

Интелигентна система за обмен на съобщения при КПУ за УК

Златогор Минчев

Резюме: Компютърно подпомаганите учения за управление при кризи (КПУ за УК) са мощен и удобен инструмент за обучение, както в цивилния така и във военния сектор на сигурността, тъй като осигуряват гъвкава и икономически ефективна среда за обучение.

През последните три години (2004-2007) в България беше създаден Център на компетентност по Операционен Анализ (ЦК-ОА) и Съвместен център за обучение симулации и анализ (СЦОСА), които работят в сферата на управлението при кризи и създаването на изследователска среда за провеждане и изследване на сектора за сигурност чрез компютърно подпомагани учения.

В доклада ще бъде представена интелигентна система за обмен на съобщения при КПУ за УК, разработена в резултат от натрупания в България опит в тази област и базирана на обмяна на e-mail съобщения (архивирани в реляционна БД и достъпни през web портал) – решение, което позволява провеждането на географски разпределени КПУ за УК. В допълнение, към системата за обмен на съобщения е добавена и възможност за автоматично гласово възпроизвеждане на получените съобщения, както и географска информация за мястото на събитията, съдържащи се в съобщенията.

Ключови думи: моделиране, симулации, компютърно подпомагани учения, система за обмен на съобщения, управление при кризи

1. Въведение

Компютърно подпомаганите учения за управление при кризи (КПУ за УК) са мощен и удобен инструмент за обучение, както на военни, така и на цивилни представители на сектора за сигурност, тъй като позволяват обучение с висока гъвкавост и ниска себестойност. Най-често КПУ се прилагат в ситуации свързани с УК, защото пресъздаването на подобни ситуации в реалността е сложно, икономически неефективно и дори понякога невъзможно [10], [14], [11].

Провеждането на КПУ, като цяло, представлява симулация (имитация) на реална ситуация (или неин опростен модел), като самата симулация може да бъде категоризирана като: „жива”, „виртуална” и „конструктивна” [2], [9].

От своя страна, „живата-” симулация включва реални хора, работещи с реални системи на реален терен, а „виртуалната-” симулация - реални хора, работещи със симулирани системи в симулирана среда. Провеждането на „конструктивна-” симулация включва участието на симулирани хора работещи върху симулирани системи в симулирана среда.

Като правило извършването на „жива-” и „виртуална-” симулация, изисква активност от участващите хора (участниците) по време на самия процес, като резултата (изхода) от симулацията зависи от участниците. При конструктивната симулация участниците подават входни данни, но не могат да влияят на изходните резултати и въздействието върху обучаемите е индиректно [9], [23].

Използването на тези три категории симулация, обаче, не е пълно и създава трудности при класификацията на симулациите изобщо, тъй като не разглежда случая с участието на: симулирани участници, работещи в реална среда, т.е. възможността за участие на работи в сектора за УК [9], [7].

Едно по-опростено класифициране на симулацията като такава от компютърна гледна точка е: „отворена -” (симулация при която обучаемите участници могат да влияят на хода на събитията по време на нейното времетраене) и „затворена -” (симулация при която обучаемите участници не могат да влияят на хода на събитията по време на нейното времетраене), т.е. на базата на начина по-който тя се изпълнява- със или без интеракция от участниците [13].

От изложеното до тук става ясно, че най-пълен ефект при обучението може да бъде постигнат с използването и на трите категории симулация („жива-”, „виртуална-” и „конструктивна-”), като по този начин се осигури и обща оперативна картина за действие в разпределена среда за работа [23].

В следващата точка ще бъде представена обща програмна схема за провеждане на КПУ за УК, разработена и тествана в Република България, чрез поредица от изследователски проекти с национално, европейско и НАТО- финансиране в периода (2004-2007), на базата на

която е разработена и система за хибридна симулация в КПУ за УК, представляваща комбинация от трите гореизложени типа („жива-“, „виртуална-“ и „конструктивна-“).

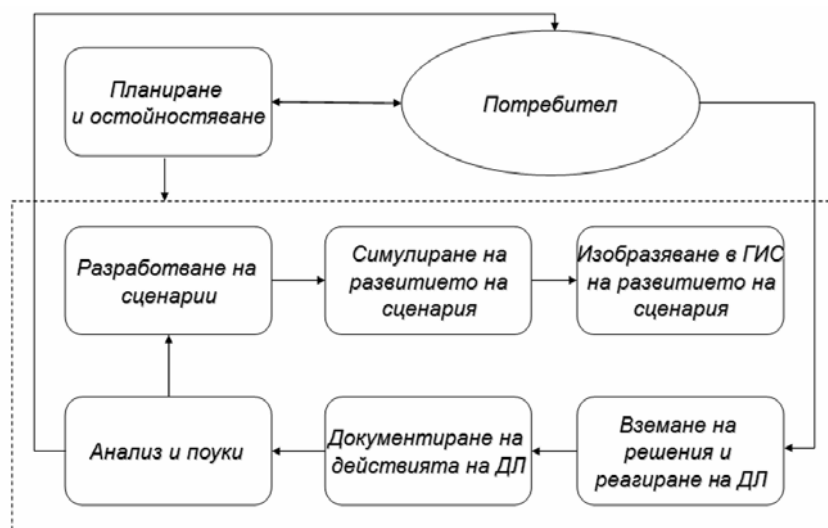
2. Обща програмна схема на КПУ за УК

Прилагането на КПУ за УК изисква разработването на обща програмна схема за това. С тази цел през 2004г., у нас, започва изграждането на Център на компетентност по операционен анализ – ЦК-ОА (НАТО SfP 981149) и неговата изследователска среда за работа – Съвместен център за обучение, симулации и анализ (СЦОСА), ситуиран в Института за паралелна обработка на информацията - БАН.

ЦК-ОА е основан през 2005 година в рамките на проекта SfP 981149 project “Operations Research Support to Force and Operations Planning in the New Security Environment” на програмата на НАТО “Наука за мир”. Участници в проекта са: Институт по паралелна обработка на информацията – БАН (ИПОИ-БАН), ВА “Г.С. Раковски” и Институт по математика и информатика – БАН [18].

Основната цел на ЦК-ОА е да създаде човешки и технологичен капацитет в областта на моделирането и симулациите с фокус КПУ за УК.

На базата на натрупаните знания и опит в ЦК-ОА и СЦОСА, в Република България, беше разработена и обща програмна схема на КПУ за УК [12]:



Фиг.1. Обща програмна схема на КПУ за УК

Идеята на програмната схема на КПУ за УК от Фиг.1 е чрез използване и минимална доработка на съществуващи софтуерни решения за обмен, визуализация, архивиране и анализ на информация да бъде извършено своеобразно пресъздаване на виртуална реалност за дадено критично събитие (терористична атака, природно бедствие, социална аномалия), която да послужи на обучаемите, от сектора за сигурност, в тяхната подготовка за УК чрез КПУ.

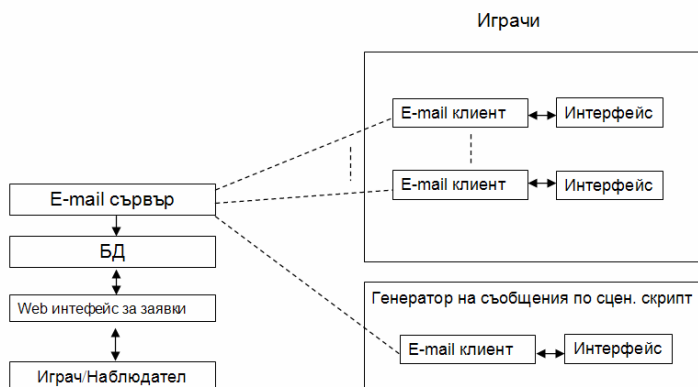
Детайлно описание на общата програмна схема на КПУ за УК е представено в [12] като тук ще отбележим, че след практическото провеждане на КПУ за УК от ЦК-ОА и СЦОСА [3] беше проектирана и настоящата интелигентна система за обмен на съобщения интегрираща общата идея от Фиг.1 и позволяваща икономически ефективно провеждане на КПУ.

В следващата точка ще бъде представена и обща архитектура на интелигентна система за обмен на съобщения при КПУ за УК.

3. Обща архитектура на интелигентна система за обмен на съобщения

Общата архитектура на интелигентната система за обмен на съобщения се основава на използването на компютърни станции, върху които чрез специализиран софтуер за обмяна на e-mail съобщения в LAN/WAN мрежа (в локални или разпределени КПУ) в съответствие с

предварително подготвен скрипт (поредица от съобщения) на сценария за КПУ. Блок-диаграма на общата архитектура на интелигентна система за обмен на съобщения е показан на Фиг.2:



Фиг.2. Обща архитектура на интелигентна система за обмен на съобщения

Както става ясно от архитектурата на Фиг.2. използвана е „клиент-сървър” архитектура за обмяна на съобщения, разширена с потребителски интерфейс и машинен интелект, към които е добавена база данни (БД), позволяваща анализ на КПУ по време на (или след) самото му провеждане.

Идеята е да се създаде предварителен скрипт (списък) от познати съобщения по сценария, който да се използва от генератора на съобщения по сценариен скрипт и обучаемите играчи. Това решение позволява участието както на реални, така и на виртуални играчи, участващи в КПУ за УК по определени, предварително, фиксирани или предвидимо изменящи се правила с използването на статичен или динамичен скрипт на сценария за КПУ [3].

4. Език и формат на съобщенията

В тази точка ще бъдат разгледани някои детайли касаещи езика и формата на съобщенията в интелигентната система за обмен на съобщения от Фиг.2.

Тук ще отбележим, че докато за провеждането на КПУ за УК във военната област съществуват множество стандарти (АТР-45, АСР 123 [4], [1]) и езици (BML [5]), то в цивилния сектор, за момента, подобни стандарти и езици са в процес на формиране: Common Alerting Protocol – CAP, Emergency Data Exchange Language (Distribution Element) - EDXL – (DE), Global Justice XML Data Model – GJXDM, National Information Exchange Model – NIEM и IEEE 1512.1 - IEEE 1512.4) и предлагане за стандартизиране от организации като: OASIS, (Organization for the Advancement of Structured Information Systems), DHS (U.S. Department of Homeland Security), FEMA (U.S. Federal Emergency Management Agency) и правителството [4], [21], [26].

Основна причина за създаването на такива стандарти, изискващи специализирани структури на обменните съобщения, привилегировано (ускорено) рутиране и специализирани речници за многоезична комуникация е подобряване на комуникационните възможности между участващите в процеса на УК ведомства в регионален, национален и глобален план, водещо от своя страна до увеличаване на спасените при реална кризисна ситуация.

Настоящото решение за интелигентна система за обмен на съобщения използва модифициран EDXL v. 1.0 (Emergency Data eXchange Language) [26].

Формално, описанието, на примерно съобщението за кризисно събитие изглежда по следния начин:

```
<?xml version="1.0" encoding="UTF-8"?>
<mess_id>mess11</mess_id>
<DateTime>2007-01-01T12:53:00-05:00</DateTime>
<mess_type>0</mess_type>
```

```
<mess_sender>user0@test.org</mess_sender>
<mess_receivers>user1@test.org,user2@test.org</mess_receivers>
<mess_urgency>3</mess_urgency>
<mode>0</mode>
<level>0</level>
<confidentiality>0</confidentiality>
<mess_event>TBD</mess_event>
<mess_event_geo_loc>place.kml</mess_event_geo_loc>
<mess_event_extra_info>TBD</mess_event_extra_info>
<mess_action>TBD</mess_action>
<mess_action_geo_loc>place1.kml</mess_action_geo_loc>
<mess_action_extra_info>TBD</mess_action_extra_info>
```

Тук ще отбележим че гореизложените полета имат следния смисъл: <mess_id> „идентификатор на съобщението”, <DateTime> „дата_време”, <mess_type> „тип на съобщението” (известие, информационен, заповед), <mess_sender> „съобщение_подател”, <mess_receivers> „съобщение_получатели”, <mess_urgency> „съобщение_спешност” (нормално, незабавно, светкавично), <mode> „режим” (текущ, извънреден, информационен), <level> „ниво” (стратегическо, операционно, тактическо), <confidentiality> „конфиденциалност” (некласифицирано, класифицирано, строго секретно). В допълнение, са добавени и полетата <mess_event> „съобщение_събитие” и <mess_action> „съобщение_действие” с допълнителна географска информация: <mess_event_geo_loc>„съобщение_събитие_географско_разположение”, <mess_action_geo_loc>„съобщение_действие_географско_разположение” и друга информация в свободна форма - <mess_event_extra_info>, <mess_action_extra_info>) с цел подобряване разбираемостта на съобщенията от обучаемите реални хора.

5. Софтуерна реализация

Показаната на Фиг.2 архитектура беше използвана за разработването на софтуерен пакет, състоящ се от: *Генератор на сценариев скрипт от съобщения*, *Клиентско приложение за съобщения*, *e-mail сървър* и *архивираща система с БД и веб-интерфейс*. Подолу градивните елементи от софтуерния пакет на интелигентната система за обмен на съобщения при КПУ за УК ще бъдат разгледани в детайли.

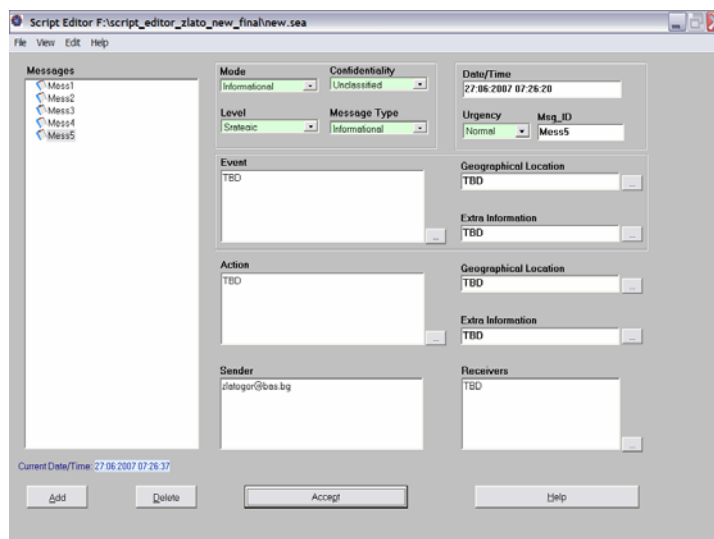
Генератор на сценариев скрипт от съобщения

Генераторът на сценариев скрипт от съобщения беше разработен като компютърно приложение в среда Borland Delphi[®] [16], чрез използване на специализирания компонент Indy 10 SMTP [22].

Принципното разработване на сценарии в КПУ за УК може да бъде извършено с инструменти като I-SCIP и PowerSim[®] [8], [12], а самия процес на симулация – чрез разработването на скрипт на сценария на КПУ за УК [3].

В интелигентната система за обмен на съобщения при КПУ за УК, скриптът на сценарий представлява произволен списък от обекти (обозначен в лявата част на Фиг.3 с **Messages** - „Съобщения”), подреден според полето **Date/Time** - „Дата/Време”. Атрибутите на всяко съобщение (вж. т.4) са позиционирани от дясната страна на Фиг.3. Провеждането на самата симулация се осъществява на базата на изпращане на съобщения по полето **Date/Time** - „Дата/Време” от страна на *генератора на сценариев скрипт от съобщения* или *Клиентско приложение за съобщения*. Към *генератора на сценариев скрипт от съобщения* е вградена възможност за външна намеса и скок във времето с цел осигуряване на „изненада” за участниците в КПУ за УК или ускоряване (прескачане) в симулацията.

Всички съобщения от даден сценариев скрипт могат да бъдат запазени в отделен файлов формат с цел провеждане или повтаряне на дадено КПУ за УК и последващ негов анализ [3].



Фиг.3. Екранна снимка на генератор на сценариен скрипт от съобщения

Клиентско приложение за съобщения

Клиентското приложения за съобщения е разработено в среда Borland Delphi® [16] но чрез използването на специализираните компоненти Indy 10 SMTP и POP3 [22].

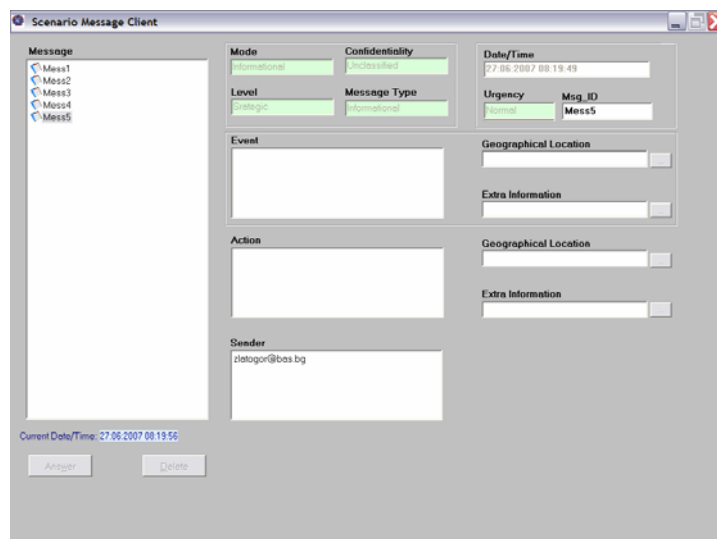
Подобно на всички стандартни e-mail приложения, клиентското приложение за съобщения има два режима на работа: получаване и изпращане. Визуалното разположение на елементите на клиентското приложение за съобщения са подобни на генератора на сценариен скрипт от съобщения (вж. Фиг. 3), като тук ще отбележим че наличието на полето **Geographical Location** - „Географско разположение” за **Event** - „Събитие” и **Action** - „Действие”, изисква предварителна инсталация на продукта Google Earth [19] и достъп до интернет с цел визуализация на географските координати на дадено събитие или действие.

С цел подпомагане на обучаемите, при получаване, всяко съобщение може да бъде автоматично машинно прочетено от клиентското приложение за съобщения при налична инсталация на пакета MS Voice Engine [17]. Допълнително в клиентското приложение за съобщения, съществува възможност за зареждане на сценариен скрипт за клиенти, който на базата на предварително определените роли в дадено КПУ за УК на участниците, по полето **Date/Time** - „Дата/Време” отговаря автоматично след изтичането на определен времеви интервал вместо обучаемия.

Всички съобщения от даден сценариен скрипт могат да бъдат запазени в отделен файлов формат с цел провеждане или повтаряне на дадено КПУ за УК и последващ негов анализ [3].

Двете приложения (Генератор на сценариен скрипт от съобщения и Клиентско приложение за съобщения) позволяват работа както на английски език така и на български език.

Екранна снимка на Клиентско приложение за съобщения е показана на Фиг.4:



Фиг.4. Екранна снимка на *Клиентско приложение за съобщения*

E-mail Сървър

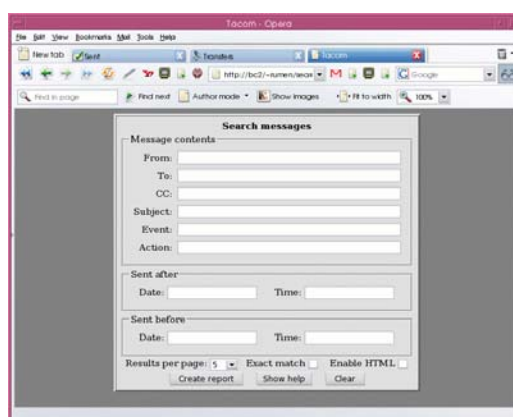
Тъй като идеята на настоящата интелигентна система за обмен на съобщения при КПУ за УК е провеждането на КПУ с учебни цели, изискванията към софтуера на *e-mail сървъра* не са високи и съответно може да се използват комерсиално достъпни продукти които са базирани както на MS Windows [24], така и на Unix/Linux [20].

Архивираща система

Архивиращата система съдържа три основни модула: БД за архивиране и търсене, специализиран POP3 e-mail клиент за всички обменяни съобщения и уеб базиран клиентски интерфейс (вж. Фиг.5). За организация на БД беше избран реляционен тип [6] – PostgreSQL, като всички данни за БД се събират от специализиран POP3 e-mail клиент, който получава, анализира и подава данните за БД.

Архивираните съобщения са видими за външен потребител на *архивиращата система* посредством уеб интерфейс, позволяващ лесно и удобно търсене според формата на съобщението от т.4.

Целият POP3 клиент от *архивиращата система* е разработен на Perl [25] и използва Apache web сървър [15].



Фиг.5. Екранна снимка на уеб интерфейс на *архивираща система*

6. Заключение

През последните три години (2004-2007) в Република България в рамките на проект на НАТО - SfP981149 беше създаден Център на компетентност по операционен анализ (ЦК-ОА, ИПОИ-БАН), Лаборатория за операционен анализ (ИМИ-БАН) и Лаборатория за аналитична поддръжка на трансформацията (ВА „Г.С. Раковски“). Допълнително беше изграден и

Съвместен център за обучение симулации и анализ (СЦОСА, ИПОИ-БАН) в сферата на гражданско-военната сигурност.

ЦК-ОА и СЦОСА работят съвместно с ЦИНСО-БАН, ИКИ-БАН, ГФИ-БАН, НИМХ-БАН, ФХИ-БАН, МО, МВР, МДПБА и ПКЗНБАК при МС за академично изследване на управлението при кризи чрез провеждане на компютърно подпомагани учения и подпомагане трансформацията на сектора за сигурност чрез операционен анализ.

Представената интелигентна система за обмен на съобщения, разработена в ЦК-ОА, предоставя възможност за създаване на съвременно, гъвкаво и икономически ефективно провеждане на обучение както в цивилния така и във военния сектор на сигурността чрез прилагане на моделирането и симулациите като инструмент за създаване на виртуална среда за работа.

7. Благодарност

Авторът изказва благодарност за финансовата и техническа подкрепа към Научната Дивизия на НАТО и програмата “Наука за Мир”, проект: SfP 981149 “Изследване на операциите в подкрепа на планирането на силите и операциите в новата среда за сигурност” (“Operations Research Support to Force and Operations Planning in the New Security Environment”). Той благодари също на: д-р Велизар Шаламанов (директор на НАТО SfP 981149 за България и р-л секция ИРИС, ИПОИ-БАН), г-н Клаус Нимайер (НАТО директор на SfP 981149), акад. Кирил Боянов (директор ИПОИ-БАН), проф. Стефан Хаджитодоров (директор ЦИНСО-БАН), ПКЗНБАК при МС, ръководството на БАН, инж. Румен Богдановски, инж. Георги Дуков и всички колеги от ЦК-ОА/СЦОСА за оказаната подкрепа.

8. Литература

- [1]. *Allied Command Publication 123 (ACP 123)*, 15 August, 1997.
- [2]. *DoD Modeling and Simulation (M&S) Management*, DoD Directive 5000.59, January 4, 1994.
- [3]. *Lessons Learned*, EU TACOM SEE 2006, NOA, TR-25, 18.09.2006.
- [4]. *Modelling and Simulation Systems for Emergency Response Planning and Training*, RTA, NIAG SG98, Final Report, February 2007.
- [5]. *Coalition Battle Management Language*, (C-BML) Study Group Final Report, SISO-REF-016-2006-V1.0, July 31, 2006 .
- [6]. Codd, E. *A Relational Model of Data for Large Shared Data Banks*, Communications of the ACM, vol. 13, no. 6, 377-387, 1970.
- [7]. Loftin, R. *The Future of Simulation*, In Virtual Media for Military Applications. Meeting Proceedings RTO-MP-HFM-136, KN3-1 – KN3-4, 2006.
- [8]. Minchev, Z. *Intelligent Scenario Development for CAI*, NATO ARW: “Scientific Support for the Decision Making in the Security Sector”, Velingrad, Bulgaria, October, 2006, (IOS Press, Amsterdam, Series D: *Information and Communication Security* 12), 16-24, 2007.
- [9]. *NATO Modelling and Simulation Master Plan*, North Atlantic Council, AC/323 (SGMS) D/2, Version 1.0, 7 August, 1998.
- [10]. Shalamanov, V. *Terrorist Threat and Integrated Security Sector - New Challenges for Crisis Management in CEE*, Security Focus and Security Sector Watch, George C. Marshall Association-Bulgaria, no. 11 (June 2004), <http://www.gemarshall.bg/security/issues/11/index.shtml#content2>.

[11]. Shalamanov, V. *Computer Assisted Exercise Environment for Terrorist Attack Consequence Management*, NATO MSG Symposium on Transforming Training and Experimentation Through M&S, MSG-045/RSY-006, Rome, 5-6 October, 2006.

[12]. Минчев, З., Павлов, Н., Николова, И., Томов, Н. и Цанков, А. *Програмна структура на система за КПУ по управление в извънредни ситуации*, Сборник с доклади от Първа национална научно-практическа конференция по управление в извънредни ситуации и защита на населението, ЦИНСО-БАН, София, 10 Ноември, 340-351, 2005 (публикувана 2006).

[13]. Минчев, З. *Използване на моделирането и симулациите в компютърно подпомагани учения за подобряване на гражданската сигурност*, Сборник с доклади от Национална конференция под патронажа на Министър-председателя на Република България - „Европейската интеграция, младежта на България и иновационното и информационно общество”, София, БАН, 18 май 2007.

[14]. Шаламанов, В., Томов, Н., Павлов, Н., Минчев, З., Николова, И., и Семерджиев, А. *Ролята на компютърно подпомагани учения (КПУ) за ефективно управление при кризи*, сборник с доклади от международна конференция „Структури за сигурност на Балканите. Управление при кризи”, организирана от сдружение „Балкански форум по сигурността” (София, Интер-експо център, 14-15 Септември, 2005г.), 70-84, 2006.

[15]. <http://httpd.apache.org>

[16]. <http://www.borland.com>

[17]. <http://www.bytecool.com>

[18]. <http://www.gcmarshall.bg/sfp981149>

[19]. <http://earth.google.com>

[20]. <http://www.emailman.com/unix/servers.html>

[21]. http://www.incident.com/cookbook/index.php/A_Roadmap_to_Emergency_Data_Standards

[22]. <http://www.indyproject.org>

[23]. <http://www.jfcom.mil/>

[24]. http://www.kerio.com/kms_home.html

[25]. <http://www.perl.com>

[26]. <http://xml.coverpages.org/edxl.html>

Автор:

д-р Златогор Минчев – н.с. II ст., Институт по паралелна обработка на информацията-БАН, София 1113, ул. „акад. Г. Бончев”, бл.25А, ст. 116, тел.: +3592 979 6631, e-mail: zlatogor@bas.bg