого трафика в информационной сети.

Для моделирования трафика современных телекоммуникационных систем предлагается использовать самоподобные случайные процессы. Анализ литературы показывает, что используются два подхода к моделированию самоподобных процессов:

1) метод на основе использования Броуновского движения;

2) метод Мандельброта, который предполагает использование несколько независимых ON-OFF источников, у которых закон чередования включенного и выключенного состояния распределен по закону Парето.

Учитывая простоту задания параметра Херста в методе Мандельброта, второй метод получил наибольшее распространение при моделировании самоподобных случайных процессов. Указанные выше методы моделирования позволяют получить случайный самоподобный процесс заданной степенью самоподобия.

Однако, интенсивность нагрузки, создаваемая пользователями информационной сети существенно изменяется в течении суток, это связано с различной активностью пользователей, получающих как одинаковые, так и различные услуги. Следовательно, одного параметра Херста, недостаточно для моделирования суточного трафика, необходимо учесть динамические изменения нагрузки в течение суток, которая будет иметь место на практике.

Актуальной научно-практической задачей является разработка такого способа построения имитационной модели телекоммуникационной сети, которая позволила бы исследовать степень самоподобности трафика в телекоммуникационных сетях, полученного с учетом реально предоставляемых пользователям услуг.

Одного показателя Херста недостаточно для генерации адекватного самоподобного трафика, поэтому обеспечим адекватность генерации самоподобного трафика. Для решения за-

дачи имитационного моделирования используем агентное моделирование.

Предложенный подход позволяет сгенерировать пакетообразный трафик, но при этом не учитывается реальная активность абонентов, получающих различные услуги. Постоянным остаются такие параметры, как: средний объем передаваемых данных в единицу времени, распределение интенсивности в течении суток, признаки групп пользователей, признаки типа сервиса. Такой подход делается модель неадекватной с точки зрения предоставляемых услуг и является принципиальным недостатком предложенного способа моделирования.

Предлагается использовать агентный метод моделирования. Заменим ON-OFF датчик агентом – некоторой сущностью, которая будет обладать необходимой активностью, автономных поведением и будет принимать решения в соответствии с некоторым набором правил.

Построение агентной модели позволит получить представление об общем поведении системы, исходя из предположений об индивидуальном, частном поведении ее отдельных активных элементов и их взаимодействии в системе.

Обозначим число N - количество агентов в модели, тогда множество A - множество таких агентов, A_i - i-й элемент множества агентов и содержит характеристики агентов, a_i^j - j-я характеристика i-го агента, где $j = \overline{1,m}$, m-количество характеристик. В предложенной модели будем использовать 3 группы агентов ($N = 3$), а каждая группа агентов будет характеризоваться 5-мя признаками ($m = 5$) следующими признаками: количество агентов данной группы, продолжительность сессии, объем передаваемых пакетов, типы сервиса, полезность группы.

Агентный метод моделирования позволяет сгруппировать абонентов по любым признакам: по возрасту, профессиональной деятельности, увлечениям и др., что в свою очередь, даст возможность более детально учесть в модели особенности поведения абонентов и соответственно получить более точные результаты. В результате моделирования получен трафик, который характеризуется пачечным характером, однако заметна зависимость интенсивности нагрузки от времени суток. Предварительный анализ результатов моделирования показал, что трафик обладает свойствами самоподобия, а параметр Херста имеет значение в пределах 82-90. Экспериментально установлено, что при одном объеме трафика, большее количество пакетов, с меньшим объемом создадут трафик с большим коэффициентом самоподобия Херста, чем меньшее количество больших по объему пакетов. Построенная модель позволяет варьировать параметром Херста и суточным распределением интенсивности трафика, что может представлять интерес для дальнейших исследований в теории телетрафика.

Прагматическая значимость результатов моделирования сети обусловлена возможностью более точного прогнозирования динамических параметров нагрузки, что позволит в дальнейшем более точно оптимизировать структуру и состав телекоммуникационного оборудования и решить две основные задачи:

1) повысить, в целом, качество обслуживания агентов в сети;

2) осуществить повышение качества обслуживания не за счет затратных методов.

Применение описанного подхода позволит проводить оценку эффективности работы методов управления трафиком с различными исходными характеристиками.

УДК 510.12

Сезонова И.К.

ИНФОРМАЦИОННАЯ СИСТЕМА КРЕДИТНО-МОДУЛЬНОЙ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Для полноценного участия нашей страны в Болонском процессе, в соответствие с решением Берлинской конференции 2003 года, предстоит принять ряд мер по модернизации образования, и, в частности, ввести сопоставимую с общеевропейской систему многоуровневого

высшего образования.

Переход к Болонской системе образования предполагает создание условий для функционирования:

- двухуровневой системы высшего профессионального образования;
- введение системы зачетных единиц и балльно-рейтинговой системы оценки успеваемости для признания результатов обучения.

Эффективной современной технологией, позволяющей реализовать поставленные задачи, является технология электронного документооборота. Электронный документооборот позволяет организовать движение документа в электронном виде, что качественно меняет процесс составления, изменения содержания, узаконивания и хранения документа. Заметим, что речь идет не о делопроизводстве на компьютеризированном рабочем месте, а о принципиально иной структуре документооборота на основе современных информационных технологий.

Примером информационной системы кредитно-модульной организации учебного процесса ВУЗа является созданная в Харьковском национальном университете внутренних дел система Офис Методиста.

Основные задачи, решаемые с помощью Офис Методиста:

- построение единой информационной среды в рамках учебного процесса;
- формализация и прозрачное управление учебным процессом;
- учет и ведение индивидуальных учебных планов курсантов и студентов;
- мониторинг успеваемости и выполнения учебных планов;
- проведение сессии: электронные зачетные книжки, отслеживание академической успеваемости курсантов и студентов;
- автоматизированная подготовка типового набора документов, включая ведомости модульных контролей, итоговых модульных контролей, индивидуальных зачетных книжек;
- ведение журналов регистрации документов;
- гибкая система прав доступа к данным, возможность настройки специфических автоматизированных рабочих мест (арм);
- доступ в режиме просмотра для сотрудников, курсантов, студентов;
- оперативное предоставление информации родителям и опекунам курсантов и студентов;
- возможность удаленного доступа к единому банку данных и получения актуальной информации.

Курсанты с помощью Офис Методиста могут просмотреть:

- свою сводную ведомость успеваемости по итогам сессии; - расписание и график учебного процесса группы;
- свою электронную зачетную книжку;
- проверить правильность заполнения своего рейтинга, оценок и пересдач.

Сотрудники и преподаватели университета могут получить информацию:

- по контингенту курсантов и студентов университета;
- статистику по заполнению электронных рейтинговых ведомостей;
- по незаполненным и незакрытым ведомостям своей кафедры;
- найти информацию о курсанте, студенте, группе, специальности, институте и многое другое.

Однако следует отметить, что, как и всякое новшество, информационные технологии несут в себе и новые опасности, они могут служить и дестабилизирующим фактором. Ошибки, сделанные в процессе проектирования системы, дают о себе знать достаточно быстро в процессе эксплуатации системы и не всегда поддаются устранению. Поэтому процесс проектирования системы требует особого внимания и привлечения специалистов.

К типичным проектным ошибкам подобных систем можно отнести:

- отсутствие четкого разделения прав доступа в систему (с возможностью изменения данных) в соответствии с должностными обязанностями сотрудников;
- отсутствие модуля-анализатора процессов изменения данных в системе, который позволяет отследить подозрительные или неправомерные транзакции;

- отсутствие протокола действий системного администратора;

- отсутствие надежной системы идентификации пользователя (к сожалению, обычный парольный доступ продемонстрировал свою несостоятельность);

- отсутствие правил ведения архива, которые адекватны проектируемой технологии документооборота.

Созданный электронный архив должен обеспечивать оперативный и полноценный доступ ко всем документам, которые хранятся и поступают в систему. Для этого необходимо:

- ввести в систему модуль (базу данных) хранящихся в архиве документов;

- обеспечить возможность оперативного полнотекстового доступа к электронным документам.

Процесс управления внедрения проекта показал необходимость более детально нужно подходить к вопросу технологической зрелости организации, в данном случае вуза. Наличие достаточно количества компьютеров и локальной сети не эквивалентно технологической зрелости. В это понятие также необходимо включать наличие достаточного уровня знаний и навыков роботы с информационными системами у сотрудников и корректировку (утвержденную соответствующими внутренними приказами организации) их должностных обязанностей.

Система защиты информации должна выполнять следующие задачи.

Конфиденциальность. Информация должна быть защищена от несанкционированного прочтения как при хранении, так и при передаче. Если сравнивать с бумажной технологией, то это аналогично запечатыванию информации в конверт. Содержание становится известно только после того, как будет открыт конверт. Обычно обеспечивается шифрованием.

Контроль доступа. Информация должна быть доступна только для того, для кого она предназначена. Если сравнивать с бумажной технологией, то только разрешенный получатель может открыть запечатанный конверт. Обеспечивается также шифрованием.

Аутентификацию. Возможность однозначно идентифицировать отправителя. Если сравнивать с бумажной технологией, то это аналогично подписи отправителя. Обеспечивается электронной цифровой подписью и сертификатом.

Целостность. Информация должна быть защищена от несанкционированной модификации как при хранении, так и при передаче. Обеспечивается электронной цифровой подписью.

Неопровергаемость. Пользователь не может отказаться от совершенного действия. Если сравнивать с бумажной технологией, то это аналогично предъявлению отправителем паспорта перед выполнением действия. Обеспечивается электронной цифровой подписью и сертификатом.

УДК 371:004

Колісник Т.П.

ПЕДАГОГІЧНА МОДЕЛЬ ОПАНУВАННЯ ІНФОРМАЦІЙНИМИ ДИСЦИПЛІНАМИ КУРСАНТАМИ ВНЗ МВС УКРАЇНИ

Протидіяти сучасній злочинності здатні лише кваліфіковані, компетентні, фізично розвинені правоохоронці, які мають спеціальні навички боротьби зі злочинністю. Від рівня підготовки фахівців правоохоронної сфери залежить майбутнє не тільки держави, а й кожного члена суспільства. Професійна діяльність не може бути успішною, якщо працівник органів внутрішніх справ, не володіє адекватними навиками роботи у сучасному інформаційному середовищі, не володіє інформаційною культурою.

Процес інформатизації суспільства ініціює процес інформатизації освіти, в особливості - інформатизації вищої школи. Інформатика поряд з філософією і математикою по відношенню до інших галузей знань розглядається в якості системоутворюючої науки. Вона стала і однією з основних навчальних дисциплін.

Завдання, що постають перед системою інформаційної підготовки фахівців, призводять до

пошуку не тільки нових форм й методів навчання, але й нової концепції методичної системи.

У зв’язку з вищенаведеним, вважаємо достатньо актуальним і доцільним акцентувати увагу на питанні удосконалення методики навчання інформатики курсантів ВНЗ МВС України.

Відповідно до методології наукового пізнання будь-яке судження з будь-якого предмету завжди спирається на деяку модель даного предмету - уявний образ досліджуваного об'єкта чи процесу, який заміняє його в процесі пізнання і який передає його найбільш істотні з погляду розв'язуваної задачі якості і властивості. У педагогічних дослідженнях існує кілька підходів до моделювання процесу навчання [1, 2], однак у дослідженнях з методики навчання дисциплін фізико-математичної групи є традицією використовувати модель методичної системи навчання.

Згідно А.М.Пишкало, методична система навчання являє собою сукупність п'яти ієрархічно підлеглих компонентів: цілей навчання, його змісту, методів, засобів, організаційних форм навчання.

Модель методичної системи навчання повинна відповідати наступним принципам.

Предметність моделі. Моделі навчання різних предметів можуть включати різні сукупності компонентів, а ці компоненти - знаходитися в специфічних для даного предмета відношеннях між собою. Таким чином, можна очікувати, що структурно методичні системи навчання різних предметів будуть відрізнятися.

Локальність моделі. Через істотні й все більш зростаючі розходження в цілях і умовах навчання в різних навчальних закладах вже не можна говорити про методичну систему навчання предмету взагалі. Модель повинна враховувати не тільки розходження у навчанні різних предметів, але й особливості у вивченні предмета, що склалися в конкретному навчальному закладі. Таким чином, удосконалена модель методичної системи повинна враховувати локальні особливості навчання інформатики, тобто змінюватися від одного навчального закладу до іншого.

Динамічність моделі. Компоненти методичної системи, як правило, знаходяться у швидкому розвитку, регулярно перебудовуються зв'язки між цими компонентами. Так для інформатики характерна нестабільність, швидкі зміни в змісті навчання, бурхливий розвиток засобів інформатизації, що впливають на цілі, зміст, методи, засоби навчання. Методична система, як модель навчання, повинна передбачати розвиток практики навчання, включати компоненти, які передбачають розвиток їхнього змісту, які допускають перебудову їх структурних зв'язків.

У якості методологічної основи удосконалення методичної системи навчання інформатики розглядається принцип гуманітаризації.

Гуманітаризація освіти є метою і засобом цілісного розвитку та формування духовно багатої, орієнтованої на загальнолюдські цінності особистості. Гуманітаризація освіти - це процес, спрямований на засвоєння особистістю гуманітарного знання, гуманітарної культури, гуманітарного потенціалу кожної досліджуваної області знань, на присвоєння особистістю суспільно-значущих цінностей досліджуваного знання. Основне завдання гуманітаризації освіти - зробити суспільно-значущі цінності будь-якого виду освіти, в тому числі і навчання інформатики, особистісно-значимими для кожного курсанта.

Всі компоненти традиційної методичної системи повинні бути якісно переосмислені з позицій гуманітаризації освіти. Сучасна дидактика трактує навчання як цілеспрямоване, заздалегідь запроектоване спілкування, в ході якого здійснюється освіта і розвиток курсантів. Тому зазначені елементи системи повинні бути доповнені ще одним, що впливає на зміст всіх інших, - особистісним, моделлю цілісної структури особистості. Таким чином, методична система навчання інформатики включає в себе наступні елементи: цілісну структуру особистості, цілі, зміст, методи, форми та засоби навчання (у тому числі нормативні документи, підручники, навчальні посібники, методичні рекомендації), готовність викладача.

Сутність кожного компонента системи визначається його складними багатосторонніми зв'язками з іншими. Виходячи з моделі цілісної структури особистості і відповідно цілісного розвитку особи-

стості (психічної підструктури, що включає в себе емоційно-вольовий компонент, а також сприйняття, уявлення, пам'ять, мислення; пізнавальної підструктури, орієнтованої на присвоєння гуманітарно-орієнтованого змісту, спрямованості, що складається з переконань, ідеалів, світогляду та ін.), розглядаючи інформатику з позицій специфіки її викладання, можна визначити гуманітарно-орієнтований зміст і цілі навчання інформатики.

Випускник вищого навчального закладу опанував інформаційними технологіями, якщо він знає сутність предмета інформатики; знає основні поняття інформатики і вміє оперувати ними; володіє комп'ютерною мовою та математичною символікою; має уявлення щодо комп'ютерного моделювання; вміє будувати інформаційні моделі найпростіших реальних явищ і процесів; має уявлення про прикладні аспекти інформатики; має уявлення про вплив інформатики на соціальний розвиток суспільства і навпаки; долучився до досвіду творчої діяльності і вміє застосовувати його в інших видах діяльності; знає основні загальнонаукові методи пізнання (евристичні та логічні) і вміє застосовувати їх як у програмуванні, так і в інших видах діяльності; володіє основами культури мислення; володіє культурою спілкування, культурою праці; має уявлення про основні періоди розвитку інформаційних технологій як частини загальнолюдської культури.

Проведене дослідження дозволяє зробити такі **висновки:** ефективність навчання інформатики курсантів значно підвищиться, якщо навчання інформатики буде будуватися на принципах поетапності й модульності побудови навчання; структура формування інформаційної культури працівника органів внутрішніх справ буде побудована на основі діяльністної моделі.

Методична система навчання інформатики курсантів ВНЗ МВС України потребує подальшого удосконалення. Основні напрями її удосконалення пов’язані з формуванням інформаційної культури працівника правоохоронної сфери, з специфікою сучасної їх діяльності.

Список використаних джерел

1. Беспалько В.П. Слагаемые педагогической технологии.-М:.Педагогика, 1989.-192 с.
2. Гинецинский В.И. Основы теоретической педагогики.-СПб.:Изд-воСпбУ,1992.-154с.

УДК 351: 681.5

Тузіков С.А., **Писарєв А.В., Карманний Є.В.**, **Яценко В.В.**

ІНТЕРАКТИВНІ АСПЕКТИ ПІДГОТОВКИ СПІВРОБІТНИКА ПРАВООХОРОННОГО ОРГАНУ ЯК ВИХОВАТЕЛЯ

Обговорюються системоутворюючі характеристики сучасного вихователя, способи їх впровадження в систему підготовки співробітника правоохоронного органу із застосуванням інтерактивних аспектів інформаційних технологій

В сучасних умовах розвитку суспільства в Україні важливу роль грає процес виховання молоді, який на даний час є незадовільним. У зв’язку з цим значно зростає роль співробітників правоохоронних органів (ПО), як вихователів молоді. Тому підготовка співробітника правоохоронного органа як вихователя у вищих навчальних закладах (ВНЗ) стає об'єктивною потребою.

Формування фахівців ПО – процес тривалий і багатогранний. Він продовжується все життя людини і обіймає виховання необхідних культурно-духовних цінностей та культуру мовлення, моральних, інтелектуальних, психологічних та естетичних якостей. В сучасному українському суспільстві все більше відчувається нестача вихователів, які є носіями високої культури та освіти.

У ВНЗ необхідно поряд з навчанням за основними навчальними дисциплінами створити об'єктивні умови для гармонічного розвитку особистості майбутнього співробітника ПО, як вихователя. Перспективним напрямком у вирішенні проблеми підготовки співробітника правоохоронного органа як вихователя є впровадження в організацію освітнього процесу новітніх інтерактивних аспектів, як найбільш вагомої складової інформаційних технологій.

З точки зору авторів, найбільш суттєві результати серед інтерактивних аспектів дають такі методи навчання як: ситуація-ілюстрація; ситуація-проблема; ситуація-інцидент; інформаційний лабіринт тощо. Вказані методи широко використовуються нашою кафедрою при підготовці співробітника ПО як вихователя.

Зростання масштабів, складність і динамізм інтерактивних аспектів сучасних інформаційних технологій в галузі планування, керування діями в правоохоронний діяльності а також ролі інформаційної боротьби наполегливо вимагає не тільки кількісного збільшення, а й якісного розширення виховних можливостей співробітника при отриманні та обробці великих масивів інформації.

Керування правоохоронною діяльністю є найважливішим чинником попередження скоєння злочинів. Знання, досвід, особисті можливості співробітника - вихователя сьогодні потребують невідкладного використання комп'ютерів. Застосування комп'ютерних мереж по-новому вирішує задачу розробки методик розрахунку правоохоронних дій, вирішення задач попередження скоєння злочину, а також ефективної роботи ПО в умовах реального часу.

Розвиток інтерактивних аспектів сучасних інформаційних технологій призводить до зростання ролі викладача як керівника педагогічного процесу та виховання студента (курсанта). Студентам важлива допомога не лише в оволодінні системою знань, а ще в їх систематизації. Майстерність викладача передбачає збудження творчої індивідуальності кожного студента. Усе це, в цілому, зумовлює і формує у студентів творчу співпрацю, інтуїцію, інтелект, винахідливість, передбачливість, постійний культурний ріст та інші здібності.

Таким чином, однією з найважливіших задач, що стоять перед ВНЗ, є впровадження новітніх інтерактивних аспектів інформаційних технологій, вдосконалення методів викладання та зростання ролі викладача при формуванні співробітника правоохоронних органів, як вихователя.

УДК 614: 681.5

Лазутський А.Ф., **Зенін А.П., Молодцов В.А.**, **Чудновський І.Т.**

ПРАКТИКА ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНИХ ЗАСОБІВ У ВИВЧЕННІ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ"

Розглядаються актуальні методики застосування інформаційно-технічних засобів при викладанні дисципліни "Безпека життєдіяльності", їх вплив на якість підготовки викладача та засвоєння програми дисципліни студентами, з урахуванням змін у функціонуванні потоків різнопланової інформації

Короткий аналіз розвитку методики використання екранно-звукових засобів та інформаційних технологій у викладанні курсу навчальної дисципліни "Безпека життєдіяльності" та комп’ютерних технологій у вищій школі свідчить про наявність низки невирішених питань, які необхідно враховувати в ході подальшого удосконалення педагогічного процесу. Найактуальнішими з них є:

1. Визначення наукової і дидактичної цінності відео-, фотодокументів, фонозаписів, комп’ютерних навчальних програм, отриманих в результаті використання інформаційних технологій.

2. Визначення місця і ролі інформаційних технологій і аудіовізуальних засобів у системі навчальних занять з усіх навчальних предметів у вищій школі.

3. Розробка методики роботи з інформаційними технологіями і аудіовізуальними засобами на лекційних і практичних заняттях вищів з урахуванням соціально-психологічних особливостей студентів.

4. Визначення форм і методів комплексного використання інформаційних технологій і аудіовізуальних засобів у педагогічному процесі.

Вирішення цих завдань дозволить цілеспрямованіше і ефективніше залучати інформаційні технології і традиційні екранно-звукові посібники при вивченні навчальної дисципліни "Без-

пека життєдіяльності" у ВНЗ і зробити викладання інтенсивним, об'ємним і оптимальним.

Останнім часом інформаційне поле України (як одне з трьох, у яких, за сучасних понять, живе людина) значно змінилось. Такі аргументи, як екологія, техногенність, соціально-економічні умови, кількісні і якісні чинники комунікаційних систем змінили докорінно результати функціонування потоків інформації. Ці потоки можна звести до: сенсорного потоку, що сприймається органами почуттів через центральну нервову систему; вербального потоку усних і письмових слів; структурного потоку, компонентами якого є вода, їжа, повітря.

Виходячи з вищевикладеного, можна зробити висновок про те, що в зв'язку з інформатизацією, що бурхливо протікає, і комп'ютерізацією навчального процесу і навчальних закладів, кожний викладач навчальної дисципліни "Безпека життєдіяльності" повинний мати навички роботи з ТЗН, а зокрема з ПЕОМ для створення прикладних пакетів навчання і автоматизованого обліку педагогічного процесу.

Список використаних джерел

1. Кухаренко В.М, Рибалко О.В., Сиротинко Н.Г. Дистанційне навчання: Умови застосування. Дистанційний курс: Навчальний посібник. 3-є вид. / За ред. В.М. Кухаренка. – Х.: НТУ "ХПІ", "Торсінг", 2002. – 320 с.

2. Машблиц Е.И. Психолого-педагогические проблемы компьютеризации обучения. – М.: Педагогика, 1988. – 192 с.

3. Основні технології: Навч.-метод. посіб. / О.М. Пєхота, А.З. Кіктенко, О.М. Любарська та ін..; За заг. ред. О.М. Пєхоти. – К.: А.С.К., 2002. – 255 с.

УДК 614: 681.5

Малько О.Д., **Ковжога С.О.**, **Полєжаєв А.М.**, **Карташов І.М.**

ПРО ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАННЯ У СФЕРІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Розглядаються методичні аспекти використання інформаційних технологій навчання, як пріоритетний напрямок вдосконалення навчального процесу у сфері безпеки людини, що дозволить створити принципово нову інформаційну освітню складову захисту людини від небезпек

В сучасних умовах одним із основних напрямків інтенсифікації навчального процесу у сфері безпеки життєдіяльності є використання інформаційних технологій навчання (ІТН). В якості елементів ІТН можуть використовуватися:

– електронні підручники і навчальні посібники, курси лекцій;

– програми-тренажери (репетитори);

– контролюючі елементи (тестові завдання);

– інформаційно-довідкові джерела (довідкова інформація та енциклопедії);

– імітаційні моделі;

– демонстраційні засоби (слайди або відеофільми);

– навчально-ігрові засоби (ситуаційні та логічні завдання, правила і стратегії поведінки, рольові вправи тощо).

Застосування зазначених елементів ІТН в навчальному процесі при вивченні безпеки життєдіяльності дозволить підвищити:

– ефективність навчального процесу за рахунок одночасного доведення викладачем теоретичних положень і показу демонстраційного матеріалу;

– візуалізацію знань, індивідуалізацію та диференціацію навчання студентів внаслідок поліпшення можливостей отримання будь-якої навчальної інформації та її практичного використання;

– достовірність і наочність викладання навчального матеріалу;

– мотивацію студентів до навчання за рахунок привабливості мультимедійних ефектів, які можливо використовувати в комп'ютері;

– оперативність оцінки обстановки наслідків можливих надзвичайних ситуацій внаслідок проведення електронних розрахунків та застосування моделювання небезпечних процесів та явищ і використання інформаційної бази як окремих комп'ютерів, так комп'ютерних систем і мереж в процесі вирішення навчальних завдань;

– навички наглядно-образного мислення, моторні, комунікативні та вербальні можливості студентів.

Отже, впровадження ІТН є пріоритетним напрямом вдосконалення навчального процесу у сфері безпеки людини. Широке використання ІТН дозволить створити принципово нову інформаційну освітню складову захисту людини від небезпек, що розкриває широкі можливості для активізації навчального процесу і модернізації традиційної системи навчання.

УДК 681.324

Алексєєв С. В.

ОПТИМАЛЬНА ФРАГМЕНТАЦІЯ ПАКЕТІВ У МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ

Комутація пакетів у сучасних мережах передачі даних є основним способом передачі, оскільки:

- характеризується малими затримками передачі даних;
- не вимагає однакової пропускної спроможності всіх ліній зв'язку, із яких формується канал (як при комутації каналів);
- передача пакетами створює найкращі умови для мультиплексування потоків даних (розділення часу роботи лінії зв'язку для одночасної передачі декількох потоків даних);
- мала довжина пакету дозволяє виділяти для проміжного зберігання даних менший розмір пам'яті;
- менша дина пакетів у порівнянні з повідомленнями зменшує ймовірність їх спотворення в каналах зв'язку (КЗ) і спрощує процедури перезапиту даних.

У мережах передачі даних з комутацією пакетів використовуються три способи передачі даних: хвильовий, дейтаграмний і віртуальний канал.

Хвильова доставка інформації застосовується у випадках, коли потрібне сповіщення всіх вузлів мережі. Найчастіше - для передачі службової інформації, наприклад, для корекції таблиць маршрутизації.

При дейтаграмному способі пакети передаються як незалежні об'єкти, внаслідок чого кожен із пакетів може слідувати будь-яким із можливих маршрутів і поступати до одержувача в довільному порядку. Не гарантується також і надійність доставки даних.

У режимі віртуального з'єднання заздалегідь встановлюється логічне з'єднання - віртуальний канал, по якому передаватимуться дані. Віртуальним каналом є множина вузлів комутації і ліній зв'язку, що з'єднують їх і створюють маршрут руху пакетів через мережу від джерела до одержувача. При цьому зберігаються всі переваги комутації пакетів відносно швидкості передачі і мультиплексування, а також забезпечується природний порядок проходження даних.

На ефективність роботи мережі впливають розміри пакетів даних, які передаються в ній.

Великі пакети наближають мережу з комутацією пакетів до мережі з комутацією каналів. Крім того, при цьому збільшується час буферизації на комутаторах. Малі пакети істотно збільшують частку службової інформації, оскільки кожен пакет містить заголовок фіксованої довжини.

У більшості типів сучасних локальних і глобальних мереж визначено поняття максимального розміру поля даних кадру (пакету), в які повинен інкапсулювати свій пакет протокол IP. Цю величину зазвичай називають максимальною одиницею транспортування - Maximum Transfer Unit, MTU. Мережі Ethernet мають значення MTU, що дорівнює 1500 байт, мережі

FDDI - 4096 байт, а мережі X.25 найчастіше працюють з MTU в 128 байт.

У складеній мережі, класичним прикладом якої є Інтернет, початковий пакет може бути фрагментований.

Розбиття дуже великого для конкретного типу складової мережі пакету на коротші здійснюється протоколом IP. При цьому фрагменти забезпечуються набором службових полів, необхідних для подальшої їх збірки в початковий пакет. IP-маршрутизатори не збирають фрагменти в крупніші пакети, навіть якщо на шляху зустрічається мережа, що допускає таке укрупнення. Це пов'язано з тим, що окремі фрагменти можуть переміщатися далі по мережі різними маршрутам.

При виборі довжини пакету необхідно враховувати якість каналу зв'язку. На ненадійних каналах доцільно використовувати пакети менших розмірів, оскільки це зменшує обсяг даних, що передаються повторно.

Проведені дослідження біт-орієнтованої процедури передачі даних з квитуванням для однієї ланки передачі без урахування додаткових потоків інформації на вузлах комутації показали, що при довільному законі розподілу помилок у каналі зв'язку за заданих умов можливо досягти зменшення середнього часу доставки і/або підвищення достовірності даних за рахунок вибору числа фрагментів.

Критерієм оптимальної фрагментації пакетів для досягнення максимально можливого зменшення середнього часу доставки даних без урахування зміни ймовірності помилки в них є максимум відношення середнього часу доставки вихідного пакету до середнього часу доставки фрагментованого пакету.

Критерієм фрагментації вихідних пакетів для досягнення максимально можливого зменшення ймовірності помилки даних без урахування зміни середнього часу їх доставки є максимум відношення ймовірності помилки вихідного пакету до ймовірності помилки фрагментованого пакету.

Критерієм оптимальної фрагментації вихідних пакетів для досягнення найбільшого можливого зменшення ймовірності помилки даних і середнього часу їх доставки може бути максимум множення відношення ймовірності помилки вихідного пакету до ймовірності помилки фрагментованого пакету на відношення середнього часу доставки вихідного пакету до середнього часу доставки фрагментованого пакету при обмеженні, що кожне з відношень більше одиниці.

Віртуальний канал за своєю суттю є впорядкованою підмножиною елементарних ланок передачі даних, що є елементами мережі, оскільки складається з деякого фіксованого числа ліній зв'язку і комутаторів. Тому представляє інтерес дослідження можливості поліпшення основних імовірнісно-часових характеристик процесу передачі даних за рахунок вибору розміру фрагментованих пакетів.

При цьому основними напрямами досліджень будуть:

- оптимальна фрагментація в кожній ланці віртуального каналу;
- вибір розміру фрагмента, єдиного для всіх ланок віртуального каналу.

Дуденко С.В., Колмиков М.М.

МЕТОДИКА ПЛАНУВАННЯ ПРОФЕСІЙНОГО НАВЧАННЯ ФАХІВЦІВ ВНУТРІШНІХ ВІЙСЬК МВС УКРАЇНИ

Запропонована методика планування професійного навчання фахівців внутрішніх військ МВС України дозволяє аналізувати складений план навчання та приймати рішення щодо доцільності проведення підготовки фахівців за варіантом плану.

Процес організації професійного навчання фахівців внутрішніх військ МВС України та місце запропонованої методики планування подано на рис.1.

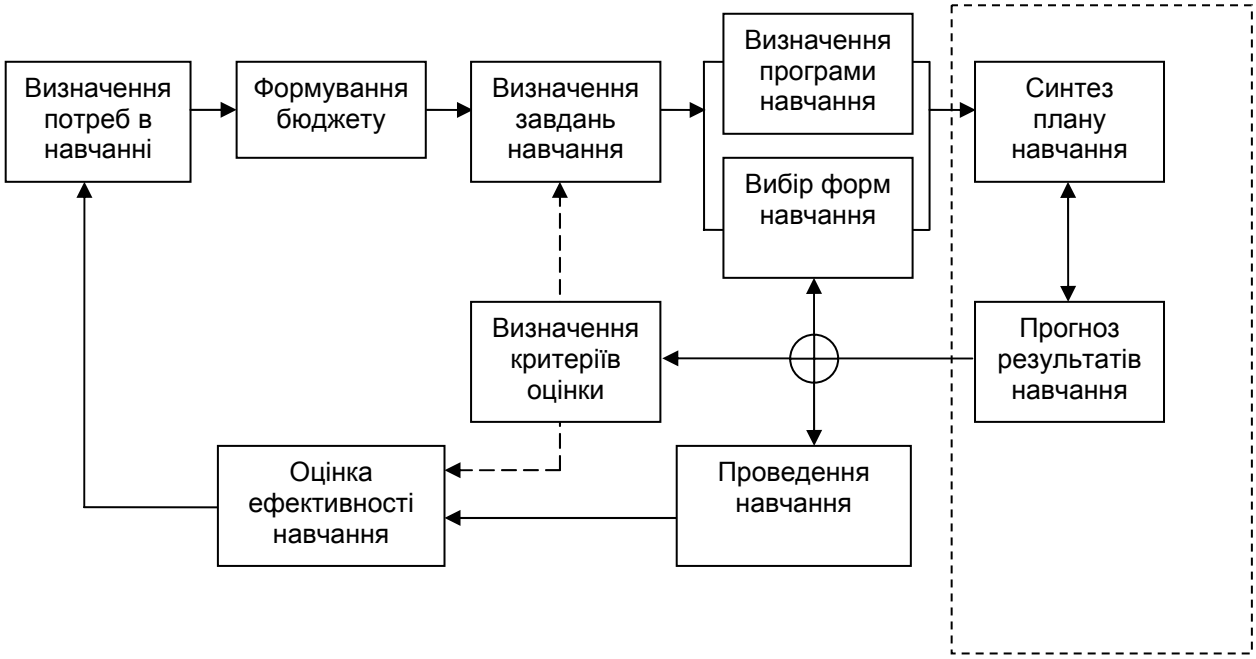


Рис. 1. Організація професійного навчання фахівців з використанням запропонованої методики планування

Розглянуті в дослідженнях моделі та методи інформаційної підтримки процесу планування професійного навчання представлені узагальненою методикою їх використання, яка представлена у вигляді алгоритму на рис. 2. Таким чином, створена певна послідовність дій, при виконанні якої отримаємо необхідну інформацію щодо доцільності організації професійного навчання фахівців внутрішніх військ МВС України з погляду прогнозу рівня знань.

Розглянемо кожен з цих кроків, які демонструють основні прецеденти сценарію підготовки.

Етап 1. Після виникнення задуму на підготовку фахівців внутрішніх військ МВС України виникає задача формування завдань проекту впровадження, до вирішення якої можуть бути залучені досвідчені фахівці. Декомпозиція завдань дозволить визначити потреби в навчанні (рис. 2). Маючи відповідний бюджет на організацію навчання та завдання (цілі) навчання можна приступати до другого етапу.

Етап 2. Оцінка початкового рівня підготовки фахівців внутрішніх військ МВС України, наявної навчально-матеріальної бази, що планується до використання, досвід викладачів, які будуть проводити заходи підготовки є підґрунтям для моделювання (прогнозу) результатів навчання.

Етап 3. Маючи вихідні данні маємо змогу проводити синтез варіанту плану організації професійного навчання на основі алгоритму синтезу плану, тобто моделювати взаємозв'язані заходи різних організаційних форм системи підготовки фахівців на основі розрахункової моделі забування знань і втрати умінь та навичок тих, хто навчається.

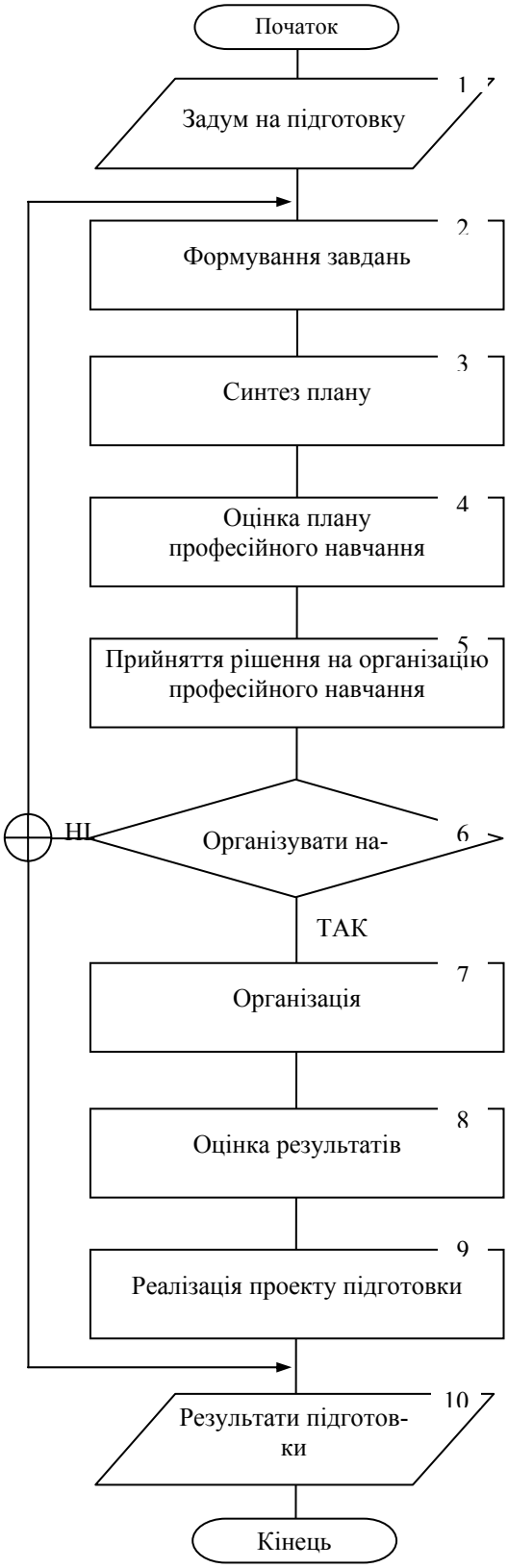


Рис. 2. Узагальнений алгоритм методики планування професійного навчання фахівців внутрішніх військ МВС України

Процес планування складається з операцій додавання заходів плану у чарунки робочого поля програми та подальшого їх редагування. При цьому автоматично проходить зміна даних панелі графіка, що відображає автоматичні розрахунки прогнозу.

Етап 4. Оцінка плану здійснюється за двома основним показниками: прогноз рівня підго-

товки фахівців внутрішніх військ МВС України і показника повернення на навчання фахівців.

Етап 5. Провівши автоматично оцінку плану інформаційна система забезпечує особу, що приймає рішення, необхідною інформаційною підтримкою для прийняття рішення на доцільність проведення професійного навчання з метою виконання завдань підготовки. Ця інформація включає в себе:

1. Відповідь на питання чи можливо ефективно виконати проект підготовки з погляду вкладених інвестицій.
2. У випадку неможливості досягнення мети встановлює причини та можливі шляхи вирішення.
3. Економічні показники від реалізації як професійного навчання фахівців внутрішніх військ МВС України так і впровадження підготовки.

Виконання кожного з етапів вимагає відповідної підготовки та чіткої координації дій спеціалістів та фахівців МВС України.

УДК 378.172

Русскін В.М.

ВИКОРИСТАННЯ СУЧАСНИХ КОМП'ЮТЕРНО-ОРІЄНТОВАНИХ ЗАСОБІВ НАВЧАННЯ ПРИ ВИВЧЕННІ ДИСЦИПЛІН ФІЗИКО-МАТЕМАТИЧНОГО ЦИКЛУ

Сьогодні велика увага приділяється комп'ютеризації навчальних закладів, інформатизації навчально-виховного процесу, розробці індивідуальних завдань різних рівнів складності, створення електронних підручників, інтелектуальних комп'ютерних і дистанційних технологій навчання. І саме створення сучасних засобів навчання, що поєднують матеріал конкретної дисципліни з можливостями інформаційно-комп'ютерних технологій і є важливою передумовою досягнення цілей освіти.

Інформатизація сучасної вищої освіти, з одного боку, і поступове зменшення кількості годин, що відводяться на вивчення деяких навчальних дисциплін у вузах (зокрема математичного напрямку), з іншого, змушують шукати такі форми проведення традиційних навчальних занять (лекцій, лабораторних чи практичних робіт), які дозволили б в умовах зменшення часу навчання не тільки домогтися збереження рівня підготовки студентів, але навіть підвищити його.

Багато викладачів здійснюють пояснення нового матеріалу традиційно, використовуючи у своїй практиці лекційний метод, орієнтуючись при цьому на рівень підготовки кожного студента. Вони вважають, що лекція - один з найважливіших видів навчальних занять, вона дозволяє педагогові викладати навчальний матеріал в узагальненій формі, адаптованій до рівня знань і професійної орієнтації студентів певного курсу відповідної спеціальності [2].

При проведенні лекції проявляється наукова ерудиція педагога, визначається його особиста позиція з окремих питань. Тому ті, хто говорить, що викладач не є головним й безпосереднім джерелом інформації, особливо під час лекції, дуже помиляються. Для того, щоб лекція була проведена на високому рівні, студенти одержали глибокі знання, необхідно на ній використовувати найпередовіше устаткування, а саме: комп'ютери, мультимедійну дошку Smart Board, сучасні технічні засоби навчання (діапроектор, епіпроектор) тощо. При цьому слід також враховувати те, що не кожна лекція може бути оснащена сучасним комп'ютерним устаткуванням, оскільки воно дуже дороге і не кожний навчальний заклад може собі дозволити його купити.

В цілому очевидно, що комп'ютеризація лекції не робить цей вид навчальних занять найбільш ефективним. Можна відмітити те, що традиційна форма проведення лекцій відповідає сучасному стану навчального процесу й не має потреби в значній комп'ютеризації.

Метою статті є показати переваги комп'ютерного забезпечення навчального процесу над традиційними формами проведення лабораторних робіт.

Комп'ютеризація навчального процесу повинна безумовно торкатись лабораторних занять, їх виконання при вивченні дисциплін фізико-математичного циклу.

З метою підвищення ефективності професійної підготовки студентів Харківського гумані-

тарно-педагогічного інституту, майбутніх вчителів інформатики, нами був застосований комплекс комп'ютерних програм для застосування їх при проходженні лабораторного практикуму з дисциплін фізико-математичного циклу, а саме: «Методи обчислень», «Комп'ютерне моделювання», «Фізика» та ін., який містить у собі взаємозв'язок «комп'ютер-викладач»: джерело навчальної інформації (електронний підручник, в якому багато графічних матеріалів, фото - та відео ілюстрацій); тренажер розвитку практичних навичок для професійної діяльності; засіб діагностики і контролю знань студентів (безпомилкова перевірка правильності ходу лабораторної роботи та висновків.

Ми вважаємо, що комп'ютеризація лабораторно-практичних робіт дозволить активізувати діяльність студентів, дасть можливість наочніше продемонструвати зв'язок теорії із практикою, підвищити рівень лабораторних експериментів, наблизивши їх до експериментально-дослідницьких методів досліджуваних наук, забезпечить зацікавленість молодих людей у сучасних формах роботи з інформацією, інтелектуалізацію навчальної діяльності [1].

Переваги комп'ютеризації лабораторних робіт очевидні. Це відсутність підготовчої частини лабораторних робіт, що займає значну частину часу лабораторного заняття; швидкість виконання лабораторних робіт; дешевизна устаткування в порівнянні із традиційними приладами, стендами; можливість виконання більшої кількості робіт.

Якщо розглянути будову сучасних лабораторних стендів, то це найчастіше закриті ящики, в яких всередині відбуваються всі досліджувані процеси, назовні виводяться на екрані монітора чи осцилографа кінцеві результати. Таким чином, протікання зазначених експериментальних процесів залишається схованим від зору студента. Це є серйозним недоліком, тому що на старших курсах студентам пропонується самим створювати, а потім збирати найпростіші лабораторні стенди-схеми при вивченні фізики. Якщо ж така схема створюється студентом на комп'ютері, він одразу ж випробовує її дію у своїй дослідницькій діяльності.

Таким чином, комп'ютеризація лабораторних робіт, зокрема при викладанні фізико-математичних дисциплін, дозволяє вирішити важливі завдання навчального процесу, а саме дати можливість студентам експериментальним шляхом, самостійно переконатись у вірності того чи іншого твердження, чи явища.

Підвищення ефективності навчального процесу спостерігається й у застосуванні комп'ютерів при проведенні практичних занять. По-перше, комп'ютери, придбані для проведення лабораторних робіт, можна використати й для виконання завдань практичного змісту на заняттях. По-друге, розв'язання завдань на комп'ютері дозволяє позбавити студента від рутинних розрахунків і досить значно заощаджує час. З методичної точки зору, виконання студентами завдань у спеціалізованих пакетах прикладних програм повинне заохочуватися, оскільки пакети спрощують важкі математичні розрахунки. Перевагою прикладного програмного забезпечення є супровід його великою кількістю демонстраційного матеріалу. Користувачі можуть обмінюватися результатами своїх робіт, обговорювати виникаючі проблеми, тобто обмінюватись між собою інформацією, що сприяє їх розвитку як науковців, співрозмовників, особистостей, які на все мають свою думку. Набуті під час розв'язування завдань знання та практичні навички слугуватимуть достатньо міцним підґрунтям для успішного розв'язування конкретних прикладних задач, зокрема з математики, фізики, інформатики тощо.

Комп'ютерно-лабораторні практикуми дозволяють студентам закріпити і розширити знання, отримані на лекціях та при роботі з книгою. Процес виконання лабораторної роботи багато в чому відтворює процес перебігу наукової роботи: одержання "спостережних" даних, первинна їх обробка, обчислення, аналіз отриманих результатів та їх оформлення, формулювання висновків.

Список використаних джерел

1. Бержанський В.Н., Лагуиов І.М., Гордієнко Т.П. Застосування інформаційних технологій при недостатності знань комп'ютерних дисциплін //Вісник Чернігівського державного педагогічного університету імені Т.Г.Шевченка. Випуск 3. Серія: Педагогічні науки: Збірник. - Чернігів: ЧДПУ, 2000, ЖЗ, С. 149-154.

2. Леонтьева В. Компьютеризация и «креативная педагогика»/ В.Леонтьева, М.Щербина //Высшее образование в России. - 2002. - №3. - С. 138-141.

УДК 378.172

Русскін В.М.

ЗАДАЧНИЙ ПІДХІД ЯК ПРОВІДНИЙ ЗАСІБ ФОРМУВАННЯ ТВОРЧОЇ АКТИВНОСТІ НА ЗАНЯТТЯХ З ІНФОРМАТИКИ

Удосконалення системи національної освіти і підвищення якості сучасного навчально-виховного процесу відкривають широкі можливості для оновлення змісту, обсягу та структури всіх шкільних предметів, посилення їх розвиваючих функцій і спрямованості на формування всебічно-гармонійної особистості. Особливої актуальності на сучасному етапі розвитку нашої держави набувають проблеми формування всебічно-гармонійної особистості. Орієнтуючись на сучасний ринок праці, освіта до пріоритетів сьогодення відносить уміння оперувати такими технологіями та знаннями, що задовольнять потреби інформаційного суспільства, готують молодь до нової ролі в цьому суспільстві. Саме тому важливим нині є не тільки вміння користуватися власними знаннями, а й бути готовим змінюватись і пристосовуватись до нових потреб ринку праці, оперувати й управляти інформацією, активно діяти, швидко приймати рішення, навчатись протягом життя. Освітня спільнота ставить перед собою нове завдання – сформувати в школяра та дорослого вміння вчитись.

У науково-педагогічній літературі існують різні підходи до проблеми "задача". Так, можна відзначити плідну пошукову діяльність у цьому напрямі вчених Л.Ф. Спіріна, В.О. Сластьоніна, Д.М. Гришина, Л.М.

Застосовуючи індивідуалізацію навчання, слід враховувати змістовну та організаційну сторони навчального процесу як комплекс розвивальних завдань, які активізують навчально-пізнавальну діяльність

Формування творчої активності учня засобами комп’ютерних технологій недостатньо розкрито у вітчизняній педагогіці, а разом з тим не визначено підходи до розвитку формування творчої активності, тому завданням нашого дослідження є аналіз задачного підходу та його можливостей у підготовці учня як творчого фахівця, який само реалізує себе у професійній діяльності.

Педагогічна задача усвідомлюється як задача, коли виконуються наступні умови:

1) у процесі педагогічної діяльності виникають певні утруднення, подолати які можна декількома способами;

2) висувається вимога знаходження оптимального способу досягнення бажаного результату із множини рішень. Задачний підхід як провідний засіб формування творчої активності учня обирається одне, яке слугує критерієм;

3) має місце система обмежень при переході з одного стану в інший. Як обмеження виступають засоби, що обов'язково використовуються при розв'язанні задачі.

Отже, процес розв'язання задачі можна уявити у вигляді пошуку виходу з проблемної ситуації або як процес досягнення мети. Проблемне навчання спрямоване на розвиток цілісної особистості, здатної самостійно оволодівати знаннями і творчо використовувати їх на практиці. Воно передбачає створення проблемної ситуації, розробку проблемних завдань, питань, які містять у собі приховане протиріччя. Відправним пунктом у процесі формування творчої активності виступає проблемна ситуація. Структурно вона поєднує три компоненти:

1) дія, що народжує пізнавальну потребу в новому;

2) те нове, що треба відкрити для виконання діяльності;

3) рівень знань і можливості суб’єкта (в тому числі творчих). Отже, зберігаються усі три сторони формування творчої активності майбутнього фахівця, на які спрямовані дидактичні умови.

Перспектива задачного підходу у формуванні творчої активності майбутнього фахівця полягає у введенні засобів комп’ютерних технологій у процес підготовки майбутнього фахівця.

Багато педагогів-дослідників, які розвивають тему проблемного навчання, згадують бінарні методи (за М. Махмутовим), що є для нашого дослідження вагомим підґрунтям. Ці методи відображають характер взаємодії "викладач – учень" і пов'язані з розумовою діяльністю студента та самою діяльністю, тобто із використанням засвоєних нових понять, дій, умінь, навичок на практиці. Бінарні методи спрямовані на активізацію мислення, пам'яті, пізнавальної самостійності. До них належать: метод повідомлення інформації та виконання; пояснювально-ілюстративний метод і репродуктивний; інструктивний та практичний методи; пояснювально-спонукальний і частково-пошуковий; спонукальний та пошуковий.

Особливого значення для формування творчої активності набувають три останні парні методи. Метод повідомлення інформації та виконання поєднує в собі інформаційне забезпечення учнів теоретичними поняттями з боку викладача і виконання практичних завдань суб'єктами навчання за зразком, на основі існуючого теоретичного досвіду. Він передбачає актуалізацію знань та втілення їх у практику без поглибленого осмислення. Пояснювально-ілюстративний метод полягає в узагальненні та розкритті викладачем сутності нових теоретичних понять на прикладах з метою усвідомленого засвоєння їх студентами. Репродуктивний метод (відтворюючий) націлений на встановлення учнями зв'язків між новими знаннями і попередніми, відтворення їх самостійно за зразком. Інструктивний та практичний методи проблемного навчання належать до активних методів і передбачають, з боку викладача, організацію практичної діяльності учня, а з боку учнів – опрацювання практичних навичок, умінь засобами усвідомленого аналізу теоретичної інформації, виконання завдань на комп'ютері, нескладних імпровізацій.

Пояснювально-спонукальний метод викладання націлений на активізацію самостійних дій учня. Він характеризується частковим поясненням матеріалу і постановкою проблеми для самостійного оволодіння майбутнім фахівцем новими теоретичними знаннями. Частково-пошуковий метод поєднує сприйняття інформації та індивідуальну творчу діяльність, у процесі якої учень самостійно долає всі (чи майже всі) етапи пізнавального шляху.

Завдяки спонукальному методові активізується розумова робота учня у напрямку пошуковості, дослідництва, творчості. Цей метод, націлений на стимуляцію мисленнєвої діяльності, дозволяє керувати пізнавальною самостійністю, спрямовувати її у творче русло.

Пошуковий метод характеризується тим, що учень сам розкриває сутність поняття, яке вивчається. Це означає, що він без допомоги викладача відкриває для себе нові знання, способи дій, оволодіває необхідними уміннями й навичками. Шляхом постановки та розв'язання проблем майбутній спеціаліст виходить на творчий рівень застосування знань.

Таким чином, адаптовані в галузі фахової підготовки майбутнього фахівця бінарні методи проблемного навчання забезпечують співпрацю викладача і учня у напрямку формування його творчої активності, здійснюють саморозвиток майбутнього фахівця, а задачний підхід цементує схему педагогічної технології формування творчої активності майбутнього фахівця, яка містить принципи, дидактичні умови, пошукові ситуації, задачний метод.

Перспектива задачного підходу у формуванні творчої активності майбутнього фахівця полягає у введенні засобів комп'ютерних технологій у процес підготовки майбутнього фахівця.

Результативність навчання кінець кінцем визначається тим, які саме завдання, в якій послідовності і якими способами вирішують вчителя і учні або студенти.

УДК 519.7

Борзенков Б.И., Бритик В.И., Струков Е.В.

СПОСОБ КОДИРОВАНИЯ ИНФОРМАЦИИ С ВЫСОКОЙ КРИПТОСТОЙКОСТЬЮ

Аннотация Разработан метод кодирования информации с возможностью реализации как с открытым так и с закрытым ключом с высокой криптостойкостью без потери точности геометрических особенностей с улучшенной возможностью сжатия относительно известных методов ZIP, ARJ.

Процесс передачи конфиденциальной информации с подвижных объектов является одной из актуальных задач. Основными недостатками алгоритмов, используемых в системах кодирования и сжатия информации, является сложность взаимного согласования основных требований к алгоритму (генерации и распределения ключей, распределение ключей и их накопление, цифровая подпись и генерация ключей). Уровень этих требований можно значительно понизить, используя следующий подход к формированию ключа/ключей. Между пользователями поставленная задача решается следующим образом.

Все пользователи имеют доступ к некоторым изображениям, хранимым на каком-то носителе.

Пользователь произвольным образом выбирает некоторое изображение, произвольного размера, например N×M, из множества K. Вероятность определения этого изображения криптоаналитиком составляет:

$$P_1 = 1/K$$

На выбранном изображении пользователь задаёт множество L произвольных S-угольных фигур, покрывающих изображение, которые являются начальными данными для формирования кода шифрования. Криптоаналитик может распознать координаты одной выбранной точки с вероятностью 1/(N×M), а вероятность распознавания криптоаналитиком всех точек составляет:

$$P_2 = \left(\frac{1}{NM}\right)^{LS}$$

Из произвольного числа фильтров (масок) F, выбирается один. Общее число фильтров зависит от размеров (P×Q) и может составить $511^{P\times Q}$ при условии, что каждое значение фильтра лежит в диапазоне $-255 \le m \le 255$. Вероятность определения выбранного фильтра криптоаналитиком при условии, что ему известен набор фильтров F, составляет:

$$P_3 = 1/F$$

С помощью выбранного фильтра на заданном множестве L произвольных S-угольных фигур, покрывающих изображение, выделяем характерные точки, полученные в результате свёртки точек локального фрагмента с маской (например, максимум отклика в выделенных фигурах или какая-либо другая особенность)

$$\max g_{i,j} = \max \{ \sum_{p=-P/2}^{+P/2} \sum_{p=-Q/2}^{+Q/2} m_{p,q}\ B(x_{i+p}, y_{j+q}) \}$$

S_{Li} S_{Li}

Очевидно, что при использовании жёсткого неравенства при поиске эта точка единственная. Данные L точек имеют 2L координат (L координат x и L координат y).

Формирование кода состоит в конкатенации полученных координат x и y. Количество всех возможных вариантов конкатенации составляет (2×L)!, а вероятность распознавания криптоаналитиком:

$$P_4 = 1/(2L)!$$

Общая вероятность вскрытия представленного кода криптоаналитиком составляет:

$$P_0 = \frac{1}{K}\cdot\left(\frac{1}{NM}\right)^{LS}\cdot\frac{1}{F}\cdot\frac{1}{(2L)!} = \frac{1}{K}\cdot\left(\frac{1}{NM}\right)^{LS}\cdot\frac{1}{511^{PQ}}\cdot\frac{1}{(2L)!}$$

Достоинства предлагаемого способа:

- цифровая подпись обеспечивается передачей обратного сообщения, закодированного изменённым кодом;

- генерация ключей сочетает в себе простоту запоминания и использует генератор «натурального» случайного процесса;

- накопление ключей в виде их составляющих, что исключает возможность считывания ключа;

- распределение ключей - прямой обмен ключами между пользователями информационной системы, позволяющих выполнить идентификацию личности, послав ответ с помощью личного ключа.

Каревик А.А., Котова М.А.

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА ОПЕРАТИВНОГО ДИАГНОСТИРОВАНИЯ ПАРАМЕТРОВ АНАЛОГОВЫХ ЭЛЕКТРОИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ В МЕСТАХ ИХ ЭКСПЛУАТАЦИИ

Повышение оперативности метрологического обслуживания средств измерения и контроля параметров вооружения и военной техники во многом определяется способами их калибровки (поверки), а также измерительными средствами, при помощи которых проводится эта калибровка.

В настоящее время во многих военных формированиях Украины в том числе и Внутренних войсках широко применяются аналоговые электроизмерительные приборы переменного тока (ЭИППТ), как автономные – установленные на аппаратуре, так и переносные комбинированные. Эти ЭИППТ контролируют параметры, как вооружения и военной техники, так и средств обеспечения безопасности жизнедеятельности личного состава. Поэтому от качественного и надежного функционирования этих средств измерения и контроля параметров во многом зависит выполнение поставленных задач подразделениями, так и достоверность полученной информации о их техническом состоянии.

Качественное состояние ЭИППТ определяется их калибровкой (поверкой) через определенные интервалы времени в специальных метрологических структурах. В тоже время очень важно провести оценку работоспособности этих средств измерения и контроля параметров непосредственно на объекте эксплуатации без демонтажа из аппаратуры. Проведение калибровки (поверки) ЭИППТ осуществляется при помощи целого комплекса средств измерения и контроля параметров с более высоким классом точности – эталонными средствами измерений (ЭСИ). Широко распространенным ЭСИ для данной группы приборов является переносной комплект поверочного оборудования, выпускаемый ОАО «Меридиан» г.Киев. В состав комплекта входят: источник калибровочного сигнала, две многозначные меры сопротивления и мультиметр – который составляет основу комплекта. Мультиметр AGILENT 34401A импортного производства, дорогостоящий, с явно завышенными точностными характеристиками. Меры сопротивления громоздки и не удобны в эксплуатации при расчете точностных характеристик калибруемых омметров, что снижает оперативность их метрологического обслуживания.

Авторами предложены новые методы проведения диагностики и калибровки ЭИППТ и омметров при помощи аппаратуры, реализующей новый принцип формирования тестового калибровочного сигнала с более упрощенным контролем его характеристик и применением ЭСИ отечественного производства.

При этом оперативность калибровки омметров достигается за счет применения регулируемой меры постоянного напряжения для проведения диагностирования измерителя омметра приведенная погрешность которого нормируется в процентах от длины шкалы, что существенно осложняет процедуру проведения их поверки (калибровки) классическими методами.

В докладе излагаются принципы формирования тестового калибровочного сигнала, принципы контроля его динамических и точностных характеристик, раскрываются способы оперативного проведения калибровок ЭИППТ и омметров. Авторы предлагают принципы построения малогабаритного, транспортируемого калибратора с метрологическими характеристиками обеспечивающими надежный контроль параметров широкого парка ЭИППТ.

Волков С.Г., Товстик А. В.

ОЦЕНКА СОЦИАЛЬНОЙ НАПРЯЖЕННОСТИ НА ПРЕДПРИЯТИИ

Трансформация социально-экономических отношений в Украине сопровождается негативными последствиями во всех сферах жизнедеятельности общества и требует механизмов поддержки уровня и качества жизни широких слоёв населения. Самые острые противоречия концентрируются в социально-трудовой сфере.

Негативные последствия конфликтов являются разрушительными в экономическом, социальном, социально-психологическом аспектах. Как свидетельствует общественная практика, наиболее продуктивным является выявление социальной напряженности на латентной стадии, что позволяет решить противоречия, лежащие в её основе, с наименьшими экономическими и социальными убытками.

Однако, в исследовательской практике чаще всего социальная напряжённость изучается в стадии её объективации, то есть перехода в открытый конфликт, когда уже можно фиксировать проявление недовольства на поведенческом уровне.

Предложенная методика имеет новизну, которая заключается в том, что её концепция учитывает специфику социальной трудовой сферы, социальная напряженность рассматривается как показатель состояния социально-трудовых отношений. Она рассчитана на изучение социальной напряженности в латентной (скрытой) стадии, до перехода её в открытый конфликт, социологический подход позволил разработать комплексный критерий оценки уровня социальной напряженности на разных её стадиях, с учётом объективных и субъективных показателей.

Методика исследования и анализа полученной социологической информации позволяет разработать механизмы предупреждения и конфликта, снятия социальной напряженности в ранних её стадиях.

Для измерения социальной напряженности было целесообразно использовать комплексный подход, при котором показатели должны фиксировать как социальное настроение, уровень сознания, так и социальное поведение, уровень социальной активности персонала с отстаиванием своих трудовых прав, формы, методы, которые они готовы использовать. Социологические методы исследования позволяют использовать разные типы шкал, которые дают представление об интенсивности социальной напряженности на той или иной стадии или фазе.

Общий индекс социальной напряженности на предприятии (в учреждении, организации) может быть рассчитан как среднее из полученных индексов по формуле:

$$\sum_{i=1}^{i=n} \frac{I_i}{n},$$

где I_i - индекс по отдельному вопросу. Сумма индексов:

$$\sum_{i=1}^{i=n} I_i,$$

где n - общее количество индексов

Зависимость уровня социальной напряженность на предприятии (в учреждении, организации) отвечают соответствующие значения индексов:

- фоновый : $0{,}5 < I \leq 1$
- низкий : $0 < I \leq 0{,}5$
- средний : $-0{,}5 < I \leq 0$
- высокий : $-1 < I \leq -0{,}5$

Для объяснения степени воздействия объективных и субъективных факторов на уровень социальной напряженности в коллективе используется двумерный анализ для поиска взаимосвязи между социальными явлениями, объяснения причин полученных данных. Выделяют три стадии анализа:

1) установление связи между признаками;

2) измерение связи между признаками;

3) объяснение связи между признаками.

Для установления связи между признаками используется статистический критерий «хи-квадрат». Установление величины этого коэффициента и его статистической значимости позволяет ответить на вопрос о наличии связи между исследуемыми признаками.

Если связь установлена, то происходит переход к следующей стадии анализа – измерению связи для ранговых порядковых при помощи коэффициентов ранговой корреляции Спирмена и Кенделла, а для номинальных шкал – коэффициентов ассоциации и контингенции (для дихотомических шкал) и коэффициентов соединённости (Пирсона и др. для шкал большой размерности).

Целью анализа является объяснение полученных в результате исследования фактов. Установление причинной зависимости между разными социальными и социально-психологическими явлениями открывает возможности социального прогнозирования и управления исследуемыми процессами.

Создание информационной системы оценки социальной напряженности на предприятии позволило автоматизировать расчёты, увеличить точность и скорость получения результатов для любого количества опрошенных респондентов.

Ліпатов А.О., Мазниченко Ю.А., Черкасова Ю.О.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ СИСТЕМ СУПУТНИКОВОГО ЗВ'ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЇ VSAT

На цей час існує величезна кількість технологій і технічних засобів зв'язку, які використовують різні радіочастотні діапазони. Їх вибір для потреб збройних сил обумовлюється жорсткими вимогами до військових систем зв'язку та необхідністю відповідати сучасним умовам проведення військових операцій.

Розвиток військових супутникових систем зв'язку (ВССЗ) пов'язаний зі зростанням кількості мобільних абонентів, впровадженням автоматизованих систем управління, а також збільшенням обсягів та різноманітності даних, що передаються по високошвидкісних каналах.

Основною перевагою ВССЗ, на думку представників військових відомств, є можливість управління військами в кризових ситуаціях без попереднього узгодження з комерційними операторами, висока завадозахищеність і функціональна пристосованість космічних апаратів (КА) для вирішення завдань в інтересах збройних сил у складній радіоелектронній обстановці.

Розгляд сучасних ВССЗ провідних країн світу показав, що їхня оптимальна архітектура може включати супутники зв'язку військового призначення та/або канали, орендовані в комерційних системах супутникового зв'язку.

За оцінками аналітиків, тенденція використання комерційних систем зв'язку в інтересах збройних сил неухильно розширюватиметься. Це пов'язано, передусім, з бюджетними обмеженнями, оскільки не кожна країна у змозі мати свою ВССЗ. Разом з тим розвиток технологій комерційних систем супутникового зв'язку відбувається значно швидше, ніж військових з їх специфічними вимогами.

Однією з технологій, які використовуються для створення мереж супутникового зв'язку, є технологія VSAT (Very Small Aperture Terminal). До основних переваг систем супутникового зв'язку VSAT відносяться: глобальний просторово-часовий рівень забезпечення зв'язку; малі габарити призначених для користувача терміналів та їхня відносно невисока вартість, у тому числі й експлуатаційна; можливість оперативної організації стаціонарного зв'язку з високою надійністю у важкодоступних (віддалених) районах.

В Україні використання VSAT технології реалізується дуже швидкими темпами. На цей час експлуатацією VSAT мереж займається близько десяти операторів. Оскільки Україна на

цей час не має свого КА можливо використати технічні засоби цих операторів для забезпечення супутниковим зв'язком Збройних Сил України.

Аналіз сучасного стану реалізації технології VSAT, дозволяє зробити наступні висновки: застосування технології VSAT є перспективним для Збройних Сил України з точки зору узгодження вимог до військових систем супутникового зв'язку зі стандартами НАТО, а також зниження вартості обладнання та можливості його використання після запуску національного супутника зв'язку.

Волков А.В., Мазниченко Ю.А., Бондаренко О.Е.

ИСПОЛЬЗОВАНИЕ МОБИЛЬНЫХ СЕТЕВЫХ МОДУЛЕЙ ДЛЯ ПОСТРОЕНИЯ ТЕРРИТОРИАЛЬНОЙ СЕТИ СВЯЗИ

Территориальные сети связи (ТСС) возникли как ответ на потребности создания сетей связи в определенных регионах при относительно малых затратах и в относительно сжатые сроки проведения этих работ на территориях, где до этого связные структуры неразвиты (отдаленные районы, горная местность и т.д.). Кроме того, при определенных применениях (военная связь, связь в чрезвычайных (кризисных) условиях и т.д.), обладая высокой скоростью развертывания и мобильностью установления связи, ТСС оказываются предпочтительными.

ТСС предназначена для обеспечения телекоммуникационными услугами стационарных и мобильных абонентов на локальной территории при сжатых сроках установления связи. Она состоит из зон связи, которые развертываются на базе мобильных сетевых модулей (МСМ) с ретрансляторами. Модуль размещён в контейнере с полным комплексом аппаратуры для развертывания линий связи (привязки) и обеспечения передачи речи и данных.

По целевому назначению ТСС могут играть как самостоятельную роль в виде автономных сетей абонентской связи, так и выполнять вспомогательные функции в других сетях, в виде организации и поддержки подсистемы соответствующей сети связи. При этом они выступают в качестве унифицированных системных элементов, организуемых автономно по своим правилам и процедурам и работающих по собственным алгоритмам. Модули связаны с остальными элементами сети через соответствующие интерфейсы.

ТСС обладают следующими положительными качествами:

- принципиально высокой маневренностью, т.е. возможностью быстрой организации связи и конфигурации зоны обслуживания на значительных территориях без "прокладки" кабельных линий;
- высокой живучестью сети связи, определяемой по существу живучестью ретранслятора, применением децентрализованного управления всеми средствами сети в реальном масштабе времени, самовосстановлением структуры сети и резервированием линий связи;
- обеспечением надежности и непрерывности связи, вследствие возможности оперативного создания требуемой напряжённости электромагнитного поля и концентрации всех энергетических ресурсов сети для обеспечения связи с любой точкой в зоне обслуживания;
- структурной интеграцией как внутри сети, так и самого объекта связи;
- возможностью создания системы в относительно короткие сроки.

Таким образом, использование МСМ позволяет:

- значительно сократить время развертывания и установления связи;
- оперативно осуществлять сопряжение ТСС с существующими сетями связи;
- обеспечить связью мобильные объекты, для которых, никакие другие виды кроме как стационарной и мобильной радиосвязи неприемлемы;
- нивелировать жесткие климатические и температурные ограничения, которые могут возникнуть в условиях их эксплуатации.

Создание ТСС должно включать в себя следующие направления:

- разработку модели топологической структуры сети;
- разработку номенклатуры аппаратных средств и технических требований к ним;
- способы и средства создания необходимой напряжённости электромагнитного поля для

обеспечения требуемой зоны обслуживания абонентов;

- разработку интерфейсов для сопряжения данной системы с другими системами связи.

При этом необходимо исходить из ограничений по номенклатуру аппаратных комплексов.

Для ТСС, как и для любой другой системы связи, ограничивающими факторами являются:

- зона обслуживания и физические ограничения на установку аппаратных комплексов в нужных точках (в основном определяются кривизной Земли и возможностью подъема антенны в заданной точке на заданную высоту). При этом значительную роль играет характер рельефа земной поверхности в зоне обслуживания. В результате в зоне обслуживания возникают "мертвые" пространства и т.д.;
- технические ограничения на параметры аппаратных комплексов;
- ограничения, обусловленные взаимными помехами от смежных систем;
- эксплуатационные ограничения, связанные с поддержанием системы в работоспособном состоянии.

Указанные проблемы частично уже рассматривались в литературе [1-4], где показано, что системы, образованные ретрансляторами на мачтах и на летно-подъемных средствах, адекватно отвечают современным тенденциям и динамике требований к военной и гражданской связи, вследствие характерной для них принципиальной возможности комплексного управления всеми ресурсами и физической конфигурацией системы.

Для обеспечения скрытности связи в ТСС используются: режим ППРЧ, применение широкополосных сигналов, маневр используемыми диапазонами частот, формой диаграммы направленности антенн, структурой сигнала и мощностью излучения по отдельным направлениям связи.

Одним с факторов, влияющих на концептуальные решения при проектировании ТСС, можно указать протекающий в настоящее время процесс внедрения в сети связи пакетных методов передачи. Это обусловлено следующими обстоятельствами:

- возможностью получения максимально гибкого управления ресурсами сети на базе внедрения рек. G.802.11 и G.802.16 МСЭ;
- широкими возможностями интеграции сети для различных видов передачи речи и данных;
- возможностью автоматизации управления сетью и ее структурой.

При этом системы с пакетной коммутацией ориентированы на организации сетей для обслуживания стационарных и мобильных абонентов, а для военных систем, кроме того на противодействие активному физическому и радиоэлектронному поражению.

Таким образом, ТСС потенциально отвечают требованиям, предъявляемым в настоящее время к мобильным системам связи со стороны военных и гражданских структур в соответствии с условиями их деятельности, а применение МСМ позволяет существенно сократить количество техники связи для развертывания сетей связи.

Список использованных источников

1. Флейшман Б.С., Рудеман С.Ю., Брусиловский П.М. Оптимизация систем к наступлению катастроф. – Калининград, 1978. –140 с.

2. Скородумов А. Автоматизированная система связи MSE // Зарубежное военное обозрение, №10, 1991. – С.24-29.

3. Дмитриев В.И. Линии и сети связи через средневысотные ретрансляторы. Часть 1. – СПб.: ВАС, 1993. – 324 с.

4. Макаров Л.П. Аэростатные радиолокационные комплексы США // Зарубежное военное обозрение, №9,1991. – С.36-40.

Люлін Д.О., Кайдаш І.Н., Васильєв А.Г., Петросян І.А.

УДОСКОНАЛЕННЯ СИСТЕМИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ І РЕМОНТУ ЗАСОБІВ ЗВ'ЯЗКУ І АВТОМАТИЗАЦІЇ ЗБРОЙНИХ СИЛ УКРАЇНИ

Взаємодія між органами штабу відбувається через відділи та представників управлінь з розмежуванням функцій та завдань.

Проведений аналіз свідчить, що систему технічного забезпечення засобів зв'язку і автоматизації необхідно будувати за наступними принципами:

- чітке розподілення функцій між органами управління системи матеріально-технічного забезпечення за об'ємом та переліком робіт, що виконуються;
- відповідність технічної оснастки, запасів матеріально-технічного майна та кваліфікації особового складу;
- централізоване управління силами та засобами технічного забезпечення і децентралізоване постачання військ (сил) в інтересах раціонального розподілу предметів постачання.

На прикладі організації Управління систем зв'язку і автоматизації Європейського командування ЗС США (ECJ6) (рисунок 3) можна побачити, що завдання матеріально-технічного забезпечення виконуються через відділ управління ресурсами (ECJ6-R).

Основні функції відділу управління ресурсами (ECJ6-R):

- ресурсне забезпечення;
- загальна організація та контроль за технічним забезпеченням системи зв'язку і автоматизації Європейського командування ЗС США;
- контроль за формуванням вимог до бюджету Європейського командування ЗС США в частині, що стосується матеріально-технічного забезпечення системи зв'язку та автоматизації;
- контроль використання фінансів ECJ6 (Сухопутні війська) при забезпеченні функціонування системи зв'язку і автоматизації;
- надання консультацій Європейському командуванню ЗС США (USEUCOM) щодо придбання ресурсів для функціонування системи зв'язку і автоматизації;
- управління контрактами;
- управління державною власністю ECJ6;
- контроль організації технічного обслуговування та ремонту засобів зв'язку і автоматизації.

Питання з організації та проведення технічного обслуговування, ремонту, транспортування, зберігання виконуються управлінням тилу і озброєнням J4.

Наведемо основні функції, що притаманні J4:

- облік майна;
- організація резерву запасних частин;
- забезпечення постачання;
- створення системи експлуатації (ТО, ремонт);
- поступове вилучення системи з експлуатації;
- утилізація.

З аналізу основних функцій відділу управління ресурсами можна зробити висновки, що управління ECJ6 при організації матеріально-технічного забезпечення виконує контролюючу функцію та надає пропозиції щодо планування організації матеріально-технічного забезпечення, безпосередньо організації та проведення технічного обслуговування, ремонту, транспортування, зберігання покладається на управління тилу і озброєння (управлінням логістики) J4.

Згідно програми розвитку Збройних Сил України на 2006-2011 рр за організацію системи матеріально-технічного забезпечення Збройних Сил відповідатиме **Об'єднання сил забезпечення** (J4), що було заплановано створити у 2006 р. на базі Командування сил підтримки.

Одним із основних завдань перспективної системи управління матеріально-технічним забезпеченням Збройних Сил є об'єднання функцій технічного забезпечення міжвидових угру-

повань військ (сил) та тилового забезпечення за територіальним принципом матеріально--технічного забезпечення з централізацією управління та укрупненням і спеціалізацією органів забезпечення.

Організація матеріально-технічним забезпеченням засобів зв'язку і автоматизації проводиться через Центри забезпечення ОВТ та ремонтні частини **Об'єднання сил забезпечення** (J4).

На даний час можливо сформувати основні напрямки вирішення проблемних питань:

1.Проведення наукових досліджень з розробки нормативної бази організації матеріально-технічного забезпечення ЗСУ.

2. Розробка нової редакції керівництва з технічного забезпечення зв'язку і автоматизації.

3. Уніфікація процедур планування та організації матеріально-технічного забезпечення.

4. Розробка загальної автоматизованої системи Кодифікації ОВТ ЗСУ (приклад Система Кодифікування НАТО STANAG-4177).

5. Розробка автоматизованої служби планування та організації матеріально-технічного забезпечення (прототип системи замовлень eBid служби NAMSA (Агентство НАТО з технічного обслуговування і постачання)).

6. Проведення робіт з автоматизації та моніторингу руху матеріально-технічних запасів бази (складу) зберігання з автоматичним оновленням баз даних.

7. Організація та проведення військових навчань з метою практичного відпрацювання взаємодії між органами управління J4 і J6.

Перехід Генерального штабу на структуру, наближену до стандартів НАТО, дозволить спростити механізм прийняття управлінських рішень, чітко визначити рівень відповідальності та повноважень посадових осіб, позбавити структурні підрозділи невластивих їм функцій та значно скоротити обсяги листування між органами військового управління.

Люлін Д.О., Єрохін В.Ф.

ПРОБЛЕМИ РОЗРОБКИ АЛГОРИТМІВ ДЕМОДУЛЯЦІЇ БАГАТОЧАСТОТНИХ ЦИФРОВИХ СИГНАЛІВ

Вимоги до мінімальної конфігурації нових модемів для магістральних і тактичних ліній зв'язку, які дозволяють гарантувати здатність до взаємодії у системах військового зв’язку містяться у стандартах НАТО STANAG 4481, 4197, 4285, 4415, та MIL.STD 188.110. Ці модеми призначені для використання в системах зв'язку “абонент – абонент”, у каналах, що комутируються, загального користування (PSN), а також у спеціалізованих системах зв'язку середньо- і короткохвильового діапазону та ін. Аналіз таких вимог надає можливість пошуку шляхів їх модернізазії та подальшого розвитку.

Для забезпечення ортогональности окремих піднісівних багаточастотного сигналу у відповідності із вище згаданими стандартами НАТО та стандартами серії MIL.STD 188.110 використовується частотне рознесення. Сигнал на виході модулятора складається з 39 ущільнених по частоті інформаційних каналів, кожний з яких модулюється за допомогою відносної чотирьохфазної модуляції (QDPSK). Наприклад, при технічній швидкості передачі 44,44 бод (тривалість інформаційної посилки τ =22,5 мс незалежно від швидкості даних на вході модему) частотний рознос між сусідніми піднісівними 39 тонового сигналу відповідно до MIL.STD 188.110 складає 56,25 Гц. Передача кожного сигнального елементу здійснюється за допомогою зміни фази частоти каналу відносно фази попереднього елементу.

Разом з тим, фазові співвідношення між окремими піднісівними є фіксованими. Очевидно, вибір цих співвідношень продиктований бажанням мінімізувати пік-фактор групового сигналу.

При формуванні OFDM-сигналів співвідношення між начальними фазами складових диктуються винятково прагненням до їхньої ортогоналізації на тривалостях інформаційних посилок.

В обох зазначених випадках детермінований взаємозв'язок між початковими фазами піднісівних може бути використаний для поліпшення якості їх оцінки на прийомі. Для цього слід формувати опорні піднісівні коливання на прийомі від одного джерела, початковою фа-

зою якого необхідно управляти за результатами спостережень у кожному з підканалів.

Для розв'язання завдання синтезу може бути застосована теорія оптимальної нелінійної фільтрації дискретно-безперервних Марковських процесів.

Додатковою перевагою пропонованого підходу є можливість подальшого застосування на вході демодулятора гребенчастого керованого фільтру, який забезпечить можливість адаптивного виключення з обробки підканалів, уражених перешкодами.

УДК 621.396

Люлін Д.О.

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПОБУДОВИ ПЕРСПЕКТИВНОЇ СИСТЕМИ ЗВ'ЯЗКУ ТА АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ВІЙСЬКАМИ В ЗБРОЙНИХ СИЛАХ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Керівництво військ зв'язку Збройних Сил Російської Федерації (ЗС РФ) підкреслює необхідність проведення повної модернізації існуючої системи зв'язку та автоматизованого управління військами (АУВ) в ЗС РФ. Розглядаються концептуальні підходи до побудови перспективної системи зв'язку та АУВ в ЗС РФ.

1. Шляхи модернізації системи зв'язку та АУВ, а саме: розвиток автоматизованої системи управління ЗС РФ, переведення системи зв'язку ЗС РФ на цифрові засоби передачі та комутації інформації, оснащення польових компонентів військ зв'язку ЗС РФ сучасними системами, комплексами, засобами зв'язку та автоматизації управління.

2. Основні напрямки розробок комплексів засобів автоматизації в інтересах ЗС РФ, а саме: розширення функціональних можливостей засобів автоматизації, забезпечення планування бойового застосування військ в реальному масштабі часу, вдосконалення архітектури автоматизованих систем управління для реалізації принципів розподіленої обробки даних, стандартизація та уніфікація інформаційного та програмного забезпечення, вдосконалення інтелектуальної складової комплексів засобів автоматизації.

3. Основні напрямки наукових досліджень та розробок засобів зв'язку в інтересах ЗС РФ, а саме: підвищення ефективності захисту від навмисних завад, підвищення пропускної здатності засобів зв'язку, створення автоматизованих радіоцентрів, уніфікація засобів радіозв'язку в рамках взаємодії радіоцентрів ЗС РФ та інших зацікавлених відомств, підвищення надійності експлуатаційних характеристик та комплексів зв'язку, зменшення ваги та габаритів засобів зв'язку, зменшення енергоспоживання засобів радіозв'язку, автоматизація процесів призначення та розподілу радіочастот.

4. Результати, які очікується досягнути в результаті модернізації системи управління військами (в частині, що стосується системи зв'язку та АУВ).

Таким чином, аналіз концептуальних підходів до побудови перспективної системи зв'язку та АУВ в ЗС РФ дозволяє зробити висновок, що в РФ проблемі переоснащення військ зв'язку перспективними комплексами засобів автоматизації та зв'язку приділятиметься значна увага як з точки зору науково-технічного, так і фінансового забезпечення.

Біленький А.В., **Білан А.М.**

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПОБУДОВИ ПЕРСПЕКТИВНОЇ СИСТЕМИ ЗВ'ЯЗКУ ТА АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ВІЙСЬКАМИ В ЗБРОЙНИХ СИЛАХ ПРОВІДНИХ КРАЇН СВІТУ

В сучасних умовах ефективне застосування авіації, як і інших родів військ, неможливе без розвиненої системи зв'язку та автоматизованого управління військами (АУВ).

На теперішній час в ЗС більшості провідних країн світу створено комплекси засобів автоматизації (КЗА) різного рівня управління для потреб авіаційної компоненти повітряних сил (ПС).

В доповіді розглядаються концептуальні підходи до побудови перспективної системи

зв’язку та АУВ в ПС ЗС провідних країн світу.

1. Шляхи модернізації системи зв’язку та АУВ, а саме: розвиток автоматизованих систем управління ПС ЗС, переведення систем зв’язку ПС ЗС на цифрові засоби передачі та комутації інформації, оснащення польових компонентів підрозділів військ зв’язку ПС ЗС сучасними системами, комплексами, засобами зв’язку та автоматизації управління.

2. Основні напрямки розробок комплексів засобів автоматизації в інтересах ПС ЗС, а саме: розширення функціональних можливостей засобів автоматизації, забезпечення планування бойового застосування військ в реальному масштабі часу, вдосконалення архітектури автоматизованих систем управління для реалізації принципів розподіленої обробки даних, стандартизація та уніфікація інформаційного та програмного забезпечення, вдосконалення інтелектуальної складової комплексів засобів автоматизації.

3. Основні напрямки наукових досліджень та розробок засобів зв’язку в інтересах ПС ЗС, а саме: підвищення ефективності захисту від навмисних завад, підвищення пропускної здатності засобів зв’язку, створення автоматизованих радіоцентрів, уніфікація засобів радіозв’язку в рамках взаємодії ПС ЗС з іншими підрозділами ЗС, підвищення надійності та експлуатаційних характеристик комплексів зв’язку, зменшення ваги та габаритів засобів зв’язку, зменшення їхнього енергоспоживання, автоматизація процесів призначення та розподілу радіочастот.

4. Результати, які очікується досягнути при модернізації системи управління військами (в частині, що стосується системи зв’язку та АУВ).

Таким чином, аналіз концептуальних підходів до побудови перспективної системи зв’язку та АУВ ПС ЗС провідних країн світу дозволяє зробити висновок, що проблемі переоснащення ПС ЗС перспективними КЗА та зв’язку приділятиметься значна увага як з точки зору науково-технічного, так і фінансового забезпечення.

Білан А.М., Біленький А.В., **Зеленко О.В.**

МЕТОДИКИ ПІДТРИМАННЯ НЕОБХІДНОЇ (ЗАДАНОЇ) ЯКОСТІ РОБОТИ ОПЕРАТОРА АСУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Діяльність операторів автоматизованих систем управління військового призначення (АСУ ВП) протікає в умовах, що висувають до них підвищенні вимоги. До таких умов відносяться [1]:

− наявність факторів ризику;
− ускладнення функцій оператора;
− сумісна діяльність, тобто виконання оператором двох і більше задач одночасно;
− переробка великих об’ємів і потоків інформації (перевантаження інформацією);
− неповнота інформації для прийняття рішення (сенсорний голод);
− виникнення екстремальних (аварійних) ситуацій;
− дефіцит часу на прийняття рішення та виконання необхідних дій;
− монотонність роботи в умовах очікування сигналу до дій;
− безперервність роботи та обмеження рухової системи людини-оператора на протязі тривалого часу та інші.

Особлива увага при цьому приділяється діяльності оператора в умовах потоку заявок, що потрапляють йому на обслуговування. Вибір цього виду операторської діяльності обумовлений наступними факторами:

− робота в умовах потоку заявок є найбільш розповсюдженим видом операторської діяльності в АСУ ВП;
− потік заявок і обумовлена ним черга на обслуговування здійснюють суттєвий вплив на психофізіологічний стан оператора (напруженість, втому) та показники якості його роботи.

Такими показниками є [2, 3]:

− вірогідність своєчасного прийняття рішення;

− вірогідність правильного (раціонального) прийняття рішення оператором;

− інтегральний критерій, що враховує вищевказані показники.

Потік заявок характеризується інтенсивністю їх надходження. За ступенем впливу інтенсивності вхідного потоку на перелічені показники, діяльність оператора АСУ ВП можна представити у вигляді чотирьох фаз його роботи [3]:

I. Мала інтенсивність вхідного потоку заявок, що надходять на обслуговування оператором. Даній фазі характерна відсутність напруженості у оператора, що призводить до зростання помилкових дій. Це пояснюється розслабленістю оператора в умовах очікування сигналів (монотонна діяльність), що може бути також наслідком пропуску заявок та несвоєчасного прийняття рішення.

II. При збільшенні темпу надходження інформації кількість помилкових дій оператора зменшується. Це досягається за рахунок мобілізації людини-оператора і концентрації уваги на виконанні своїх функцій.

III. При високій інтенсивності вхідного потоку показники якості діяльності оператора знову погіршуються, що обумовлено невідповідністю його перепускної спроможності інтенсивності надходження заявок. Це призводить до збільшення черги на обслуговування, в результаті чого виникає дефіцит часу на прийняття рішення, та різко зростає психофізіологічне навантаження людини-оператора.

IV. Подальше збільшення інтенсивності вхідного потоку заявок призводить до виникнення стресової ситуації та зриву діяльності оператора.

Розрахунок інтенсивності вхідних потоків інформації, що потрапляють на обслуговування операторів, здійснюється, як правило, тільки на етапі проектування інженерно-психологічної взаємодії людини з технічними засобами автоматизації за загальними (усередненими) даними, тобто на одному з етапів проектування АСУ ВП в цілому. Це не дає змоги більш ефективно використовувати індивідуальні якості людини-оператора на етапі функціонування системи шляхом врахування негативних впливів вхідного потоку на показники якості його роботи.

Тому, пошук оптимального темпу роботи оператора АСУ ВП на протязі всього часу прийняття ним участі в процесі управління, при якому забезпечується необхідна (задана) якість його роботи та висока перепускна спроможність, остається на сьогоднішній день *актуальною* задачею, яка може мати рішення завдяки застосуванню адаптаційних інформаційних моделей (АІМ) на автоматизованих робочих місцях операторів АСУ ВП.

Застосування АІМ передбачає здійснення адаптаційної зміни складу та об’єму тієї інформації, що відображається на засобах візуалізації, при тому як моменти та інтенсивність її надходження залишаються випадковими процесами.

В даній доповіді пропонується розглянути можливість підвищення якості роботи оператора АСУ ВП за рахунок адаптаційної зміни інтенсивності вхідного потоку заявок до його індивідуальних психофізіологічних якостей на протязі всього часу прийняття ним участі в процесі управління.

В такому випадку, в склад системи управління крім основного контуру управління „комплекс технічних засобів (КТЗ) – інформаційна модель (ІМ) – оператор” повинен бути включений контур управління ІМ. Адаптивне управління інформаційною моделлю буде здійснюватися наступним чином:

− оцінюється поточний стан якості операторської діяльності;

− при розбіжності поточної та необхідної (заданої) якості його роботи формується сигнал управління ІМ;

− блок вибору засобу управління ІМ перевіряє причину виникнення такої розбіжності, оцінює можливі наслідки та здійснює зміну структури, параметрів ІМ або інтенсивності вхідного потоку заявок до тих пір, поки якість роботи оператора не досягне потрібного рівня.

Основним та найбільш трудомістким елементом схеми адаптивного управління ІМ є блок оцінки поточної якості. Оцінка якості потребує еталонів для визначення точності, безпомилковості і своєчасності дій оператора та ускладнена в технічній реалізації. Тому для прогнозу-

вання якості доцільно використовувати модель операторської діяльності. Подібна модель буде специфічною для кожного оператора, тому умовно можна назвати таку модель „паспортом" оператора АСУ ВП.

„Паспортизація" оператора здійснюється шляхом спеціальних експериментів та статистичної обробки отриманих даних про вплив внутрішніх та зовнішніх факторів на якість діяльності конкретного оператора АСУ ВП. Важливою властивістю моделі („паспорта") оператора є те, що вона динамічна, тобто дозволяє в кожний поточний момент часу давати оцінку якості діяльності на основі об'єктивних даних про зовнішні та внутрішні фактори діяльності оператора.

Пропонується здійснювати добір та обробку статистичних даних про вплив інтенсивності вхідного потоку заявок, що потрапляють на обслуговування оператору АСУ ВП, на показники якості його роботи за допомогою наступних методик:

І. Методика збільшення ймовірності своєчасного доведення керуючих рішень об'єктам управління за рахунок створення динамічних пріоритетів вхідних заявок на обслуговування, сутність якої полягає в [4]:

− застосуванні не статичних, а динамічних пріоритетів для тих заявок, що надійшли на обслуговування оператору АСУ ВП та знаходяться у черзі;

− врахуванні прогнозованого часу їх очікування, обслуговування та доведення до об'єктів управління (ОУ) з метою недопущення перебування кожної із заявок у черзі більше деякого критичного значення.

Результатом застосування зазначеної методики є упорядкована черга заявок, що подаються на обслуговування оператору АСУ ВП, за максимальною вірогідністю своєчасного прийняття рішення з урахуванням пріоритетності їх обслуговування. Це дозволить збільшити ймовірність своєчасного прийняття рішення оператором АСУ ВП та ймовірність своєчасного доведення керуючих рішень ОУ за рахунок адаптаційної зміни часу очікування заявок у черзі до середнього часу обслуговування заявок оператором та перепускної спроможності телекомунікаційних напрямків.

ІІ. Методика підвищення якості роботи оператора АСУ ВП за рахунок адаптаційної зміни інтенсивності вхідного потоку заявок на обслуговування, сутність якої полягає в [5]:

− доборі та обробці даних про вплив інтенсивності вхідного потоку заявок на показники якості роботи конкретного оператора АСУ ВП на протязі деякого часу з метою побудови відповідної експериментальної залежності;

− знаходженні інтервалу, в межах якого забезпечується відповідність поточної та необхідної (заданої) якості роботи оператора;

− визначенні оптимального значення інтенсивності вхідного потоку, при якому забезпечується найвища якість роботи оператора.

Результати застосування зазначеної методики є вихідними даними для останньої із методик.

ІІІ. Методика підвищення якості роботи оператора за рахунок адаптації вхідного потоку заявок на обслуговування до поточного часу робочої зміни, сутність якої полягає в [6]:

− врахуванні негативних впливів інтенсивності вхідного потоку заявок на показники якості роботи оператора АСУ ВП на протязі всього часу прийняття ним участі в процесі управління, тобто на протязі всієї його робочої зміни, бойового чергування тощо;

− доборі та обробці відповідних даних з метою побудови функціональної залежності якості роботи оператора від темпу його роботи за весь час робочої зміни;

− здійсненні адаптаційної зміни інтенсивності вхідного потоку заявок, що потрапляють на обслуговування оператору, у відповідності з отриманими даними.

Результатом застосування третьої методики є сторінка „паспорта" конкретного оператора АСУ ВП, що має дані про залежність якості його роботи від інтенсивності вхідного потоку заявок, що потрапляють йому на обслуговування. Кількість таких даних буде залежати від особливостей організації робочої зміни (в 2 зміни, в 3 зміни і т. д.).

Комплексне застосування зазначених методик дозволить підтримувати необхідну (задану)

якість роботи конкретного оператора АСУ ВП на протязі всього часу прийняття ним участі в процесі управління.

Список використаних джерел

1. Забродин Ю.М., Ломов Б.Ф. Психологические проблемы деятельности в особых условиях. − М.: Наука, 1985. − 362 с.

2. Душков Б.А., Королев А.В., Смирнов Б.А. Основы инженерной психологии. – М.: Академический Проект; Екатеринбург: Деловая книга, 2002. – 576 с.

3. Зинченко В.П. Введение в эргономику. − М.: „Советское радио”, 1974. − 352 с.

4. Зеленко О.В., Колачов С.П. Методика збільшення ймовірності своєчасного доведення керуючих рішень об’єктам управління за рахунок створення динамічних пріоритетів вхідних заявок на обслуговування // Труди академії. – Випуск № 66. – К.: НАОУ, 2005. — С. 51 – 57.

5. Зеленко О.В., Колачов С.П. Методика підвищення якості роботи оператора АСУ військового призначення за рахунок адаптаційної зміни інтенсивності вхідного потоку заявок на обслуговування // Зб. наукових праць. – Випуск № 2. – К.: ВІТІ НТУУ „КПІ”, 2006. – С 34 – 42.

6. Зеленко О.В. Методика підвищення якості роботи оператора за рахунок адаптації вхідного потоку заявок на обслуговування до поточного часу робочої зміни // Труди академії. – Випуск № 1 (88). – К.: НАОУ, 2009. – С. 43 – 49.

Паламарчук С.А., Паламарчук Н.А., Гаврилюк О. Г.

ВИМОГИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ РУХОМИХ ЗАСОБІВ ЗВ’ЯЗКУ

До об’єктів інформаційної діяльності (стаціонарних або тих, що розміщуються в рухомих засобах зв’язку) Збройних Сил України на яких функціонують автоматизовані системи (АС) управління військами як в повсякденних так і в особливих умовах висувається ряд вимог пов’язаних з оперативністю прийняття рішення, прихованістю організації діяльності, достовірністю інформації на основі якої приймаються рішення, мобільності системи управління в цілому. Відповідно до вимог законодавства для забезпечення конфіденційності, доступності, цілісності та спостереженості інформації в кожній з таких АС повинна створюватися комплексна система захисту інформації (КСЗІ).

Створення КСЗІ регламентовано низкою нормативних документів системи технічного захисту інформації (в залежності від виду інформації – мовна, або така, що обробляється в АС). Як правило, КСЗІ складається з організаційних і інженерних заходів, технічних засобів захисту, які спрямовані на захист інформації за двома напрямами: це захист від витоку інформації з обмеженим доступом (ІзОД) технічними каналами – створюється комплекс технічного захисту інформації; захист інформації від несанкціонованого доступу (НСД) – відповідно комплекс засобів захисту (КЗЗ) від НСД. Також визначена обов’язкова послідовність робіт щодо створення КСЗІ в АС.

Відповідно, оброблення ІзОД на ОІД дозволяється лише після завершення робіт зі створення КСЗІ, проведення випробувань та оцінки рівня захищеності інформації на відповідність вимогам нормативних документів системи ТЗІ.

Виконання цих заходів є неможливим для рухомих засобів зв’язку через: відсутність постійної огороджувальної конструкції ОІД; необхідність зміни позицій та ін.

Перелічені питання щодо створення КСЗІ, повинні бути закладені на етапі проектування рухомого засобу зв’язку та відображені в технічному завданні (ТЗ) на його створення з послідуючою їх реалізацією у серійному виробі. Це дозволить значно спростити процедуру вводу та подальшої експлуатації АС.

При визначенні моделі загроз для рухомих засобів зв’язку основний акцент повинен спрямовуватися на захист від витоку інформації від випадкового прослуховування (акустичний

канал витоку) та захист інформації від витоку каналами побічних електромагнітних випромінювань та наведень (ПЕМВН).

Зазначене висуває жорсткі вимоги до зразків, що проектуються:

при підключенні проводів та кабелів до кунгу рухомих засобів виникають ПЕМВН, тому контрольована зона біля рухомого засобу зв'язку повинна бути не менше 5 м;

з'єднання повинні здійснюватися за допомогою оптоволоконних ліній, з повною відмовою від використання мідних кабелів, що дасть змогу не порушувати екранування кунгу рухомого засобу зв'язку;

жорстко регламентуються процедури доступності користувача до інформаційних ресурсів системи; автентифікації користувачів системи, підтвердження отримання інформації; достовірність отриманої інформації та ін.

Таким чином, для рухомих засобів зв'язку, що розробляються ці вимоги повинні бути детально описані в ТЗ на створення засобу. Також в ТЗ повинні бути визначені профілі захищеності для кожної підсистеми засобу зв'язку. Для засобів, що вже прийняті на озброєння, але в котрих не реалізовані заходи з захисту інформації необхідно провести аналіз особливостей їх реалізації. За результатами аналізу або відмовитися від їхнього подальшого використання або здійснити доопрацювання (модернізацію) з метою реалізації в них КСЗІ.

УДК 681.322

Овсяннiков В., Паламарчук Н.А., Паламарчук С.А.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФРАСТРУКТУР ВІДКРИТИХ КЛЮЧІВ PKI ТА SPKI В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

В даній доповіді пропонуються до розгляду особливості інфраструктур PKI та SPKI, й доцільність їх використання в процедурах ідентифікації, автентифікації та авторизації (надання повноважень) в інформаційно-телекомунікаційних системах Збройних Сил України

Політика безпеки, що розробляється для інформаційно-телекомунікаційних систем (ІТС) має організаційно-технологічну складову до якої відносяться процедури ідентифікації, автентифікації та авторизації. Дані процедури можливо реалізувати застосовуючи інфраструктури відкритих ключів *PKI* (*Public Key Infrastructure*) та *SPKI* (*Simple Public Key Infrastructure*).

Інфраструктура відкритих ключів *PKI* надає три основних сервіса безпеки: автентифікацію (суб'єкта, джерела даних), цілісність та конфіденційність. Ці сервіси дають можливість суб'єктам підтверджувати, що вони дійсно ті, за кого себе видають, отримувати гарантії, що дані не були змінені, і бути впевненими, що дані, відправлені іншому суб'єктові, будуть прочитані тільки ним.

Прикладом *сертифікату відкритого ключа* є формат X.509, який являє собою структурований двійковий запис у форматі абстрактної синтаксичної нотації *ASN.1*. Сертифікат містить елементи даних, що супроводжуються цифровим підписом *видавця сертифікату*. У сертифікаті є десять основних полів: шість обов'язкових і чотири додаткових. Зміст обов'язкових полів сертифікату може варіюватися. До них відносяться: серійний номер сертифікату; ідентифікатор алгоритму підпису; ім'я видавця; період дії; відкритий ключ суб'єкта; ім'я суб'єкта сертифікату.

Не зважаючи на перераховані сервіси безпеки інфраструктура відкритих ключів *PKI* не забезпечує авторизацію користувача та захист комп'ютерних мереж (є базисом сервісів безпеки, але не замінює інші засоби та методи захисту).

Для Збройних Сил України (ЗС України) не завжди принциповими є процедури ідентифікації та автентифікації, цього не можливо сказати про процедуру авторизації, яка підтверджує повноваження посадової особи. Проста інфраструктура відкритих ключів *SPKI* саме і надає можливості підтвердження повноважень особи та делегування даних повноважень іншим.

Сертифікати *SPKI* (сертифікати авторизації) мають зручну для сприйняття форму, містять

текст вільного формату, фотографію або іншу інформацію.

Сертифікати авторизації, за задумом авторів ідеї *SPKI*, повинні генеруватися будь-яким власником ключа, якому дозволено надавати або делегувати повноваження. Хоча *SPKI-сертифікати* мають багато загального з *сертифікатами відкритих ключів* X.509 (наприклад, поля ім'я видавця та період дії), синтаксис і семантика цих полів неоднакові. Крім того, кількість полів в сертифікатах цих двох типів не дозволяє їх еквівалентно відображати один на одного, а угоди про імена відрізняються повністю.

Робота над документами *простої інфраструктури відкритих ключів SPKI* завершена, проте на практиці в повному об'ємі не реалізована, попит на *SPKI-сертифікати* дуже невеликий.

Перевага вирішення безпеки на базі інфраструктури відкритих ключів заключається в створенні єдиної інфраструктури, котра здатна підтримувати багаточислені сервіси безпеки в складному великомасштабному середовищі з багатьма додатками.

Недоліки застосування інфраструктури відкритих ключів в ЗС України: необхідність взаємодії та функціональної сумісносності з зовнішніми користувачами, значні витрати на впровадження та підтримання функціонування інфраструктури відкритих ключів; структура сертифікату не повинна змінюватися, тому використання в даному вигляді не задовольняє ЗС України.

Таким чином, виникає необхідність в розробці стандартів відкритих ключів, які були б орієнтовані на потреби ЗС України (як для повсякденної діяльності так і під час ведення бойових дій).

Овсянніков В.В., Паламарчук Н.А.

ПОРЯДОК ВЗАЄМОДІЇ ПІДРОЗДІЛІВ УСТАНОВИ ПРИ ВВЕДЕННІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В ДІЮ

Перелік та послідовність робіт при введенні об'єктів інформаційної діяльності в дію визначається низкою законів та інших нормативно-правових актів з технічного захисту інформації. Вимоги даних документів є обов'язковими для всіх суб'єктів інформаційної діяльності, незалежно від їх організаційно-правової форми та форми власності, якщо обробляється інформація з обмеженим доступом.

З метою перекриття всіх можливих каналів витоку інформації система захисту інформації створюється за комплексним принципом. Тобто, мова йтиме про комплексну систему захисту інформації (КСЗІ). До складу КСЗІ входять заходи та засоби, які реалізують способи, методи та механізми захисту інформації від:

– витоку технічними каналами (акустичних, вібраційних, оптичних, побічних електромагнітних випромінювань і наведень, акустоелектричних тощо);

– несанкціонованих дій та несанкціонованого доступу до інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів;

– спеціального впливу на інформацію з метою порушення цілісності інформації або руйнування системи захисту.

У створенні КСЗІ беруть участь: установа, яка є замовником створення КСЗІ; виконавець робіт зі створення КСЗІ; виконавець проведення випробувань щодо створення КСЗІ; виконавець проведення державної експертизи КСЗІ (атестації).

Роботи по створенню КСЗІ на ОІД впорядковані у часі, взаємопов'язані та об'єднані в окремі етапи. Їх зміст, результати та терміни виконання визначаються в технічному завданні на створення КСЗІ. В загальному, до основних етапів створення КСЗІ відносяться: організаційні роботи; виконання передпроектних робіт; розроблення та впровадження заходів із захисту інформації; випробування та державна експертиза КСЗІ (атестація). Кожний етап роботи завершується відпрацюванням організаційно-технічних документів, згідно переліку, визначеному в технічному завданні на створення КСЗІ.

В залежності від призначення об'єкту інформаційної діяльності та складу КСЗІ можуть виконуватися різні види робіт та випробувань, і залучатися виконавці проведення робіт, які

мають відповідні ліцензії або дозвіл на провадження діяльності у сфері технічного захисту інформації. Крім того, випробування здійснюють виконавці (суб'єкти господарської діяльності), які мають необхідне технічне забезпечення для даного виду робіт.

По завершенню всіх визначених в технічному завданні етапів робіт та оформлення організаційно-технічних документів призначається виконавець державної експертизи комплексної системи захисту інформації на відповідність вимогам нормативних документів системи технічного захисту інформації. Після проведення якої надається атестат відповідності КСЗІ. Атестат відповідності комплексної системи захисту інформації вимогам нормативних документів системи технічного захисту інформації є підставою для введення об'єкта інформаційної діяльності в дію.

При розробленні та прийманні на озброєння нових інформаційно-телекомунікаційних систем висуваються ті ж вимоги, що і до об'єктів інформаційної діяльності.

Такий шлях достатньо затратний по термінам і тому не зовсім підходить для військових організацій.

Пропонується змінити порядок введення в дію об'єктів інформаційної діяльності, інформаційно-телекомунікаційних систем, а також розподіляти окремі завдання по створенню комплексної системи захисту інформації та введенню об'єктів інформаційної діяльності (інформаційно-телекомунікаційних систем) в дію між різними підрозділами установи.

Сторонні ж організації залучати лише для проведення випробувань та експертизи комплексної системи захисту інформації, при чому, для нових зразків – лише на етапі прийому на озброєння.

Місюра С.М., Радченко М. М.

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Розвиток комп'ютерних технологій призвів до масової практики автоматизованої обробки інформації в комп'ютерних мережах, в тому числі інформації персонального характеру. Виникла потреба додатково захисту інформаційних прав людини.

В Україні продовжується нормотворча робота у сфері правового регулювання конфіденційної інформації про особу. 1 червня 2010 року Верховна Рада України прийняла та 24 червня 2010 року Президент України підписав Закон України «Про захист персональних даних» (далі – Закон). Поява даного Закону обумовлено євроінтеграційними процесами України, зокрема, необхідністю виконання Україною вимог Євросоюзу, що містить спільна Угода за назвою «Матриця співробітництва». Однією з умов даного документа є зобов'язання України ратифікувати та запровадити конвенцію про захист персональних даних. Таким чином, слідом за провідними демократичними країнами, Україна врегулювала правовідносини в сфері правового захисту персональної інформації про особу, і це, безсумнівно, позитивний факт. Зроблено черговий крок, спрямований на забезпечення гарантій прав та свобод людини, що є одним з основних ознак правової держави.

Необхідність прийняття цього Закону уже давно гостро стояла в усіх учасників інформаційного обміну персональними даними (ПДн), що перш за все обумовлено тим, що стан нормативно-правової бази неефективно забезпечує захист прав людини щодо виконання положень статей 3, 32, 34 Конституції України стосовно ПДн.

Актуальність дослідження полягає в тому, що даний Закон вступає в силу з 1 січня наступного року. Тобто власники чи розпорядники бази ПДн, якими відповідно до Закону можуть бути підприємства, установи й організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, повинні до закінчення поточного року привести свою діяльність у відповідність до вимог положень Закону.

Для більш чіткого розуміння ситуації необхідно привести ряд інформаційних фактів:

1. Сучасні суспільні відносини характеризуються широким використанням персональних даних під час обігу інформації (соціального, фінансового, правоохоронного, науко-

во-технічного та ін. характеру), товарів, послуг і капіталів, що вимагає не тільки вільний рух інформації про особу, забезпечення її надійного захисту у відповідності до основних прав і свобод людини.

2. Зміцнення міжнародного соціального, економічного та науково-технічного співробітництва, розвиток інформаційних мереж, зростання транскордонних потоків персональних даних, з одного боку, та зусилля, що вживаються державною владою щодо розвитку демократичних процесів з іншого, визначають актуальність і об'єктивну необхідність захисту прав і свобод громадян України у цій сфері.

3. Конституцією України визначено зміст основних прав людини, у тому числі стаття 32 гарантує недоторканість особистого життя, зокрема – щодо збирання інформації про особу. Зазначене право повинно бути конкретизовано Законами встановленням технологій їх виконання. Бази персональних даних про своїх клієнтів сьогодні формує широке коло суб'єктів – фізичних та юридичних осіб: підприємства та торгівля, приватні лікарі, нотаріуси тощо. «Витік інформації» з цих баз даних наносить шкоду багатьом особам, що потребує термінового законодавчого врегулювання цих питань.

4. Україна спізнюється майже на чверть століття як з підписанням міжнародних угод, так й з впровадженням відповідних норм міжнародного прав. Лише у 2005 році підписано Конвенцію 1981 року Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», яку до цього часу не подано на ратифікацію. Європейське право охоплює майже два десятки загальноєвропейських конвенцій, директив та рекомендацій з питань захисту персональних даних, кожна країна ЄС видала свої базові нормативно-законодавчі акти, приймалися конкретні закони: щодо діяльності з персональними даними у медичній, статистичній, державній, журналістській, поліцейській та інших сферах. Аналогічні закони прийнято в багатьох країнах світу, у тому числі – в країнах СНД, зокрема в Росії.

5. Враховуючи необхідність застосування сучасних технологій при автоматизованій обробці інформації про особу, а також виникнення загрози для конкретної людини стосовно витоку та несанкціонованого використання персональних даних, багато європейських країн підписали Конвенцію про захист фізичних осіб під час автоматизованої обробки персональних даних (м. Страсбург, 28.01.1981 р.). Принципи, що містяться у Конвенції, уточнюються і розширюються в Директиві 95/46/ЕС Європейського парламенту і Ради від 24.10.1995 стосовно захисту фізичних осіб у питаннях обробки персональних даних і вільного обігу цих даних та в Директиві 97/66/ЕС Європейського парламенту і Ради від 15.12.1997 у стосовно обробки персональних даних і захисту приватності у телекомунікаційному секторі.

Отже з прийняттям Закону «Про захист персональних даних» можна сказати, що держава зробила перший, уже впевнений та відчутний крок до Євроінтеграції та розвитку свого інформаційного простору в частині одного із його найвагоміших сегментів «захисту прав людини під час автоматизації обробки її персональних даних». Але як кажуть, «важливо не зробити перший крок, а почати рух вперед». А для цього на виконання Закону необхідно виконати досить клопітку та важливу роботу, яка передбачає:

На державному рівні:

1. Створити (або надати повноваження вже створеному) орган контролю за станом захисту персональних даних. Крім того встановити чітку та прозору юридично-правову базу щодо забезпечення розгляду справ та відповідальності за несанкціонований доступ та використання персональних даних та/або порушень в частині забезпечення відповідного захисту.

2. Ввести в експлуатацію Державний реєстр баз персональних даних, прийняти регламент його функціонування та порядок реєстрації баз даних.

3. Розробити та запровадити загальнодержавну класифікацію відомостей, які відносяться до персональних даних та вимоги щодо їхнього захисту та автоматизованої обробки.

4. Розробити та запровадити вимоги щодо функціонального профілю захисту автоматизованих систем, в яких передбачається обробка та зберігання персональних даних.

На рівні окремих організацій та установ (державної та недержавної форм власності):

1. В рамках загальної класифікації інформації в ІТС визначити окремий клас «Персональні дані» та автоматизовані системи, в рамках яких вони обробляються.

2. Забезпечити відповідні юридично-правові та організаційно-розпорядчі заходи щодо визначення власника, розпорядника та основних вимог із захисту персональних даних, які надаються фізичними особами та/або накопичуються організаціями (угоди про використання персональних даних, реєстрація бази персональних даних в рамках єдиного Державного реєстру баз персональних даних).

3. Забезпечити захист персональних даних, які обробляються в автоматизованих системах, шляхом створення комплексної системи захисту інформації відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закону «Про захист персональних даних» в обсягах встановлених профілем захисту відповідними підзаконними актами Адміністрації Держспецзв'язку України.

Хлапонін Ю. І., Криховецький Г. Я., Криховецький В. Я.

АНАЛІЗ СИСТЕМ ЗАПОБІГАННЯ ВТОРГНЕННЯМ (IPS) ЗА 2008–2009 РОКИ

Системи запобігання вторгненням (атакам) (IPS), по суті, є розвитком систем виявлення атак (IDS). У той час як IDS лише детектували загрози в мережі й на хостах і посилали адміністраторові оповіщення різними способами, IPS зараз блокують атаки відразу в момент їхньої появи. Крім того, зараз системи IPS є частиною багатоэшелонованого захисту, оскільки інтегруються з іншими засобами захисту.

Ще п'ять років тому серед інших переважали мережні атаки, тобто атаки, що використовують слабкості протоколів мережного рівня, такі як ICMP-flooding і інші Dos/DDos-погрози. Сьогодні ж доводиться мати справу з атаками рівня додатків (7-го рівня моделі OSI). Це й поштові віруси, і мережні хробаки/трояны, і IP/P2P атаки, і Mail VoIP атаки, і spyware, і фішинг, і фармінг, проти яких більшість файрволів неспроможні.

В роботі приводиться звіт Magic Quadrant підготовлений Gartner, Inc. "Магічний квадрант'' - графічна репрезентація ринку за певний період часу. Відповідно до методики проводяться аналіз і порівняння виробників за певними критеріями, розробленим Gartner Inc. для ринку. Лідерами ринку IPS є компанії Cisco Systems, IBM, TippingPoint, McAfee, Sourcefire, Juniper Networks.

8 грудня 2009 року Cisco опублікувала свій щорічний звіт про інформаційну безпеку. У цьому документі підкреслюється вплив соціальних медіасистем (зокрема, соціальних мереж) на мережну безпеку й говориться про те, що найбільш привабливі можливості для кіберзлочинців створюють люди, а не технології.

В 2009 році соціальні мережі росли вибухоподібно. Один тільки Facebook протягом року потроїв активну користувальницьку базу, довівши її до 350 млн. чоловік. В 2010 році очікується подальше поширення соціальних мереж, тим більше, що багато організацій зрозуміли переваги цих мереж . При цьому соціальні мережі швидко стали полем діяльності кіберзлочинців, оскільки користувачі надто довіряють членам своїх мережних співтовариств і найчастіше не вживають необхідних заходів для боротьби зі шкідливими програмами й комп'ютерними вірусами.

В роботі наводяться основні атаки, які завдали найбільшої шкоди інтернет-користувачам в 2009 році: вірус-троян "Зевс'', "Промінь надії", хробак Koobface та інші.

Наведена перша десятка країн-джерел спаму.

У звіті Cisco по інформаційній безпеці за 2009 рік уперше приводиться матриця Cisco CROI, створена по методу знаменитої матриці Бостонской консалтингової групи "ріст/частка". CROI Matrix показує, які типи киберзлочинів будуть розвиватися, а які сходити нанівець протягом 2010 року. Ґрунтуючись на даних 2009 року, на 2010 рік матриця прогнозує масове поширення банківських троянів "Зевс'' і інших простих у використанні засобів, що використовують веб-уразливості. Програми типу Scareware, шпигунські програми, підміна посилань, стягнення передоплати й фармацевтичний спам залишаться привабливими

для кіберзлочинців. Атаки, потенціал яких поки неясний, такі, як використання соціальних мереж і хробаків типу Koobface, протягом 2010 року тільки почнуть свій хід по планеті.

Компанія IBM 20 липня 2010 року оголосила про випуск нового рішення в галузі захисту інформації - системи Intrusion Prevention System (IPS), яка об'єднує в єдиному пристрої засоби запобігання вторгнень із захистом даних і web-додатків. Це апаратний пристрій, що поставляється з встановленим та сконфігурованим програмним забезпеченням IBM, розширює можливості дослідницької групи IBM X-Force в галузі ефективного керування мережною безпекою при скороченні витрат.

Проведений в доповіді аналіз змін, які відбулися на ринку систем запобігання вторгнень (Intrusion Prevention System IPS) за 2008-2009 роки узагальнює відомості з різних джерел інформації. Наводяться атаки , які нанесли найбільшу шкоду інтернет-користувачам в 2009 році. Показано, які типи кіберзлочинів будуть розвиватися, а які перестануть існувати на протязі 2010 року. Доцільно використовувати напрацювання провідних світових виробників в автоматизованих системах військового призначення Збройних Сил України.

Панченко І.В., Тамаровський В.В.

ПРОЕКТУВАННЯ НЕЧІТКОГО РЕГУЛЯТОРА НА БАЗІ МІКРОКОНТРОЛЕРІВ AVR ФІРМИ ATMEL

В даний час спостерігається інтенсивний розвиток і практичне застосування нечітких систем для цілей управління і регулювання багатьох технічних об'єктів. Переваги нечіткої логіки, які явно виявляються в нечіткому управлінні, полягають в тому, що нечітка логіка дозволяє вдало представити мислення людини, а саме способи ухвалення рішень людиною, і способи моделювання складних об'єктів засобами природної мови.

Функціональна схема системи автоматичного управління на базі нечіткої логіки (системи управління з нечітким регулятором або системи фаззі-управління) складається з пристрою порівняння, нечіткого регулятора, об'єкту управління ОУ і ланцюга зворотного зв'язку.

Нечіткий регулятор (фаззі-регулятор) включає три основні блоки - блок фазіфікації, блок формування логічного рішення і блок дефазіфікації.

Нечіткий регулятор практично реалізується на мікропроцесорі (МІКРОЕОМ) і працює в дискретному режимі, тому система управління з нечітким регулятором містить пристрій сполучення мікроконтролер з об'єктом управління - аналого-цифровий перетворювач АЦП і цифро-аналоговий перетворювач ЦАП. АЦП квантує безперервну помилку.

ЦАП є фіксатор нульового порядку. Як наголошувалося, нечіткий регулятор містить блоки фаззіфікації, блок формування логічного рішення і блок дефаззіфікації, але часто АЦП, блоки оцінки першої і другої різниць від квантованої помилки і ЦАП також включають в схему нечіткого регулятора. Теорія нечіткого управління, а також питання по проектуванню і настройці нечітких регуляторів для систем автоматичного управління (за допомогою системи Matlab) розглянуті раніше.

Практично реалізувати нечіткий регулятор для систем автоматичного управління можна на сучасних мікроконтролерах різних фірм-виробників. У статті розглядається реалізація НР на мікроконтролерах AVR корпорації Atmel. Цей вибір проведений зважаючи на деякі переваги мікроконтролерів цієї корпоріциі.

Мікроконтролери сімейства AVR відрізняються високою швидкодією і низьким енергоспоживанням. Корпорація Atmel (США) добре відома як на світовому, так і на російському ринку електронних компонентів і є одним з визнаних світових лідерів в розробці і виробництві складних виробів сучасної мікроелектроніки - пристроїв незалежної пам'яті високої швидкодії і мінімального питомого енергоспоживання, мікроконтролерів загального призначення і мікросхем програмованої логіки.

Можна вважати, що AVR поступово стає ще одним індустріальним стандартом серед 8-розрядних мікроконтролерів загального призначення. В даний час у виробництві у Atmel

Corp. знаходяться три сімейства AVR:«tiny», «classic» і «mega».

Система команд мікроконтролерів AVR вельми розвинена і налічує в різних моделях від 90 до 133 різних інструкцій. Більшість команд займають тільки 1 елемент пам'яті (16 битий). Більшість команд виконуються за 1 такт Всю безліч команд мікроконтролерів AVR можна розбити на декілька груп:

- команди логічних операцій;
- команди арифметичних операцій і команди зрушення;
- команди операції з бітами;
- команди пересилки даних;
- команди передачі управління;
- команди управління системою.

Управління периферійними пристроями здійснюється через адресний простір даних. Для зручності існують «скорочені команди» IN/OUT.

Для розробки нечіткого регулятора вибраний мікроконтролер **ATmega8.**

Даний мікроконтролер відрізняється наявністю двох повноцінних портів з розрядністю 8 битий і наявністю аналогово-цифрового перетворювача, що дає можливість вимірювати такі параметри як напругу, струм, ємність що дозволяє розробити повноцінний регулятор на базі цього мікроконтролера. Так само **AtMega8** має порт UART для прийому і передачі даних. Порт для роботи по протоколу TWI(I2C). Повний опис мікроконтролера (Datasheet) можна знайти на офіційному сайті фірми Atmel [8]. На даний час у виробництві у Atmel Corp. знаходяться три сімейства AVR:«tiny», «classic» і «mega».

Для розробки програмної складової нечіткого регулятора використовується програма AVR Studio.

Існує спосіб, що використовує тільки внутрішні пристрої мікроконтролера. Для цього потрібно ініціалізувати вільний таймер-лічильник в режимі ШИМ. Також необхідно визначити частоту повтору циклів ШИМ, розрядність ШИМ перетворення і коефіцієнт заповнення прямокутного сигналу.

В цьому випадку буде потрібно введення ще одного додаткового коефіцієнта настройки нечіткого регулятора, оскільки в регістр управління ШИМ записується число від 0 до 1023 (для 10-ти розрядної роздільної здатності ШИМ), отже значення *m* потрібно перераховувати в діапазоні [0,1023]. Отримана послідовність виводиться на який-небудь вільний порт мікропроцесора. Оскільки на об'єкт управління необхідно подати безперервну напругу, що управляє, то буде потрібно введення в схему нечіткого регулятора RC-фільтру на операційному підсилювачі.

Такий спосіб приведе до деякого ускладнення програмного коду, але дозволить позбавитися від окремого ЦАП, що приведе до зменшення собівартості виробу і деякого зменшення його габаритних розмірів.

Таким чином, був реалізований нечіткий регулятор на мікроконтролері AtMega8. Принципова схема включає сам мікроконтролер, мікросхему ST232 (перетворювач ТТЛ - RS232), операційний підсилювач серії К140 і деякі додаткові елементи. Виведення інформації проводиться на COM-порт комп'ютера (є видимим програмою Hyperterminal) а також на LCD 2-х рядковий 16-ти символьний індикатор. Розрахункові дані які виводяться на засоби відображення інформації повністю відповідають даним роботи математичної моделі регулятора в Matlab.

При цьому Flash-пам'ять мікроконтролера заповнена на 75-80%, є можливість оптимізувати програмний код, ввести додаткові функції, а ввівши систему переривань можна перемикати мікроконтролер між обчисленнями на виконання який-небудь іншій функції.

УДК 355.4

Розанова Л. В.

ОСНОВНІ ШЛЯХИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ ВНУТРІШНІМИ ВІЙСЬКАМИ МВС УКРАЇНИ ПІД ЧАС ВИКОНАННЯ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ

Наведено важливість сучасного інформаційного забезпечення для прийняття рішень, напрямки наукових досліджень у цій галузі та основні практичні шляхи розвитку інформаційного забезпечення процесів управління внутрішніми військами МВС України під час виконання службово-бойових завдань.

Сьогодні масова комп'ютеризація, розвиток комунікацій, впровадження новітніх інформаційних технологій призвели до швидкого прогресу в сферах освіти, наукових досліджень, економіки, соціального життя. Завдяки цим процесам відбувається й розвиток військової справи, з'являються нові види озброєння, засновані на застосуванні інформаційних технологій, удосконалюються форми і способи застосування військ.

Впровадження сучасних інформаційних технологій у службово-бойову діяльність внутрішніх військ потребує знання доцільних напрямків розвитку системи інформаційного забезпечення процесів управління ними, що дозволить дійсно забезпечити органи управління необхідною інформацією для планування дій та управління військами під час службово-бойової діяльності, вмілого синтезу структур інформаційно-управляючих систем та обґрунтування складу інформаційних засобів пунктів управління і шляхів проходження інформації між ними.

Основною функцією системи інформаційного забезпечення процесів управління є надання управлінської інформації, яка задовольняє вимогам своєчасності, повноти даних для прийняття, доведення та виконання рішень. Це потребує: визначення складу і властивостей управлінської інформації; цілеспрямованого її формування; вибору технології її обробки та узагальнення, доведення до виконавців та використання з метою своєчасного і обґрунтованого прийняття рішень та контролю їх виконання.

Інформатизація органів управління на основі сучасних інформаційних технологій повинна забезпечувати:

– інтерактивний (діалоговий) режим рішення інформаційних, розрахункових задач і моделювання службово-бойової діяльності військ з широкими можливостями для органів управління;

– роботу органів управління в режимі маніпулювання даними;

– інформаційну підтримку рішень, які приймаються на всіх етапах проходження інформації на основі інтегрування бази даних, що передбачає єдину уніфіковану форму представлення, зберігання, пошуку, відображення, відновлення і захисту даних;

– безпаперовий процес оброблення службових документів;

– можливість колективної розробки і використання документів на основі комп'ютерних мереж;

– можливість адаптивної перебудови форм і способів представлення інформації в процесі рішення задач органами управління;

– можливість передачі візуальної і звукової інформації в єдиному потоці (технологія мультимедіа).

У свою чергу втілення комп'ютерних мереж у структуру системи управління військами дозволить успішно вирішити нижче наведені основні задачі:

– забезпечити безупинне отримання, оброблення, збереження та використання інформації, що відповідає поточним умовам обстановки;

– всебічне та узгоджене вироблення всіма посадовими особами штабів пропозицій до рішення командира (командувача) на організацію службово-бойового застосування військ;

– постійний обмін інформацією між різними рівнями системи управління військами та окремими ланками в межах одного рівня;

– прийняття рішення та своєчасну постановку завдань підлеглим;

– розроблення заходів з організації управління та взаємодії військ при виконанні завдань;

– рішення завдань всебічного забезпечення службово-бойового застосування військ по прийнятому рішенню;

– організацію постійного контролю за виконанням підлеглими завдань та вчасну корекцію їх рішень з боку командування при зміні умов обстановки;

– своєчасне інформування вищих рівнів управління про завдання, які виконуються підлеглими та їх стан.

Внесення змін у систему управління, завдяки яким при існуючих обмеженнях щодо складу сил та засобів вдається підвищити ефективність її застосування, потребує усунути відомі недоліки інформаційного забезпечення процесів управління військами.

Подолання цих недоліків вимагає активізації досліджень за такими напрямками як:

– розвиток теоретичних основ інформаційного забезпечення процесів управління внутрішніми військами;

– вдосконалення технологій математичного моделювання з метою забезпечення органів управління потрібною їм прогностичною інформацією для прийняття обґрунтованих рішень на дії в різноманітних ситуаціях службово-бойової діяльності;

– розроблення рекомендацій щодо створення необхідних інформаційно-управляючих систем та перевірки їх ефективності.

Для цього необхідно мати придатні показники оцінки ефективності засобів інформаційного забезпечення, моделі і алгоритми розрахунку значень цих показників, моделі і алгоритми формування прогностичної інформації для вирішення завдань управління, а також моделі і алгоритми формування структур системи управлення, що в сукупності складає *теоретичні основи* формування і оцінки ефективності засобів інформаційного забезпечення процесів управління військами.

Основний зміст *першого перспективного напрямку наукових досліджень* у цій галузі – оцінювання ефективності систем інформаційного забезпечення процесів управління військами.

Основний зміст *другого перспективного напрямку досліджень* – моделювання інформаційного забезпечення процесів управління військами.

Основний зміст *третього перспективного напрямку досліджень* – розробки математичних моделей формування даних, необхідних для інформаційного забезпечення процесів управління військами під час підготовки та виконання службово-бойових завдань.

Основний зміст *четвертого перспективного напрямку досліджень* – синтез структур інформаційно-управляючих систем відповідно до поточних умов підготовки та виконання службово-бойових завдань.

Застосування отриманих наукових результатів дозволить розробити та обґрунтувати *систему рекомендацій щодо інформаційного забезпечення процесів управління військами* при підготовці та під час виконання службово-бойових завдань:

– рекомендації щодо напрямків та шляхів розвитку системи інформаційного забезпечення процесів управління військами;

– щодо організації та здійснення інформаційного забезпечення процесів управління військами на етапі планування та у ході службово-бойових дій;

– щодо застосування розробленої методики синтезу структур інформаційних систем для обґрунтування оснащення та структури пунктів управління та шляхів проходження інформації між ними.

До основних практичних шляхів розвитку інформаційного забезпечення процесів управління внутрішніми військами МВС України на сучасному етапі слід віднести наступні:

– розробка інформаційно-правової бази, що стосується питань життєдіяльності, підтримання бойової готовності та бойового застосування внутрішніх військ – перш за все приведення у відповідність до нових умов керівних документів (наказів, бойових статутів, керівництв, настанов, посібників, тощо);

– вдосконалення форм бойових, плануючих, директивних, інформаційно-довідкових та інших документів;

– уточнення складу, джерел, форм та порядку проходження інформації, потрібної для управління військами при підготовці та у ході службово-бойових дій;

– вдосконалення та оптимізація структур та схем взаємозв'язку органів управління при підготовці та у ході службово-бойових дій, забезпечення їх синтезу та адаптації до змін обстановки і стану військ;

– систематизація та створення фонду офіційно прийнятих у внутрішніх військах моделей та задач, розробка програмних комплексів автоматизованих робочих місць посадових осіб з метою створення єдиної інформаційно-розрахункової системи, яка забезпечує розподілену обробку інформації при підготовці пропозицій для прийняття рішення та відпрацюванні необхідних для його впровадження документів;

– розвиток моделей та задач з питань всебічного забезпечення діяльності військ;

– розробка систем моніторингу як за станом військ, озброєння та військової техніки так і за станом потенційно небезпечних об'єктів та об'єктів, що знаходяться під охороною;

– розвиток програмного забезпечення та баз даних комплексу засобів автоматизації з метою створення автоматизованої системи управління у внутрішніх військах, яка буде використовуватися на всіх етапах – при чергуванні, при плануванні та в ході службово-бойових дій;

– поєднання процесів інформаційного забезпечення на етапі планування (підготовка інформації) та на етапі ведення дій (використання інформації, підготовленої на етапі планування);

– розробка сучасного багатоцільового автоматизованого пункту управління, розвиток агрегативно-модульного підходу до побудови таких пунктів управління;

– розробка концепції єдиного інформаційного поля для силових структур України та інформаційного забезпечення процесів управління ними;

– підготовка фахівців, здатних вміло, на сучасному рівні вирішувати всі ці питання у військах.

Безумовно, викладені положення можуть бути суттєво доповнені та деталізовані. Але аналіз показує, що завжди є ресурс ефективності дій військ, який можна реалізувати шляхом удосконалення параметрів існуючого інформаційного забезпечення процесів управління військами. В результаті, без суттєвих додаткових матеріальних витрат на озброєння та військову техніку, крім вартості програмно-технічних комплексів на базі мереж ПЕОМ, їх ефективність може бути суттєво підвищена.

Список використаних джерел

1. Дробаха Г. А. Використання інформаційних технологій та телекомунікаційних систем в процесі управління військами/ Г. А. Дробаха, С. І. Скрипнюк, Є. Г. Башкатов, Л. В. Розанова, С. О. Баєв. – Х.: Акад. ВВ МВС України, 2010. – 337 с.

2. Дробаха Г. А. Оперативне застосування та тактика дій внутрішніх військ. Частина 1. Основи службово-бойового застосування внутрішніх військ/ Г. А. Дробаха, О. В. Лавніченко. – Х.: Акад. ВВ МВС України, 2008. – 418 с.

3. Довбня В. В. Особливості інформаційного забезпечення у внутрішніх військах МВС України / В. В. Довбня// Честь і закон. – Х. : Акад. ВВ МВС України, 2009. – № 4. – С. 4-12.

УДК 355.42 : 623.618

Башкатов Є.Г.

ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ЩОДО ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ

Розглянуто перспективи щодо розроблення автоматизованої системи підтримки прийняття рішення командиром (начальником) УТрК, з'єднання, військової частини внутрішніх військ МВС України

Внутрішні війська МВС України є складною військо-організаційною системою (частини і підрозділи дислоковані на всій території України, кількість окремих складових сягає близько ста, різнорідність їх значна) і тому прийняття адекватного рішення на застосування сил та засобів військ при ускладненні оперативної обстановки, без використання сучасних математичних методів та засобів обчислювальної техніки, викликає значних труднощів. В даних умовах цей процес може зайняти значний час, а прийняте рішення виявитися "малоефективним".

Підвищення якості і скорочення часу прийняття рішень під час управління складними військовими системами неможливо без використання ефективних програмних і апаратних засобів, що забезпечують (підтримують) діяльність осіб бойових розрахунків командних пунктів (пунктів управління). Особливо гостро ця проблема відчувається при прийнятті рішень в системах управління військами, де дефіцит часу відчувається особливо сильно, а несвоєчасні чи помилкові рішення можуть мати негативні масштабні наслідки.

Суб'єктом усякого рішення є особа, що його приймає. Вона повинна бути компетентним фахівцем у своїй області і мати досвід діяльності в ній. Воно також, наділено необхідними повноваженнями і несе відповідальність за прийняте рішення.

Прийняття рішень відбувається в часі і тому являє собою процес, що починається з виникнення проблемної ситуації і закінчується вибором оптимального (найефективнішого) рішення – дії по усуненню проблемної ситуації (досягнення поставленої мети). Цей процес складається з послідовності етапів і процедур і спрямований на усунення проблемної ситуації.

У найпростіших випадках задачу прийняття рішення вирішує безпосередньо особа, яка приймає рішення без використання спеціальних процедур. Однак часто для цього вимагаються математичні моделі і методи, що допомагають особі, яка приймає рішення одержувати більш обґрунтовані рішення.

Досвід участі з'єднань внутрішніх військ у тих же збройних конфліктах на Північному Кавказі наочно показав, що для ефективного протистояння загрозам навіть локальної війни всі управлінські процеси повинні відбуватися набагато швидше. Не кажучи вже про можливе протистоянні більш серйозним загрозам, коли, щоб, наприклад, нейтралізувати вертолітний десант противника, у комбрига не буде покладених трьох годин на підготовку замислу на марш бригади.

А отже, нинішні управлінські алгоритми, розроблені в 1940-1950-і роки, вже не відповідають сучасним вимогам щодо прийняття рішення на виконання СБЗ. Що цілком природно, адже сьогодні вони вже не відповідають динаміки і характеру спеціальних операцій. Тому що змінилися і характер збройної боротьби, і системи озброєння, і можливості засобів зв'язку, управління і розвідки. Як же прискорити процес управління, зробивши його більш ефективним? Вихід тільки один: задіявши автоматику і замінивши паперову карту електронним аналогом, комп'ютеризувати процес управління військами і засобами ураження. Тому що, враховуючи швидкоплинність операцій в локальних конфліктах, сьогодні вже переносити обстановку з картки на картку, нарочним везти бойові розпорядження, збирати посадових осіб у макета місцевості. Ці та інші функції повинна взяти на себе АСУ.

УДК 378.147
Метешкин К.А.

ПЕРСОНАЛЬНЫЙ САЙТ НАУЧНО-ПЕДАГОГИЧЕСКОГО РАБОТНИКА

КАК ЭЛЕМЕНТ ТРАНСФЕРТА ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Розглянута практична реалізація персонального сайту науково-педагогічного працівника та демонструються його дидактичні властивості.

Системно-синергетический анализ структуры высшего образования Украины и состояния ее учебных заведений и учреждений показывает, что существует тенденция изменения порядка отношений между основными участниками образовательного процесса. Такие изменения обусловлены в первую очередь влиянием на образовательные процессы факторов информационно-коммуникационной революции. Все чаще научно-педагогические работники переносят личностно-учебные отношения в виртуальное пространство путем создания своих персональных сайтов и используют их для обучения студентов. Причем эти отношения официально нигде не фиксируются, а также не учитываются временные затраты научно-педагогических работников на их создание и реализацию. Вместе с тем, построение интеллектуальных сайтов с использованием методов искусственного интеллекта [1, 2], обеспечивает возможность осуществления трансферта образовательных технологий в случае, если сайт содержит модель профессиональных знаний преподавателя.

Принципы организации трансферта образовательных технологий на основе моделей профессиональных знаний преподавателей предложены в работе [3], где приведена схема мультиплексной технологии обучения одним преподавателем многих студентов из разных вузов, изучающих одну и ту же учебную дисциплину.

В настоящее время на основе требований к структуре и содержанию модели профессиональных знаний преподавателя разработан сайт, который находится на этапе заполнения и апробации отдельных его элементов.

Понятие трансферта образовательных технологий предполагает управление передачей технологий обучения из вуза в вузы или другие учебные заведения. Отличительные особенности образовательных технологий и технологий обучения приведены в работе [4]. Очевидно управление трансфертом технологий обучения необходимо осуществлять на основе механизмов специально созданных бирж под руководством Министерства образования и науки Украины.

Таким образом, при расширении сети персональных сайтов научно-педагогических работников возникнет принципиально новая ситуация в высшем образовании и кардинально изменится структура системы «Высшая школа Украины». На основе существующих тенденций использования научно-педагогическими работниками вузов и студентами Глобальной сети Интернет в учебных целях можно прогнозировать сокращение численного состава научно-педагогических работников и увеличение студентов, обучающихся на основе моделей профессиональных знаний преподавателей.

Список использованных источников

1. Метешкин К.А. Кибернетическая педагогика: теоретические основы управления образованием на базе интегрированного интеллекта: Монография/ К.А. Метешкин. – Х.: Междунар. Славянский ун-т, 2004. – 400 с.

2. Метешкин К.А. Кибернетическая педагогика: лингвистические технологии в системах с интегрированным интеллектом: Монография/ К.А. Метешкин. – Х.: Междунар. Славянский ун-т, 2006. – 238 с.

3. Шинкарук, В.Д. Системний підхід до дослідження інтеграційних процесів у вищій освіті України/ В.Д. Шинкарук, Х.В. Раковский, К.А. Метешкин// Вища школа. - №9, 2008. – С. 12 – 28.

4. Метешкин, К.А. Основы организации, функционирования и перспективы развития системы «Высшая школа Украины»: Монография / К.А.Метешкин. – Х.: Харьк. нац. акад. город. хоз-ва, 2010. – 308 с.

АБЕТКОВИЙ ПОКАЖЧИК АВТОРІВ ПУБЛІКАЦІЙ

Академія внутрішніх військ МВС України, м. Харків

Башкатов Є.Г.	- ад'юнкт	118
Горбов О.М.	- старший викладач-начальник служби	37
Горєлишев С.А.	- канд. техн. наук, доцент, ст. наук. співробітник	62
Захаров В.М.	- науковий співробітник	28
Земляна Н.В.	- студентка	12
Іохов О.Ю.	- канд. техн. наук, начальник кафедри	37,42,49, 52
Козлов В.Є.	- кандидат технічних наук, доцент, доцент кафедри	11,12
Краузе В.Г.	- студентка	12
Кузминич І.В.	- ад'юнкт	42
Малюк В.Г.	- канд. техн. наук, доцент, доцент кафедри	32
Новикова О.О.	- старший викладач кафедри	59
Орлов М.М.	- канд. військ. наук, доцент, провідний наук. співробітник	38
Побережний А.А.	- начальник НДЛ	62
Розанова Л. В.	- ад'юнкт, капітан	115
Романюк В.А.	- канд. техн. наук, доцент, доцент кафедри	17
Товма Л.Ф.	- старший викладач кафедри	12
Фик О.І.	- кандидат технічних наук, доцент кафедри	19
Хацаюк О.В.	- старший викладач кафедри	29

Військовий інститут телекомунікацій та інформатизації Національного технічного університету України "КПІ", м. Київ

Білан А.М.	- провідний наук. співробітник	103,104
Біленький А.В.	- начальник науково-дослідного відділу	103, 104
Бондаренко О.Е.	- ст. наук. співробітник НЦЗІ	99
Васильєв А.Г.	- ст. наук. співробітник НЦЗІ	101
Волков А.В.	- канд. техн. наук, ст. наук. співробітник	99
Гаврилюк О. Г.	- наук. співробітник НЦЗІ	107
Єрохін В.Ф.	- доктор техн. наук	102
Зеленко О.В.	- ст. наук. співробітник	104
Кайдаш І.Н.	- канд. техн. наук	101
Криховецький В. Я.	- канд. техн. наук	112
Криховецький Г. Я.	- канд. техн. наук	112
Лаврут О.О.	- канд. техн. наук, доцент, докторант	31
Ліпатов А.О.	- канд. техн. наук, професор	98
Люлін Д.О.	- нач. відділу НЦЗІ	101,102,103
Мазниченко Ю.А	- нач. відділу НЦЗІ	98,99
Місюра С.М.	- - ст. наук. співробітник	110
Овсянніков В.В.	- канд. техн. наук, пнс	108,109
Паламарчук С.А.	- викладач каф	107,108
Паламарчук Н.А.	- нач. лабораторії	107,108,109
Панченко І.В.	- провідний наук. співробітник	113
Петросян І.А.	- наук. співробітник	101
Радченко М. М.	- нач відділу	110
Руденко А.Л.	- ст. викладач – нач. зв'язку	52
Стрюк О.Ю.	- канд. техн. наук, доцент, докторант	31
Тамаровський В.В.	- ст. наук. співробітник	113
Хлапонін Ю. І.	- ст. наук. співробітник	112
Черкасова Ю.О.	- ст. наук. співробітник	98

Метрологічний центр військових еталонів Збройних Сил України

Котова М.А.		96

Національна академія Державної прикордонної служби України ім. Б. Хмельницького, м. Хмельницький

Хоптинський Р.П.	- ад'юнкт , кафедра зв'язку та інформатизації	69

Національний технічний університет «ХПІ», м. Харків

Дорохін І.С.	- аспірант	40
Поштаренко В.М.	- канд. техн. наук, доцент	40

Національний університет «Юридична академія України ім. Я. Мудрого», м. Харків

Зенін А.П.	- канд. техн. наук, доцент, доцент кафедри	85
Карасюк В.В.	- канд. техн. наук, доцент кафедри	22
Карманний Є.В.	- канд. техн. наук, доцент, доцент кафедри	84
Карташов І.М.	- канд. військ. наук, доцент, доцент кафедри	86
Ковжога С.О.	- канд. хім. наук, доцент, завідувач кафедри	86
Лазутський А.Ф.	- канд. військ. наук, доцент, доцент кафедри	85
Малько О.Д.	- канд. військ. наук, доцент, доцент кафедри	86
Молодцов В.А.	- канд. військ. наук, доцент, доцент кафедри	85
Писарєв А.В.	- канд. військ. наук, доцент, доцент кафедри	84
Полєжаєв А.М.	- канд. техн. наук, доцент, доцент кафедри	86
Тузіков С.А.	- канд. техн. наук, ст. наук. співробітник, доцент кафедри	84
Чудновський І.Т.	- ст. викладач кафедри	85
Яценко В.В.	- ст. викладач кафедри	84

Національний університет цивільного захисту України, м. Харків

Дерев'янко О.А.	- канд. техн. наук, доцент, начальник кафедри	53
Закора А.В.	- канд. техн. наук, доцент, ст. викладач кафедри	53,55
Селєєнко Є.Є.	- ст. викладач кафедри	53,55
Фещенко А.Б.	- канд. техн. наук, доцент, ст. викладач кафедри	53,55

Одеська філія Європейського університету

Сергєєв О.Ю.	- канд. техн. наук, доцент, завідувач кафедри	57

Українська державна академія залізничного транспорту, м. Харків

Альошин Г.В.	- доктор техн. наук, професор кафедри	20,26
Бойко Д. О.	- аспірант	26
Волков А.С.	- аспірант	34
Зинчук Ю.А.	- аспірант	35
Лысечко В.П.	- канд. техн. наук, доцент	4
Приходько С.І.	- докт. техн. наук, професор, завідуючий кафедрою	34,71
Сербин А.В.	- аспірант	20
Сопронюк І.І.	- аспірант	4
Цимбал Г.С.	- аспірант	71

Харківська національна академія міського господарства

Левковська А.П.	- студентка	8
Метешкін К.А.	- доктор техн. наук, доцент, професор кафедри	8,119

Харківський гуманітарно-педагогічний інститут

Русскін В.М.	- канд. техн. наук, ст. наук. співробітник, В.О. завідувача кафедри	91,93

Харківський державний технічний університет будівництва та архітектури

Бережний Д.О.	- слухач магістратури	13
Білоус І.О.	- слухач магістратури	14
Григор'єва Д.О.	- слухач магістратури	16
Іщенко В.М.	- слухач магістратури	17
Щербак Г.В.	- канд. техн. наук, доцент, доцент кафедри	13,14,16,17

Харківський національний аерокосмічний університет «ХАІ»

Товстик А.В.	- студент	97

Харківський національний університет внутрішніх справ

Колісник Т.П.	- канд. пед. наук, доцент кафедри	83
Сезонова І.К.	- канд. техн. наук, доцент, професор кафедри	81
Турута О.П.	- викладач кафедри	79

Харківський національний університет радіоелектроніки

Авраменко В.П.,	- доктор техн. наук, професор, професор кафедри	72,74
Белокурський Ю.П.	- ст. викладач кафедри	24
Борзенков Б.І.	- канд. техн. наук, профессор, профессор кафедри	94
Бритік В.І.	- канд. техн. наук, доцент, доцент кафедри	94
Євтухова О.Ю.	- студентка	4
Кобзев В.Г.	- канд. техн. наук, доцент кафедри	22
Коваленко О.В.	- асистент кафедри	28
Козлов Ю. В.	- асистент кафедри	9,11
Котух Є.В.	- аспирант	46
Лишенко В.В.	- провідний інженер	24
Мартиненко Т.М.	- студентка	6
Москалец М.В.	- канд. техн. наук, доцент кафедри	28
Парамонов А.К.	- здобувач	72,74
Руженцев І.В.	- доктор техн. наук, професор, завідуючий кафедрою	25
Семенов М. І.	- студент	58
Струков Є.В.	- аспірант	94
Федцова А.С.	- студентка	25
Халимов Г.З.	- канд. техн. наук, доцент кафедри	43,46,49
Чибирев А.Д.	- аспірант	72,74
Широковська А.С.	- студентка	25
Щербіна О.О.	- канд. техн. наук, доцент, доцент кафедри	24,58

Харківський соціально-економічний інститут

Волков С.Г.	- канд. техн. наук, профессор, ректор	97
Каревик А.А.	- канд. техн. наук, проректор	96

Харківський університет Повітряних Сил ім. І. Кожедуба

Алексєєв С.В.	- канд. техн. наук, ст. наук. співробітник, ст. наук. співробітник НДЛ, підполковник	76,87
Бердник П.Г.	- викладач	68
Дробот О.А.	- ст. наук. співробітник	72
Дрозд .О.А.	- страший викладач	72

Дуденко С.В.	- канд. техн. наук., ст. наук. співробітник	89
Калачова В.В.	- канд. техн. наук, ст. наук. співробітник, доцент, старший науковий співробітник НДЛ	76
Колмиков М.М.	- канд. техн. наук., ст. наук. співробітник	89
Кузнецов А.А	- начальник каф., доктор технічних наук, професор	63,65
Павленко М.А	- старший викладач	68
Першин О.В.	- старший інженер	68
Рубан І.В.	- доктор техн. наук, професор, начальник кафедри, полковник	78
Руденко В.М.	- викладач	68
Трублін О.А.	- науковий співробітник НДЛ, майор	76
Усачов О.М.	- старший викладач	72
Шитова О.В.	- викладач кафедри	78
Харківський національний університет ім.В.Н.Каразіна		
Исаев С.А.	- аспирант	63
Сорока Л.С.	- д.т.н., професор, декан факультета	63
Харківський національний економічний університет		
Король О.Г.	- викладач	65
Кировоградський національний технічний університет		
Босько В.В.	- викладач	65

Науково-практична конференція

“ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ”

Збірник тез доповідей

Відповідальний за випуск *Д.В. Павлов*
Упорядники *Н.М. Брик, В.Є. Козлов*

Підписано до друку 14.03.2011 р. Формат паперу 60х84/16. Різограф.
Папір офсетний. Ум. друк. арк. 6,98. Облік.-вид. арк. 9,47. Тираж 50 прим. Зам. №17

Редакційно-видавничий відділ Академії внутрішніх військ МВС України
Свідоцтво про державну реєстрацію ДК №2799 від. 22.03.07 р.
Друкарня Академії внутрішніх військ МВС України
61001, м. Харків, пл. Повстання, 3

ГОЛОВНЕ УПРАВЛІННЯ ВНУТРІШНІХ ВІЙСЬК МВС УКРАЇНИ

АКАДЕМІЯ ВНУТРІШНІХ ВІЙСЬК МВС УКРАЇНИ

«Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку»

Збірник тез доповідей науково-практичної конференції

17-18 березня 2011 року

м. Харків

Оргкомітет конференції

Голова оргкомітету – заступник начальника Академії внутрішніх військ МВС України з наукової роботи полковник **Морозов О.О.**, доктор технічних наук, професор.

Заступники голови оргкомітету:
начальник науково-організаційного відділу Академії внутрішніх військ МВС України майор **Павлов Д.В.**, кандидат технічних наук, старший науковий співробітник (739-26-68, 4-68, 8-067-915-55-88);
начальник кафедри інформатики та прикладних інформаційних технологій Академії внутрішніх військ МВС України майор **Іохов О.Ю.**, кандидат технічних наук (739-26-89, 4-89).

Відповідальний секретар оргкомітету – науковий співробітник науково-організаційного відділу Академії внутрішніх військ МВС України **Захаров В.М.** (739-26-68, 4-68, 8-050-140-21-61).

Члени оргкомітету:
доцент кафедри інформатики та прикладних інформаційних технологій Академії внутрішніх військ МВС України **Козлов В.Є.**, кандидат технічних наук, доцент (739-26-89, 4-89);
старший викладач кафедри інформатики та прикладних інформаційних технологій Академії внутрішніх військ МВС України **Новікова О.О.** (739-26-89, 4-89).

Адреса оргкомітету: 61001, м. Харків, площа Повстання, 3, Академія внутрішніх військ МВС України, науково-організаційний відділ.
Телефон: 8-057-739-26-68, електронна адреса: kafedra15@list.ru.

Тези надруковані в послідовності їх надходження до оргкомітету конференції.

Тези доповідей опубліковано в авторській редакції, мовою оригіналу. Відповідальність за фактичні помилки, достовірність інформації та точність викладених фактів несуть автори.