

“VASIL LEVSKI” NATIONAL MILITARY UNIVERSITY
“ARTILLERY, AIRCRAFT DEFENSE AND CIS” FACULTY

**INTERNATIONAL SCIENTIFIC
CONFERENCE 2017**

C O L L E C T I O N O F P A P E R S

DEFENSE AND SECURITY

**ARMS, TECHNOLOGIES,
LOGISTICS**

**COMMUNICATION AND
COMPUTING TECHNOLOGIES**

SOCIAL SCIENCE

Shumen, Bulgaria
2017

TO THE READERS

This collection is divided in three parts and includes science papers presented on the International Scientific Conference “Defense Technology Forum 2017” in “Artillery, Aircraft Defense and CIS” Faculty, Shumen, Bulgaria.

Authors are responsible for the contents and the papers are not further edited after sending for publication.

The reviewers committee will be thankful for all proposed notes, corrections and replies.

Reviewers committee

REVIEWERS COMMITTEE

- Prof. D.Sc.Tech. Hristo HRISTOV, “Prof. Tsvetan Lazarov” Defence Institute, MoD
- Prof. Anatoly MASLAK, D. Sc.Tech, Kuban State University, Russia
- Prof. Dr. Atanas RADENSKI, Chapman University, USA
- Prof. Slawomir BARTOSIEWICZ, PhD, Logistics Faculty, Military University of Technology, Poland
- Colonel Eng. Assoc. Prof. Traian ROTARIU PhD, Military Technical Academy of Bucharest, Head of Department
- Col. Assoc. Prof. Eng. Maciej MARCZYK, Ph.D., CIS Department, Military Studies Faculty, War Studies University, Warsaw, Poland
- LTC Assoc. Prof. Eng. Bartosz BIERNACIK, Ph.D., CIS Department, Military Studies Faculty, War Studies University, Warsaw, Poland
- Col. Assoc.Prof. Eng. Marin LUPOAE PhD, Military Technical Academy of Bucharest, Romania, Head of Department
- Col. Eng. Assoc. Prof. Dilyan DIMITROV Ph.D., Artillery, Air Defense and CIS Faculty, Bulgaria, “Vasil Levski” National Military University, Head of “Communication Networks and Systems” Department
- Col. Eng. Assoc. Prof. Atanas ATANASOV Ph.D., Artillery, Air Defense and CIS Faculty, “Vasil Levski” National Military University, Head of “Air Defense” Department
- LTC Eng. Assoc. Prof. Stanco STANCHEV Ph.D., Artillery, Air Defense and CIS Faculty, “Vasil Levski” National Military University, Head of “Artillery” Department
- LTC Eng. Assoc. Prof. Cristian-Emil MOLDOVEANU Ph.D., Military Technical Academy, Romania
- LTC Eng. Assoc. Prof. Conyu CONEV Ph.D., Artillery, Air Defense and CIS Faculty, “Vasil Levski” National Military University, Bulgaria
- LTC Eng. Assoc. Prof. Vanko GANEV Ph.D., Artillery, Air Defense and CIS Faculty, Bulgaria, Head of “Arms and Design Technologies” Department
- Col. Vasile SANDRU, PhD, “Henry Coanda” Air Force Academy, Romania
- LTC Zdzisław HRYCÍOW PhD, Mechanical Engineering Faculty, Military University of Technology, Poland
- LTC Cristian ENE, “Henry Coanda” Air Force Academy, Romania
- LTC Marian OANA, “Henry Coanda” Air Force Academy, Romania
- LTC Zdzisław HRYCÍÓW, PhD, Faculty of Mechanical Engineering, Military University of Technology, Poland
- Maj. Daniel STEFANESCU, “Henry Coanda” Air Force Academy, Romania
- Maj. Witold MATERAK, War Studies University, Warsaw, Poland

- Dr. Samarjeet BORAH, Assoc. Prof. in Computer Science & Engineering Department, Sikkim Manipal Institute of Technology, India
- Assoc. Prof., PhD. Margarita VASSILEVA, Artillery, Air Defense and CIS Faculty, “Vasil Levski “ National Military University, Bulgaria
- Assoc. Prof. Hristo DESEV Ph.D., Artillery, Air Defense and CIS Faculty, “Vasil Levski “ National Military University, Bulgaria

© “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2017.
 c/o Jusautor, Shumen
 ISSN 2367-7902

СЪДЪРЖАНИЕ

PLENARY SESSION.....	8
<i>C. Ст. Евлогиев, ОТКРИВАНЕ</i>	<i>8</i>
<i>S. S. Evlogiev, WELCOME SPEECH.....</i>	<i>10</i>
<i>Andon D. Lazarov, LATEST WEAPON TECHNOLOGY - DEVELOPMENT AND ADVANCEMENT</i>	<i>12</i>
<i>Pamfil Șomoiaș, Cristian-Emil Moldoveanu, RESEARCHES CONCERNING THE UNGUIDED ROCKET EFFECTIVENESS</i>	<i>35</i>
<i>Cristian-Emil Moldoveanu, Pamfil Șomoiaș, Thomas Gaden, RESEARCHES CONCERNING THE BULLET IMPACT AND RICCOCHET</i>	<i>43</i>
<i>Bartosz Fikus, PRELIMINARY NUMERICAL ESTIMATION OF SELECTED TERMINAL BALLISTIC EFFECTS PRODUCED BY EXPLOSION OF MORTAR PROJECTILE</i>	<i>49</i>
<i>Анатолій А. Маслак, ИЗМЕРЕНИЕ ЛИЧНОСТНЫХ КАЧЕСТВ СТУДЕНТОВ</i>	<i>59</i>
<i>Bartosz Biernacik, GROWING IMPORTANCE OF CYBERSECURITY IN OTHER COUNTRIES</i>	<i>67</i>
DEFENSE AND SECURITY.....	83
<i>Krystian Frącik, POLISH SPECIAL OPERATION FORCES - DIRECTIONS OF DEVELOPMENT</i>	<i>83</i>
<i>В. П. Петров, ВЪЗНИКВАНЕ И РАЗВИТИЕ НА ТРАНСГРАНИЧНАТА ОРГАНИЗИРАНА ПРЕСТЪПНОСТ В СВЕТА.....</i>	<i>101</i>
<i>В. П. Петров, ЦИКЪЛ НА ПОЛИТИКАТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА БОРБА С ОРГАНИЗИРАНАТА И ТЕЖКАТА МЕЖДУНАРОДНА ПРЕСТЪПНОСТ.....</i>	<i>112</i>
<i>К. К. Казаков, ПРИНЦИПИ НА РАЗУЗНАВАТЕЛНИЯ АНАЛИЗ И СИНТЕЗ.....</i>	<i>124</i>
<i>Ж. С. Йорданов, ПОДХОД ЗА ИЗСЛЕДВАНЕ НА ВЗАИМОДЕЙСТВИЕТО МЕЖДУ ВЪОРЪЖЕНИТЕ СИЛИ И ИНСТИТУЦИИТЕ, УЧАСТВАЩИ В СИСТЕМАТА ЗА ЗАЩИТА НА ВЪТРЕШНАТА СИГУРНОСТ НА СТРАНАТА</i>	<i>132</i>
<i>А. Л. Атанасов, АНАЛИЗ НА ПОНЯТИЕТО „ВИСОКОТОЧНО ОРЪЖИЕ”</i>	<i>140</i>
<i>Ст. Н. Чанев, ЗЕНИТНОРАКЕТНА СИСТЕМА ЗА БЛИЗКО ДЕЙСТВИЕ КАТО СИСТЕМА ЗА МАСОВО ОБСЛУЖВАНЕ.....</i>	<i>149</i>
<i>К. А. Илиев, Р. Б. Чалъков, „СЪВМЕСТНА ОГНЕВА ПОДДРЪЖКА” – ФАКТОР В СЪВРЕМЕННИТЕ ОПЕРАЦИИ.....</i>	<i>158</i>
<i>И. И. Кешишев, БОРБА ЗА НЕЗАВИСИМОСТ НА ТУАРЕГИТЕ В ОБЛАСТТА АЗАБАД.....</i>	<i>166</i>
<i>Х. А. Десев, ПОДХОДИ ЗА ПОВИШАВАНЕ НА ЕФЕКТИВНОСТТА ПРИ ПРОТИВОДЕЙСТВИЕ НА ИЗПОЛЗВАНЕТО НА ПАРИТЕ, ПРИДОБИТИ ОТ ПРЕСТЪПНА ДЕЙНОСТ.....</i>	<i>169</i>

<i>K. Slavyanov</i> , CONTEMPORARY SYNTHETIC APERTURE RADAR SYSTEMS. MARKET SITUATION	175
<i>Д. К. Марков</i> , ПОРАЗЯВАНЕ НА ЦЕЛИ ОТ АРТИЛЕРИЙСКИ ФОРМИРОВАНИЯ, ВЪОРЪЖЕНИ СЪС 122-ММ СГ 2С-1 „ГВОЗДИКА“ В БЛИЗОСТ ДО ЗОНАТА ЗА КООРДИНИРАНЕ НА ВЪЗДУШНОТО ПРОСТРАНСТВО	181
<i>Д. К. Марков</i> , ПОРАЗЯВАНЕ НА ЦЕЛИ ПРИ СЪВМЕСТНА ОГНЕВА ПОДДРЪЖКА В ЗОНАТА ЗА КООРДИНИРАНЕ НА ВЪЗДУШНОТО ПРОСТРАНСТВО	192
<i>Д. К. Марков</i> , ТРАНСФОРМИРАНЕ НА КООРДИНАТИТЕ НА ТОЧКИ МЕЖДУ КООРДИНАТНИ СИСТЕМИ СК-42 И WGS – 84 ЗА НУЖДИТЕ НА АРТИЛЕРИЙСКИТЕ ФОРМИРОВАНИЯ	199
<i>Н. Г. Борисова</i> , ОПАЗВАНЕТО НА ОБЩЕСТВЕНИЯ РЕД ОСНОВНА ДЕЙНОСТ НА ОРГАНИТЕ НА МВР	208
<i>М. М. Галиб, Х. Й. Косева</i> , ПРИЛОЖЕНИЕ НА КРИПТОВАЛУТАТА BITCOIN В ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА СИГУРНОСТ	216
<i>М. М. Галиб, Х. Й. Косева</i> , НЕОТОРИЗИРАНО ПРИДОБИВАНЕ НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ ЧРЕЗ КИБЕРАТАКАТА PHISHING	221
<i>В. Д. Делев</i> , ЕНЕРГИЙНАТА СИСТЕМА КАТО КОМПОНЕНТ НА НАЦИОНАЛНАТА СИГУРНОСТ	225
<i>В. Д. Делев</i> , МЕТОДИ ЗА ПРЕВЕНЦИЯ НА ТЕРОРИЗМА В НАШИ ДНИ	228
<i>К. М. Желев</i> , ТРАФИК НА ХОРА	233
<i>К. М. Желев</i> , ВОДОИЗТОЧНИЦИТЕ КАТО ИЗТОЧНИК НА ЗАПЛАХА ЗА ЕКОЛОГИЧНАТА СИГУРНОСТ	237
<i>С. А. Славчев</i> , ОРГАНИЗИРАНА ПРЕСТЪПНОСТ В СТРАНАТА И ИЗВЪН НЕЯ	242
<i>Т. Т. Желязков</i> , КИБЕРТЕРОРИЗЪМ	246
<i>Т. Т. Желязков</i> , МЕТОДИ ЗА ПРЕОДОЛЯВАНЕ НА ОБЩЕСТВЕНО-ПОЛИТИЧЕСКАТА КРИЗА	249
ARMS, TECHNOLOGIES, LOGISTICS	254
<i>Tudor V. Tiganescu, Ovidiu G. Iorga, Marcel Sonu, Ana M. Harbu</i> , RESEARCH AND DEVELOPMENT OF A MULTI-PURPOSE LATENT FINGERPRINT RECOVERY CABINET	254
<i>Tudor V. Tiganescu, Ovidiu G. Iorga, Voicu E. Andreea, Ana M. Florea</i> , RESEARCH, DESIGN, DEVELOPMENT AND BENCH TESTING OF A HYBRID REACTIVE PROPULSION SYSTEM FOR SPACE LAUNCHER APPLICATIONS	260
<i>Andreea Voicu, Gabriela Toader, Mircea Teodorescu, Octavian Orban, Viorel Tiganescu, Traian Rotariu</i> , ECO-FRIENDLY POLYMERIC BINDERS FOR ENERGETIC FORMULATIONS	269
<i>Marek Gąsiorowski, Bartosz Fikus</i> , ESTIMATION OF MORTAR SHELL TRAJECTORY USING THEORETICAL MODEL	284

<i>Şandru Vasile</i> , COMPARATIVE ANALYSIS OF SURFACE BASED AIR DEFENSE SYSTEMS' FIRE CONTROL UNIT	293
<i>Lyubomir Lazov, Erika Teirumnieka, Edmunds Teirumnieks, Hristina Deneva</i> , DANGERS OF IRRADIATION OF MILITARY STAFF WITH LASER LIGHT ...	302
<i>Lyubomir Lazov, Erika Teirumnieka, Edmunds Teirumnieks, Hristina Deneva</i> , INFRARED LASERS IN THE MILITARY ACTION	313
<i>С. С. Евлозиев, И. Г. Кацев</i> , ПРЕГЛЕД НА СЪВРЕМЕННИТЕ ОПТИЧЕСКИ ПРИБОРИ ЗА РАЗУЗНАВАНЕ, ПРЕДНАЗНАЧЕНИ ЗА ИЗПОЛЗВАНЕ ОТ АРТИЛЕРИЙСКИТЕ ПРЕДНИ НАБЛЮДАТЕЛИ.....	323
<i>K. S. Davidov, Ts. G. Tsonev</i> , A METHOD FOR SOLVING THE TASK FOR MODERNIZATION OR PURCHASING OF LIGHTLY ARMORED COMBAT VEHICLES.....	329
<i>A. I. Bogdanov</i> , USE OF HEURISTIC ALGORITHMS IN LOGISTICS.....	336
<i>Y. D. Dimitrova, Ts. G. Tsonev</i> , EXPERIMENTAL IVESTIGATION ON THE DEVIATION OF THE MIDPOINT OF THE HITS OF THE SHOTS AND THE GROUPING AT SHOOTING WITH SMALL ARMS WITH FITTED SILENCER	341
<i>С. И. Антонов, И. С. Христозов</i> , МОДЕЛИ НА СЪЩЕСТВУВАЩАТА СИСТЕМА ЗА ТЕХНИЧЕСКО ОБСЛУЖВАНЕ И РЕМОНТ НА ВЪОРЪЖЕНИЕТО	348
COMMUNICATION AND COMPUTING TECHNOLOGIES.....	364
<i>Г. Л. Димитров</i> , КОМУНИКАЦИОННИ РЕШЕНИЯ ЗА БЪРЗО РАЗВРЪЩАНЕ ПО ВРЕМЕ НА БЕДСТВЕНИ СИТУАЦИИ.....	364
<i>Г. Л. Димитров</i> , МОБИЛНА РОБОТИЗИРАНА КОМУНИКАЦИОННА МРЕЖА ЗА БЪРЗО РАЗВРЪЩАНЕ В СЛУЧАИ НА АВАРИИ И БЕДСТВИЯ.....	373
<i>М. Х. Ламбева</i> , СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ. ВЪЗМОЖНОСТИ ЗА ОЦЕНЯВАНЕ	380
<i>М. Х. Ламбева</i> , МОДЕЛ НА СЪВМЕСТИМОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ	387
<i>М. Х. Ламбева</i> , РАЗМИТ МОДЕЛ ЗА ОЦЕНЯВАНЕ НА ОПЕРАТИВНАТА СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ.....	394
<i>D. I. Dimitrov, D. A. Atanasov</i> , IMPLEMENTATION OF THE HOUGH TRANSFORM IN DETECTION OF TARGET TRAJECTORY	400
<i>M. K. Kirov, I. A. Iliev</i> , CORRELATION-PULSE METHOD FOR INCREASING THE SENSITIVITY OF THE PROXIMITY RADAR RECEIVER.....	408
<i>В. Т. Стоянова, Н. Ж. Кулев</i> , АНАЛИЗ НА ПОКАЗАТЕЛИТЕ ЗА КАЧЕСТВОТО В СТЕГАНОГРАФИЯТА С ИЗОБРАЖЕНИЯ.....	414
<i>Д. Т. Дойчинов</i> , МЕРКИ ЗА ЗАЩИТА НА УЕБ ПРИЛОЖЕНИЯ ОТ АТАКИ...420	
<i>Д. К. Хубенов</i> , ТЕХНИКИ ЗА ПОДДЪРЖАНЕ НА ИНФОРМАЦИЯ ЗА СВОБОДНИЯ РАДИОЧЕСТОТЕН СПЕКТЪР В КОГНИТИВНИТЕ РАДИО МРЕЖИ, ИЗГРАДЕНИ ПО СТАНДАРТ 802.22	427

<i>И. Г. Кацев, АНАЛИЗ НА ПРЕДИМСТВАТА И НЕДОСТАТЪЦИТЕ ОТ ИЗПОЛЗВАНЕТО НА МОБИЛНИ GPS ПРИЕМНИЦИ ЗА ВОЕННИ ЦЕЛИ ...</i>	435
<i>Г. Р. Парашикеванова, В. П. Василев, В. В. Лилов, ВИДЕОНАБЛЮДЕНИЕ ОТ НОВО ПОКОЛЕНИЕ С INTELLIGENT VIDEO MANAGEMENT SYSTEM.....</i>	442
<i>Д. Р. Денев, Т. С. Исмаил, Т. Н. Тончев, ЦИФРОВА АУДИО РАБОТНА СТАНЦИЯ FL STUDIO ЗА АУДИО ОБРАБОТКА</i>	449
<i>Т. Н. Тончев, А. Б. Александрова, РАЗПРОСТРАНЕНИЕ НА ЕЛЕКТРОННИ КНИГИ</i>	457
<i>L. G. Nikolov, D. K. Hubenov, BER PERFORMANCE FOR WCDMA SIGNAL IN A JAMMED RADIO ENVIRONMENT</i>	464
SOCIAL SCIENCE	469
<i>Г. Петков, М. Митевска, ИЗБОРЪТ НА КАРИЕРА КАТО ФУНКЦИЯ НА ЛИЧНОСТТА.....</i>	469
<i>Г. Петков, М. Митевска, ЛИЧНОСТНИ ПРОЕКЦИИ ВЪРХУ УДОВЛЕТВОРЕНОСТТА ОТ ЖИВОТА</i>	478
<i>Н. М. Петров, ИЗСЛЕДВАНЕ СТЕПЕНТА НА УДОВЛЕТВОРЕНОСТ НА КОМАНДИРИТЕ НА ФОРМИРОВАНИЯ ЗА КОМУНИКАЦИОННО-ИНФОРМАЦИОННА ПОДДРЪЖКА ОТ НИВОТО НА ИЗГРАДЕНИТЕ ПРОФЕСИОНАЛНИ КОМПЕТЕНЦИИ В ОФИЦЕРИТЕ, ЗАВЪРШИЛИ СПЕЦИАЛИЗАЦИЯ „ВОЕННИ КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ“</i>	487
<i>Р. Б. Чалъков, К. А. Илиев, Д. К. Марков, ПОДХОДИ ЗА ОБУЧЕНИЕ НА БЪДЕЩИ ОФИЦЕРИ В НЯКОИ ОТ ВОДЕЩИТЕ АРМИИ НА НАТО.....</i>	496
<i>В. М. Симеонова, ИМИДЖЪТ И КОМУНИКАЦИИТЕ КАТО ВОДЕЩИ ФАКТОРИ В РАЗВИТИЕТО НА ВОЕННАТА ОРГАНИЗАЦИЯ.....</i>	503
<i>Х. А. Христов, СРЕДСТВА ЗА КОНТРОЛ И СПОСОБИ ЗА ПОЛУЧАВАНЕ НА ИНФОРМАЦИЯ.....</i>	508
<i>Х. А. Христов, СЪЩНОСТ И СВОЙСТВА НА ОСНОВНИТЕ МЕТОДИ ЗА КОНТРОЛ</i>	515

PLENARY SESSION

С. Ст. Евлогиев,

ОТКРИВАНЕ

на Международния научен форум:
“DEFENSE TECHNOLOGY – SHUMEN 2017”

Декан на Факултет „Артилерия, ПВО и КИС“
Полк. проф. д-р инж. Сашо Ст. Евлогиев

Уважаеми г-н Заместник-кмет на Община Шумен,
Уважаеми г-н Зам.-областен управител,
Уважаеми господа генерали, офицери, курсанти и студенти,
госпожи и господа,
Скъпи гости,

За мен е чест да Ви приветствам с „Добре дошли“ на Международния научен форум „Отбранителни технологии Шумен 2017“. Тази година Форумът ще се проведе на два основни етапа: международна научна конференция на тема „Изложение на съвременни отбранителни продукти“ и Демонстративни стрелби. Първият етап ще се проведе на 3 и 4 октомври в гр. Шумен, а вторият – на 5 октомври на АП „Марково“.

Уважаеми гости, госпожи и господа,

с огромно удоволствие мога да обявя, че настоящата научна конференция се организира от Факултет „Артилерия, ПВО и КИС“ на НВУ „В. Левски“ и Военната техническа академия – Букурещ, Румъния; Военен университет за технологии, Варшава, Полша; Военновъздушната академия „Хенри Коанда“, Румъния; Университет за военни науки, Варшава, Полша.

Наши гости са:

Зам.-кметът по образование, наука и култура – д-р Найденов Косев;

Зам.-областен управител на Област Шумен – инж. Петко Шаренков.

Фирми от отбранителната промишленост – „Дунарит“, „Арсенал“, „Аркус“, „Черно море“, „Оптикоелектрон“, „Вазовски машиностроителни заводи“ – Сопот.

За първи път Факултетът кандидатства с Проект за подкрепа на международни научни форуми, провеждани в Република България, към Фонд „Научни изследвания“ на Министерство на образованието и науката (МОН), който беше одобрен. Научният форум е съфинансиран на стойност 6929 лв.

Уважаеми госпожи и господа,

Същността на дискусиата, отнасяща се до отбранителните технологии, е изключително важна. През последните 15-20 години отбранителният сектор беше сериозно намален и трансформиран по отношение на европейската и евроатлантическа действителност. Трансформацията в откритията и технологиите в полето на сигурността и отбраната се изразява в следното:

- закриване на важни научни и изследователски структури за отбрана;
- значително намаляване на предприятията в отбранителната индустрия в сравнение с 1990 година;
- преместване на централизираната структура за контрол и координация на научни и откривателски дейности и производството в интерес на отбраната;
- намаляване на резултатността на международната активност за коопериране и интеграция в системата за открития в технологиите за сигурност и отбрана;
- значително намаляване на научния потенциал, изграждан с десетилетия;
- остаряла материална база и нейното неефективно използване за отбраната;
- липса на ясна политика за ролята на изследванията, развитието и производството на дейността в системата за сигурност и отбрана.

В същото време Европейският съюз (ЕС) има кристално ясна цел за устойчиво финансиране и дългосрочни перспективи за научни изследвания и технологии. Политиката на Съюза е насочена за изграждането на европейска интеграция в сферата на изследванията, за постигане от предприятията на дългосрочно и устойчиво икономическо развитие. Това стимулира най-добрите компании за изграждане на конкурентноспособно стопанство, основано на знания и умения.

Организацията на науката и технологиите в НАТО стартираха обща Съюзна политика. Тя е концентрирана в изграждането на съюзни отбранителни умения. Главната цел на организацията е да увеличава националните отбранителни способности на базата на съвместни научни и съюзни изследвания и размяна на информация.

Днес ние сме свидетели на един сложен процес. От една страна, динамичността на съществуващите заплахи и непрекъснатите нови заплахи. От друга страна, подобряването на международната среда за сигурност и намаляването на възможността за класическа военна агресия.

Ние можем да видим нов път за националната сигурност. Главната точка е личната сигурност на индивида, обществените и икономически аспекти на личната сигурност без подценяване на обществената сигурност, чуждестранните политики, разузнаване и т.н.

Уважаеми гости,

Искам да съобщя, че в настоящата научна конференция са регистрирани повече от 100 участници, ще бъдат представени повече от 58 доклада и научни съобщения от 63 автори.

Още веднъж от името на ръководството на Факултета и академичния състав благодаря за вашето присъствие. Вашият опит, експертиза и готовност да споделите знания и идеи са високо ценени и много необходими.

Бих искал на всички вас да пожелаая ползотворни дискусии, споделяне на интересни идеи и предложения!

Откривам Международната научна конференция „Изложение на съвременни отбранителни продукти“.

S. S. Evlogiev.
WELCOME SPEECH

at the International Scientific Conference
“DEFENSE TECHNOLOGY FORUM SHUMEN 2017”

Dean of Faculty "Artillery, Air Defense and CIS"
Colonel Ph.D. engineer Sasho Stefanov Evlogiev
Shumen, Bulgaria
2017 October 3-d

Deputy Mayor for Culture and Education,
Deputy Governor of Shumen,
Gentlemen generals, officers, cadets and students,
Distinguished guests and dear friends,

I am honored to welcome you all at the International Scientific Conference “DEFENSE TECHNOLOGY FORUM SHUMEN 2017”.

Thank you for the interest you have shown – and thank you for coming here from near and far to take part in our discussions over the next days.

First, I would like to express my deepest gratitude to the Dean of the Faculty of the Military Technical Academy in Bucharest, Romania, Dr. and the delegation for coming to Bulgaria and being a true partner in co-organizing this international event.

I'm very pleased to see here in Shumen representatives from neighboring countries and partner countries, companies in the defense industry, project implementers.

Our guests are:

- Deputy Minister of Defense of the Republic of Bulgaria
- Governor of Shumen Region
- Deputy Governor of Shumen
- Deputy Mayor for Culture and Education
- Director of "Weapons and ammunition" Head Office
- Companies in the defense industry – "Dunarit", "Arsenal", "Arcus", "Black Sea", "Opticoelectron", "Vazov Machine Works" – Sopot;
- Representatives of the company "Telelink" EAD - Sofia
- Representatives of the company "Rohde & Schwarz"

Among conference participants are:

- Representatives of the "Military Police" - MoD;
- Representatives of the Ministry of Economy, Energy and Tourism;
- Lecturers from Shumen University “Bishop Konstantin Preslavsky”;
- Lecturers from the University of Library Studies and Information Technologies.

Dear ladies and gentlemen,

Discussing matters concerning the defensive technologies is extremely important. In the last 15-20 years the defense sector underwent serious reductions and transformations regarding the European and Euro-Atlantic realities. The transformation of the researches and technologies in the field of security and defense is expressed in the following:

- Closing important structures for scientific and research activities in the field of defense;
- Significant reduction of defense industry enterprises in comparison with 1990;
- Removing the centralized structure for control and coordination of the scientific and research activity and production in favor of the defense;
- Low effectiveness of the international activity for cooperation and integration in the system of the research and in the defense and security technologies;
- Reduction of significant scientific resource built for decades;
- Obsolete material basis and its ineffective use concerning the defense;
- Lack of clear state policy for the role of the research, developing and production activity in the defense and security system.

At the same time, the European Union has crystal clear goals, stable financing and long-term perspectives for scientific researches and technologies.

The Union policy is aimed at building an integrated European research society for achieving long-term and stable economic growth.

It stimulates the best teams for building competitive economy based on knowledge and skills.

The NATO science and technology organization runs the total Union policy. It is pointed at building allied defensive skills. The main goal of the organization is to increase the national defensive abilities on the basis of joint scientific and applied researches and information exchange.

Today we are witnesses of one complex process. On the one hand, dynamics of existing threats and incessantly appearing new threats. On the other hand, improvement of the international security environment and decreasing the possibility for classic war aggression.

We can see a new approach to the national security. The main point is the civil person security, the public and economic aspects of the civil person security without under-rating the state defense, foreign policies, intelligence and so on.

Dear guests,

I can announce that this scientific conference will be attended by more than 100 participants. We are expecting very interesting research papers and scientific reports to be presented at the conference; the number of reports requested was 45.

Once again on behalf of the faculty and staff, I would like to thank you all for coming. Your experience, expertise and readiness to share your knowledge and ideas are highly valuable and needed. I wish to all of us fruitful discussions, interesting ideas and suggestion.

LATEST WEAPON TECHNOLOGY - DEVELOPMENT AND ADVANCEMENT

Prof. DrSc Andon D. Lazarov

BFU – Burgas, Bulgaria

Introduction

As the planet looms towards war with ever-growing tensions between the world's superpowers, armies, navies and air forces are in a constant race for the very best armament systems. The world is closer to war now than at any time in the past 60 years and a former NATO commander issued a chilling warning - global conflict could erupt as early as 2017.

The advancements in warfare and weaponry over the past 100 years have been astronomical. From the invention of the machine gun and the tank in World War One, to the modern air force and of course nuclear weapons in World War Two, military advancements have only continued to develop at a rapid pace in the latter half of the 20th century and the beginning of the 21st century. These rapid changes seem to have altered the face of warfare every decade. While much of the weaponry utilized today could still be called 'traditional,' as global tensions remain high, nations are taking extreme measures to maintain their military supremacy by developing new technologies that give them an edge over perceived threats and enemies.

The accent in the present lecture will be made on military technologies, applied in the airspace on the Earth, at sea, and under sea. A special attention will be given to futuristic weapon decisions and implementations.

1. NEW FIGHTER AIRCRAFT TECHNOLOGIES

1.1. Sixth-generation jet fighter

Next sixth-generation jet fighter is a conceptualized class of fighter aircraft design, more advanced than the fifth-generation jet fighters that are currently in service in the United States and development in other countries. The United States Air Force (USAF) and United States Navy (USN) are anticipated to field their first sixth-generation fighters



in the 2025–30 time frame. The USAF is pursuing development and acquisition of a sixth-generation fighter through the F-X program to complement existing platforms in service such as the Lockheed Martin F-22 Raptor. The USN is pursuing a similar program called the Next Generation Air Dominance, likewise intended to complement and/or replace its existing aircraft such as the Boeing F/A-18E/F Super Hornet.

Boeing F/A-XX concept design

European aircraft giant Airbus is in the early stages of planning the continent's next generation fighter jet. The unnamed fighter could replace current European fighters, including the Eurofighter Typhoon, Boeing F/A-18 Hornet and Dassault's Rafale fighter, in the next ten to fifteen years. Specific characteristics of these jets are as follows:

Eurofighter Typhoon is a large, twin-engine multi-role fighter, extremely maneuverable with a powerful engine. One drawback however is that the Typhoon was originally designed in the 1980s, before stealth became a key requirement for combat aircraft, and has only marginal radar-evading capabilities [1].



Eurofighter Typhoon

The Super Hornet has an internal 20 mm M61 rotary cannon and can carry air-to-air missiles and air-to-surface weapons. Additional fuel can be carried in up to five external fuel tanks and the aircraft can be configured as an airborne tanker by adding an external air refueling system.



Boeing F/A-18 Supper Hornet

French Rafale jet fighter is a French twin-engine, canard delta wing, multi-role fighter aircraft designed and built by Dassault Aviation. Equipped with a wide range of weapons, the Rafale is intended to perform air supremacy, interdiction, aerial reconnaissance, ground support, in-depth strike, anti-ship strike and nuclear deterrence missions. The Rafale is referred to as an "omnirole" aircraft by Dassault.



French Rafale jet fighter

F-35B Lightning is unbeatable, capable of vertical take-off and speeds of up to 1,200 mph (1,931 km/h) at altitudes of 50,000ft (15, 240 m), equipped with laser guided missiles and bombs. The warplane can down rival jets without firing a shot.



F-35B Lightning (Royal Air Force)

Penetrating Counter Air

The U.S. Air Force is finalizing technology requirements for a new fighter jet to enter service sometime in the 2030s. Known as "Penetrating Counter Air," the new fighter will replace the F-22 Raptor and maintain American air superiority in future conflicts. The sixth-generation fighter will incorporate a number of new technologies that for now exist only on the drawing board.



Penetrating counter air

1.2. New generation Airbus fighter

The new generation Airbus fighter would look like a stealthy Eurofighter in both performance and mission. It would be a high-end, high performance fighter with two engines and optimized for air-to-air combat. It would have a powerful, long range radar and beyond visual range missiles such as the UK's **Meteor missile**. Like the Eurofighter, it would have a secondary air-to-ground mission. It would probably be capable of commanding a robotic wingman or a swarm of drones.

Airbus Defence & Space unveiled a concept for a FCAS (Future Combat Air System) - the future strike fighter for the 2030-40 timeframe designed to replace the Eurofighter Tornado, which may be kept in service until 2040.



Airbus Defence and Space's FCAS for a potential successor to the Tornado

Future Combat Air System (FCAS) is a twin-engine, twin-tail stealth design, and would be a twin-seat design. The second crewmember may be especially important for the FCAS concept of operations, which would see it operate in a wider battle network, potentially as a command and control asset or UCAV(Unmanned combat aerial vehicle)/UAV mission commander.

Airbus Defence & Space foresee it is not a strike aircraft in itself - but rather part of a 'system of systems' – with this manned strike platform networked with Eurofighters, unmanned bomb or missile 'mules' and even UAV swarms. FCAS is conceptualized to be a platform able to slot into a scalable system.

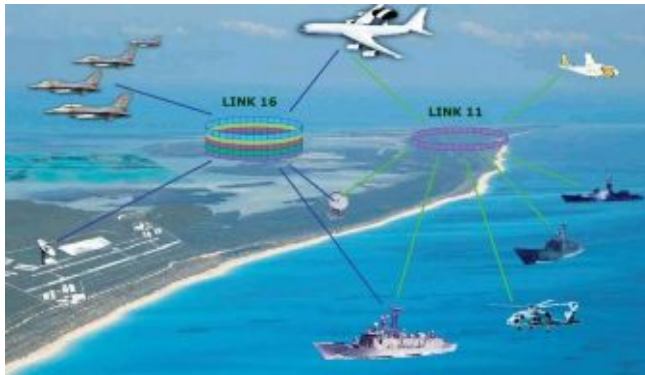
This vision closely aligns with the latest US Pentagon predictions on future air combat – where manned platforms such as F-35 and B-21 would operate as networked nodes, controlling missile 'truck' UCAVs and drone swarms in contested airspace.

1.3. Connectivity, not platforms is key (A330MRTTs)

Platforms will be enhanced with networks. For instance, a JRE (Joint Range Extension) Link 16 capability is now set to be added to French A330MRTTs (Airbus 330 Multi Role Tanker Transport).



This will turn tankers into Link 16 data relay nodes – boosting situational awareness for platforms operating beyond line-of-sight. (**Link 16** is a military tactical data exchange network). In addition laser air-to-satellite data transfer then could offer ultra-high speed, secure communications – especially suitable for the vast amounts of video, imagery and data that now need to flow around the battlefield.



JRE (Joint Range Extension) Link 16

The **connectivity** is of particular importance. Thanks to smaller, cheaper and more capable computers, the ability of networks to adapt and reconfigure on the fly (think smartphone's WiFi), is much more advanced and opens up new possibilities for air combat. The idea is: the tactical transports to become ISR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance) nodes, and the tankers to become **next-generation electronic ELINT** spy planes to help triangulate hostile emitters.

1.4. Lockheed Martin's Advanced Development Programs

Lockheed Martin's Advanced Development Programs, or **Skunk Works**, announced the future of the SR-72, a successor to the iconic SR-71 Blackbird reconnaissance aircraft. The SR-72 will be a strike and reconnaissance aircraft capable of topping Mach 6. The SR-72 is a hypersonic technology, including a combined cycle propulsion

system that merges a supersonic jet engine with a rocket engine. Following demonstrator flight testing, a full-scale twin-engine SR-72, about the same size as the SR-71, could achieve first flight before 2030.



SR-71 Blackbird

The advanced aircraft division is getting close to starting full scale development of a Flight Research Vehicle (FRV) that could be piloted or operated remotely. This FRV is expected to be about the size of an F-22 and use a full combined cycle propulsion system. Lockheed Martin optimistically plans to fly an FRV in the early 2020s.



Flight Research Vehicle (FRV)

1.5. MIG 41 Russia – Super 6th Generation Fighter

For balance, let us consider Russia – Super 6th Generation Fighter: **MIG 41 Russia – Super 6th Generation Fighter**. The MiG-41 would be a completely separate development from Russia's fifth-generation Sukhoi T-50 PAK-FA air superiority fighter. The potential new interceptor would be more of a so-called sixth-generation effort similar in concept to the U.S. Air Force's Penetrating Counter Air or the U.S. Navy's F/A-XX or Next Generation Air Dominance programs.



MIG 41 Russia - Super 6th Generation Fighter

1.6. Air-defence laser drone system

Next step in air-defence efforts is to make a missile-destroying laser drone shooting down ballistic missiles with laser beams. An unmanned, laser-firing drone could intercept nuclear missiles in flight, during the so-called "boost phase" [2]. The Pentagon's planned drone would fly at upwards of 63,000 feet (19, 202 m) of altitude and would loiter near enemy territory for a day or more, ready to shoot down ballistic missiles rising from below with a concentrated pulse of laser light. Ballistic missiles are very difficult to shoot down. Long-range missiles lob their warheads into a trajectory that typically involves a flight through low earth orbit before descending upon their targets at speeds of up to Mach 10. Missile flight is divided into three phases: boost phase (launch), midcourse (coasting through space) and terminal (the minutes or seconds before impact).



US Army drone

The U.S. has built defenses for various types of ballistic missiles that involve intercepts at the midcourse and terminal phases. For example, the Ground-Based Midcourse Defense and (Standard Missile-3: Beating ballistic missiles on land and at sea) SM-3 missiles are designed to hit longer-range missiles in the midcourse phase. Meanwhile, THAAD (Terminal High Altitude Area Defense) and the Ballistic Missile Defense (BMD) version of Patriot, PAC-3 (Patriot Advanced Capability-3 (PAC-3) • Lockheed Martin), are designed to hit warheads in the terminal phase when they are closer to their targets.

But the Pentagon currently has no defense that engages missiles in the boost phase, and as it is pointed out, shooting down missiles during these early moments is the "holy grail" of ballistic missile defense. Ballistic missiles are slowest in the boost phase, making them easier to hit. During the boost phase, the actual warheads, decoys (artificial targets), and other penetrating aids designed to fool enemy defenses are still attached to the missile. So, if you shoot down a ballistic missile in the boost phase, then you could take out multiple warheads and so-called "pen aids" with a single shot.

The problem with boost phase is that the defenses must react very quickly, and for that to happen, the defensive weapon must be as close to enemy territory as possible. Most modern ballistic missiles are launched from mobile launching pads, making launch locations difficult to predict.



Airborne Laser as it was supposed to work (Boeing YAL-1)

First attempt to developing laser weapons for this kind of purpose has been at the beginning of 21th century. The effort culminated in the (Boeing YAL-1), YAL-1, a 747 jumbo jet outfitted with a Chemical Oxygen Iodine Laser (COIL) but canceled based on its inefficiency. It has to be for long time close to the enemy base to intercept the ballistic missile.



Iranian Shahab-3 missile, 2009. (A potential target)

Now the Missile Defense Agency wants to try again. What's changed? Two big things: the rise of solid state and liquid lasers, and drones. While the COIL laser needed a 747 to store the chemicals and electronics involved in generating a one-megawatt laser beam, new solid state lasers are much smaller. The weight goal of General Atomics' 150 kilowatt HELLADS laser weapon, currently under development, is approximately 1,650 pounds (748 kG). Scale that upward to a 1 megawatt laser and you have a weight requirement of 11,550 pounds (5,239 kG), which is right in the Missile Defense Agency's drone payload requirement.

Pilotless drones have other advantages. They are cheaper to fly and can remain in flight for much longer periods of time than manned aircraft. In fact, the Missile Defense Agency (MDA) wants the new laser drone to be capable of loitering for up to 36 hours at altitudes greater than 63,000 feet (19,202 m) or higher and would have a much longer range, in the hundreds of kilometers, due to the lack of laser-degrading particles in the atmosphere at very high altitudes. Flying higher than the YAL-1, this laser drone would have more time to engage the target. It would also be more difficult for enemy forces to shoot down - and not need its own fleet of flying bodyguards to ensure its safety. A scaled-down technology demonstration is scheduled for 2021, although North Korea's progress toward fielding an intercontinental ballistic missile capable of reaching the continental United States may lend a sense of urgency to the program.

1.7. HELLADS

The High Energy Liquid Laser Area Defense System, or HELLADS, is the combination of a dozen different technologies for one awesome purpose: laser weapons mounted on fighter jets. Managed by DARPA, the HELLADS program aims to produce a 150-kilowatt laser that's light enough to fit aboard a relatively small plane like a B-1 Lancer, which means it has to be roughly 10 times lighter than any similarly powered current laser. [4]



150-kilowatt laser that's light enough to fit aboard a relatively small plane like a B-1 Lancer

HELLADS, is a weapon being developed to counter rockets, artillery and mortars. The difference between HELLADS and traditional weapons is that it utilizes lasers to shoot down threats, and is also compact enough to be deployed on a traditional fighter craft. Unlike traditional lasers that need a cooling off period, the liquid lasers HELLADS can fire consistently as long as they contain a cooling system, making them far more effective in war. The HELLADS system has been in test stages for the past six years, and are anticipated to be fully operational within the next five years, changing the face of modern warfare.



HELLADS - a weapon being developed to counter rockets, artillery and mortars

2. Terrestrial weapon systems

2.1. Long-Range Tactical Missile system Long-Range Tactical Missile system

The US Army is getting a new long-range tactical missile system, known as DeepStrike. The DeepStrike missile was originally developed for the U.S. Army's Long Range Precision Fires program. The missile system will replace the Army Tactical Missile System, or ATACMS (Army Tactical Missile System) developed as a means to strike enemy headquarters, fuel and supply depots, helicopter bases, and other high value targets at ranges of up to 190 miles (305.775 km). The DeepStrike missile will be able to strike targets up to 309 miles (497.287 km) away with precision, including moving targets both on land at sea. It means that New Long-Range Tactical Missile, DeepStrike is designed to hit targets far behind enemy lines.



Long-Range Tactical Missile system, DeepStrike



Army Tactical Missile System (ATACMS)

2.2. Devastating' New Terrestrial Weapon

The Kinetic Energy Projectile would be a tungsten warhead that moves at three times the speed of sound, destroying anything in its path [3].



Kinetic Energy Projectile (KEP), a devastating weapon that can destroy anything in its path. It is like a big shotgun shell. However, unlike a shotgun shell, The KEP moves at incredible speeds of “Mach 3 to Mach 6. Those kinetic energy projectiles are warheads that take advantage of high terminal speeds to deliver much more energy onto a target than the chemical explosives they carry would deliver alone. The exploration is in a conceptual phase and not yet any sort of actual program: But the idea is to use that capability in existing launch platforms as part of the weapons suite that already exists. The main contender for a launcher would be the Army Tactical Missile System, made by Lockheed Martin.

2.3. T-14 Armata – Russian Tank

Russia's next-generation main battle tank can fire an anti-tank missile at targets more than seven miles (11 km) away. The T-14 is a formidable-looking beast. Armed with a new 125-millimeter main gun, an unmanned turret, modular armor, and an active protection system designed to shoot down incoming missiles, the vehicle has caused a stir within NATO's tank community. One particularly dangerous feature is the Armata's ability to destroy targets at ranges of up to 12 kilometers, or 7.4 miles. Capable of speeds of up to 56mph 90 kmph – 10mph (16 kmph) faster than the US's top tank the M1 Abrams – the Kremlin's first batch of 100 are currently undergoing trials preparing for combat.



Russia's tanks can outpace their US rivals

2.4. 9K720 ISKANDER - RUSSIAN ISKANDER-M MISSILE SYSTEM: CREDIBLE DETERRENT

The 9K720 Iskander (NATO reporting name SS-26 Stone) is a mobile tactical short-range ballistic missile system. The missile systems are to replace the obsolete OTR-21 *Tochka* systems, still in use by the Russian armed forces, by 2020.



The Iskander-M is a mobile short-range ballistic missile system designed to be used in theater level conflicts with an official range of up to 500 km (minimum-50 km. Highly mobile and stealth, it can hardly be detected even with the help of space reconnaissance assets. The accuracy, range and ability to penetrate defenses allow it to function as an alternative to precision bombing for air forces that cannot expect to launch bombing or cruise missile fire missions reliably in the face of superior enemy fighters and air defenses [5].

The Iskander-M weighs 4615 kg, equipped with two solid-propellant single-stage guided missiles, which use stealth technology. Each missile in the launch carrier vehicle can be independently targeted in a matter of seconds.



The missile cruises at hypersonic speed of 2100–2600 m/s (Mach 6–7). The high velocity of the missile allows it to penetrate antimissile defenses. Flight altitude is up to 6–50 km. Interval between launches: less than a minute. The missile can maneuver at different altitudes and trajectories and can turn at up to 20 to 30 G to evade anti-ballistic missiles. It is controlled in all phases of the flight with gas-dynamic and aerodynamic control surfaces. Targets can be located not only by satellite and aircraft but also by a conventional intelligence center, by an artillery observer or from aerial photos scanned into a computer.

3. Marine Weapon: at sea and under sea surface

3.1. HMS Daring

There are incredible military weapons like invisible warships, and super submarines.

One of the Royal Navy's most advanced warships, the HMS Daring is currently battling ISIS in the Gulf after coming into active service in 2015. Sleek and stealthy, the £1 billion Daring is the leading vessel in Britain's squad of powerful Type 45 destroyers. Armed with sophisticated radar and missile systems, the Daring can also house 60 deadly Royal Marines and deploy them to the field. Despite being blighted by engine issues earlier this year, the Type 45s are still some of the most impressive warships in the world. HMS Daring is fighting ISIS in the Middle East



HMS Daring

3.2. USS Zumwalt (DDG-1000)

The new pride of the American navy the USS Zumwalt was set to be officially commissioned in Baltimore. Incredible looking with a Star Wars-esque appearance, the destroyer is already out there roaming the world's oceans undergoing sea trials – with another 32 on order. As the ship as it is designed to be almost invisible – showing up on a radar as a small fishing boat despite being a whopping 610-foot (186 m) long. It is armed with 600 rockets which can hit targets more than 70 miles (112 km) away and is set to be the world's first warship equipped with a science fiction style rail gun – which use electromagnets to hurl slugs at speeds of up to 5300 mph. 8530 kmph.



USS Zumwalt (DDG-1000). USS Zumwalt is a supreme feat of engineering

3.3. K-329 Severodvinsk

Silent and deadly, Russia's new submarine is the leading force in its growing fleet. The K-329 Severodvinsk is the centre piece of Russian's small but stealthy submarine fleet which has been warned to "outmatch" the undersea power of NATO. With its massive size of 13,600 tons, it is nuclear powered with an unlimited range and its might has already been talked up by the Kremlin's rivals in the Pentagon. Experts have already warned Russia's submarine fleet could be a key in cutting off Europe from the US in a looming invasion.



Severodvinsk - the pride of Russian's navy

3.4. Autonomous Submarine

Boeing is teaming up with America's largest military shipbuilder to work on underwater drones for the U.S Navy. The alliance is aimed at creating drone submarines [4].



Boeing was already at work on the Echo Voyager, a full autonomous underwater vehicle designed for repeated use. Measuring 51 feet (15.54 m) long, the vehicle is built to operate at sea for months at a time with a hybrid rechargeable power system. Adding

Huntington Ingalls Industries to the project will presumably add additional marine expertise. Unlike other drone systems, Boeing wants the Voyager to not need any surface ships or crew standing by [6].

4. Futuristic weapons

4.1. Railgun

An electrically charged and powered massive projectile launcher, the Railgun's technology can theoretically aid in launching aircraft into space. As a weapon, the Railgun has been built and tested to fire non-explosive ordnance at extremely high speeds, faster than the speed of sound in fact, in order to be used as anti-aircraft and anti-missile weaponry [4, 5].



Railgun

The technology to fully support the Railgun is still being developed by the U.S. Navy, in particular, the need to equip naval vessels with battery power that can support the weapon, as well as the necessity of developing Railgun technology itself to slow down the speed at which the weapon erodes. This weapon of the future is firmly in the sights of the military, and there are hopes to fully equip ships by 2025.

4.2. Free Electron Laser

The Free Electron Laser is another of the U.S. Navy's forays into harnessing laser technology to be a primary weapon to shoot down missiles, rockets and enemy aircraft. Beyond the abilities of the laser system, which runs on high speed electrons running through a magnetic tube, the laser will be capable of sensing, tracking and targeting the enemy as well as sharing information with command. While this type of laser has been used in many non-military fields for years, the U.S. Navy has only recently commissioned contracts to build prototypes of the weapon. As of yet, there has only been one prototype demonstration, with an operational prototype expected to be available by 2018.



Electron Laser



US Army: LaWS (Laser weapon system)

4.3. BioDesign Synthetic Organisms project

An extremely ambitious project, again headed by the Defense Advanced Research Projects Agency (DARPA), it is difficult to fully comprehend the purpose and ramifications of the BioDesign Synthetic Organisms project. In essence, the project aims to completely override evolution and create an engineered organism that can defy death, but transversely can also be destroyed with a kill switch. If this sounds like the film *Universal Soldier* then you would be correct in your assessment. DARPA's aim with the project is to "maintain peak soldier abilities and then restore those abilities as soon as possible after an injury. This will include the development of advanced prosthetics (featuring mind-controlled limbs), neural interfaces, the ability to survive blood loss, and even neurotechnological solutions to treat psychological trauma such as PTSD." The 'super soldier' will allegedly also have a loyalty code implanted in its DNA as well to keep them fighting for the right side. While DARPA and many commentators have said that the project has made astonishing headway, the reality of seeing a *Universal Soldier* in real-life combat anytime soon is highly unlikely.



BioDesign synthetic organism

Conclusion

The military technology is continuous developing. Invisible warships, super tanks and unbeatable planes pack the world's arsenal. We are witnesses of ever growing might and intelligence of the weapons. It is difficult to make any prognosis for the future of the world and what will be the outcome of upcoming 3th world War despite any analyzers claim that it already has started with multiple regional conflicts over the world. Let us hope that new weapon technology and their future prospective will have deterrent effect in order to avoid it.

References

1. *Airbus is planning Europe's next-gen fighter*, by Kyle Mizokami. 2017, <http://www.popularmechanics.com/military/aviation/a26933/airbus-planning-next-generation-european/>

2. *The Military will try to make a missile-destroying laser drone*: by Kyle Mizokami, 2017, <http://www.popularmechanics.com/military/weapons/a26948/the-military-wants-a-flying-anti-missile-laser-again/>

3. *US Army exploring 'Devastating' new weapon for use in war with Russia*, Defense One, 2017, <http://www.defenseone.com/technology/2017/04/us-army-exploring-devastating-new-weapon-event-war-russia/136943/>.

4. *World's ultimate weapons: Futuristic arms locked and loaded ready for World War 3*, DailyStar, 2017, <http://www.dailystar.co.uk/news/latest-news/547347/World-War-3-Ultimate-Weapons-Futuristic-Arms-Super-Best-Technology-Russia-US-UK-Nukes-WW3>.

5. *Futuristic military technology*, 2017, <http://www.dailystar.co.uk/pics/pictures/3041/Proposed-futuristic-or-tested-futuristic-military-technology-in-pictures>.

6. *Boeing is teaming up to build an autonomous submarine*, 2017, <http://www.popularmechanics.com/military/navy-ships/a26836/boeing-teaming-up-to-build-autonomous-submarine/>, DefenseOne.

A survey based on author materials of international observers in Aviation week, Defense One, Daily Star, etc, is prepared by Prof. DrSc Andon Lazarov - BFU – Burgas, Bulgaria.

RESEARCHES CONCERNING THE UNGUIDED ROCKET EFFECTIVENESS

Pamfil ȘOMOIAG
Cristian-Emil MOLDOVEANU

Military Technical Academy of Bucharest, 39-49 George Coșbuc Avenue, Bucharest, ROMANIA
pamfil.somoiag@mta.ro, cristian.moldoveanu@mta.ro

Abstract: *The effectiveness of the unguided rockets can be influenced by many factors, like initial conditions perturbations as a small displacement of the firing pods between two launches due to its oscillations. As a consequence, all those parameters have to be taken into account in order to obtain an efficacy firing. This paper will focus on the unguided rocket effectiveness. Using the physical model for the trajectory, we will study the accuracy of the unguided rocket through a statistical analysis and several target models.*

Keywords: *unguided rocket, ballistics, accuracy, impact probability and destruction*

1. Introduction

The unguided rockets are mainly used for missions such as: destroying personnel, military devices, and making target inoperative on large area; slowing down enemy movements, or imposing to enemy troops a specific move; preventing access to specific tactical areas through barrage firing; and providing support by fire tactical maneuvers to friendly troops.

The use of the unguided rockets implies the study of the problematic of their efficiency. Through a preliminary physical and ballistic study completed by some simulations, we tried to set up a model evaluating the efficiency of the weaponry system, in terms of impact accuracy on target. We managed to set up a physical system of trajectories, considering the ballistic parameters. By implementing this theoretical model in numerical methods, we have created a simulating interface for calculating the ballistic results and statistical data. It focuses mainly on the accuracy of multiple rocket launching systems [1]. This algorithm returns useful results and allows to handle different cases corresponding to missions.

2. The mathematical model for the unguided rocket trajectory

The main goals of external ballistics are to set up equations whose solutions will describe as realistically as possible the unguided rockets trajectory [2]. This requires firstly having in mind all the aerodynamic forces that are applied to the rockets. Thereupon, this part aims to describe the physical problematic of an unguided rocket flight, by calculating its trajectory system of equations. In addition, a second aim of this paragraph is to realize a numerical model solving this mathematical complex system for one unguided rocket trajectory [3].

As an object moving in the air, the rocket is subject to aerodynamic forces [5]. Those are consequences of the rocket moving in the air. The dynamic pressure distribution P_s on the rocket surface is $P_s = \frac{1}{2} \rho V^2$, which is generated by the movement of the rocket in the air [6]. The aerodynamic forces result from this dynamic pressure, moreover three resultant forces are deduced on each direction from the velocity referential system. All those forces are applied on the centre of pressure [6].

The first is called drag $\vec{F}_x$, it's opposed to the rocket velocity $\vec{V}$

$$\vec{F}_x = -\frac{1}{2} \rho V^2 S C_x \vec{x}_v \quad (1)$$

The second is the lift $\vec{F}_y$, this force is perpendicular to the velocity:

$$\vec{F}_y = \frac{1}{2} \rho V^2 S C_y \vec{y}_v \quad (2)$$

The third is $\vec{F}_z$, horizontally deviating the rocket :

$$\vec{F}_z = \frac{1}{2} \rho V^2 S C_z \vec{z}_v \quad (3)$$

where C_x, C_y, C_z are coefficients linked to α angle between velocity and rocket longitudinal axis.

The mathematical model of the unguided rocket trajectory [2], [4] is done by the following system of differential equations:

$$\begin{aligned} \frac{dV}{dt} &= -K_x V^2 - g \sin(\theta_v) + a_r \cos(\alpha_v) \\ \frac{d\theta_v}{dt} &= K_y^\alpha \alpha_v V - K_y^\omega \frac{d\eta}{dt} - \frac{g}{V} \cos(\theta_v) \\ \frac{d\theta_h}{dt} &= K_z^\alpha \alpha_h V - K_z^\omega \frac{d\xi}{dt} \\ \frac{d\alpha_v}{dt} &= \frac{d\eta}{dt} - K_y^\alpha \alpha_v V + K_y^\omega \frac{d\eta}{dt} + \frac{g}{V} \cos(\theta_v) \\ \frac{d\alpha_h}{dt} &= \frac{d\xi}{dt} - K_z^\alpha \alpha_h V + K_z^\omega \frac{d\xi}{dt} \\ \frac{d^2\xi}{dt^2} &= -K_m^\alpha \alpha_h V^2 - K_m^\omega V \frac{d\xi}{dt} - \frac{K_\xi}{J_\xi} \frac{d\xi}{dt} \\ \frac{d^2\eta}{dt^2} &= -K_m^\alpha \alpha_v V^2 - K_m^\omega V \frac{d\eta}{dt} - \frac{K_\eta}{J_\eta} \frac{d\eta}{dt} \\ \frac{dx}{dt} &= V \cdot \cos(\theta_v) \cdot \cos(\theta_D) \\ \frac{dy}{dt} &= V \cdot \sin(v) \\ \frac{dz}{dt} &= V \cdot \cos(\theta_v) \cdot \sin(\theta_D) \end{aligned} \quad (4)$$

where:

$$\begin{aligned} a_r &= \frac{T_{\text{mot}}}{m}; \quad K_x = \frac{1}{2m} \rho S C_x; \\ K_y^\alpha &= \frac{1}{2m} \rho S C_y^\alpha; \quad K_y^\omega = \frac{1}{2m} \rho l_{\text{ref}} S C_y^\omega; \\ K_z^\alpha &= \frac{1}{2m} \rho S C_z^\alpha; \quad K_z^\omega = \frac{1}{2m} \rho l_{\text{ref}} S C_z^\omega \end{aligned}$$

$$K_m^{\alpha} = \frac{1}{2I_{\xi}} \rho S l_{ref} C_m^{\alpha} = \frac{1}{2I_{\eta}} \rho S l_{ref} C_m^{\alpha} ; K_m^{\omega} = \frac{1}{2I_{\xi}} \rho S l_{ref}^2 C_m^{\omega} = \frac{1}{2I_{\eta}} \rho S l_{ref}^2 C_m^{\omega}.$$

The equation systems (4) is solved using a program presented in Fig. 1



Figure 1. The interface of the computer program used for trajectory model

The program has the following modules:

- (1) Initial conditions module;
- (2) Multiple launching module;
- (3) Single launching module;
- (4) The results.

3. Numerical results

We will use the unguided rocket trajectory (4) solved by the program presented in Fig 1. We have a precise model of target with health gauges, and we will analyze the effectiveness of firing. In this study, a 64 launching campaign will be used with a large scale of perturbation.

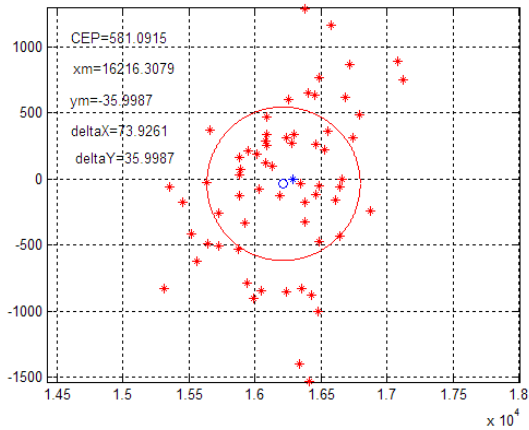


Figure 2. General 64 rockets fire campaign used for statistic study

Next we will change the number of parts inside the target. We will consider a target with an uncertain position. Therefore the mean point of impact will be situated at 357 m from the centre of the target. Here are the 3 types of target used, seen in Fig 3.

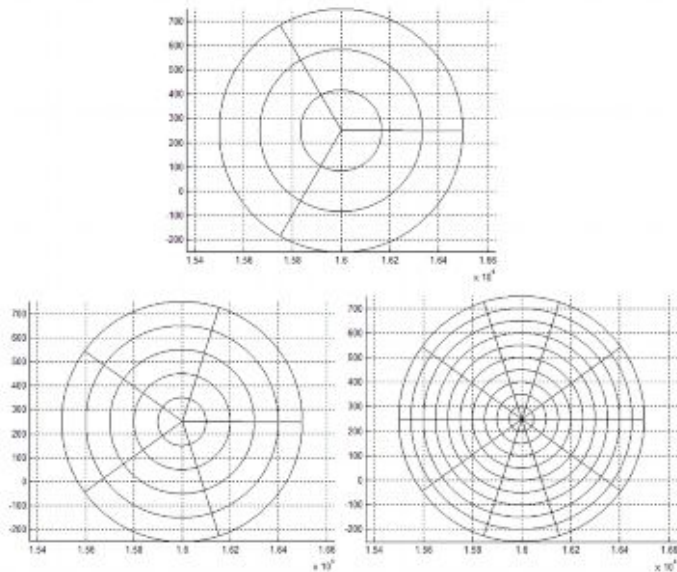


Figure 3. Target used for comparative study : (3x3), (5x5) and (10x10)

With a small number of parts, the target is totally destroyed with this firing campaign. We see that all the parts suffer hit and even the ones suffering one hit are destroyed because of the shrapnel effect. This target has a total of 180 life points.

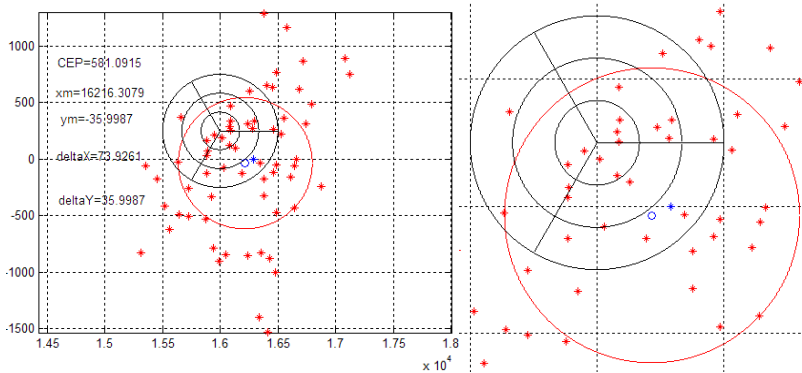


Figure 4. Large scale target with (3 x 3) parts



Figure 5. Results in the case of a large scale target with (3 x 3) parts

Therefore we could add that, to entirely destroy the target with a 34% probability to hit, the first statistical number D95% of rockets launching in order to obtain a 95% destruction of the target, is:

$$D_{95\%} = \left(\frac{95 * \text{number of life}}{100} \right) * \text{hit percentage} \quad (5)$$

$$D_{95\%} = \left(\frac{95 * 180}{100} \right) * \frac{34}{100} = 58$$

As we can see on those different schemes results, from 64 launches, only 22 reach the target in 15 parts (Fig. 6 and 7). The hits are distributed on all the rings composing the target. The hit probability is about 34. The additional data of this simulation is the destruction percentage which is about 41%. In that case the target has a total of 3040 life points, $D_{95\%} = 242$.

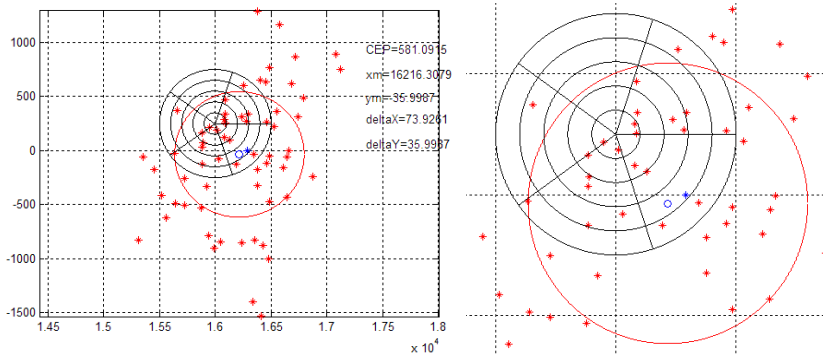


Figure 6. Large scale target with (5 x 5) parts

With a large number of parts (Fig. 8 and 9), the destruction percentage reaches only 6%, because only 19 parts are impacted and an even fewer number are impacted several times. Therefore only some peripheral ones reach 100% destruction, and the target remains quite unaffected. With a total of 5500 Life points, we have: $D_{0.5\%} = 1776$.

In this part we have mainly studied the algorithm capacity on several cases. We have seen the way the algorithm was creating random disruption in the initial conditions of launching. How it was able to compute several disturbed trajectories and the impacts on the ground. Furthermore we have conducted a statistic study on the effect of the disruption on the unguided rocket accuracy [7]. In addition the durability of various kinds of targets on several situations has been examined.

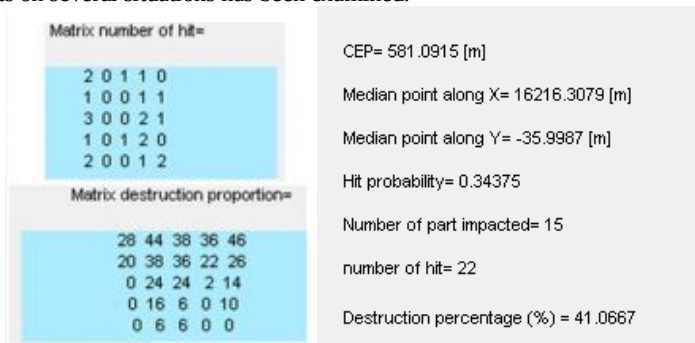


Figure 7. Results in the case of a large scale target with (5 x 5) parts

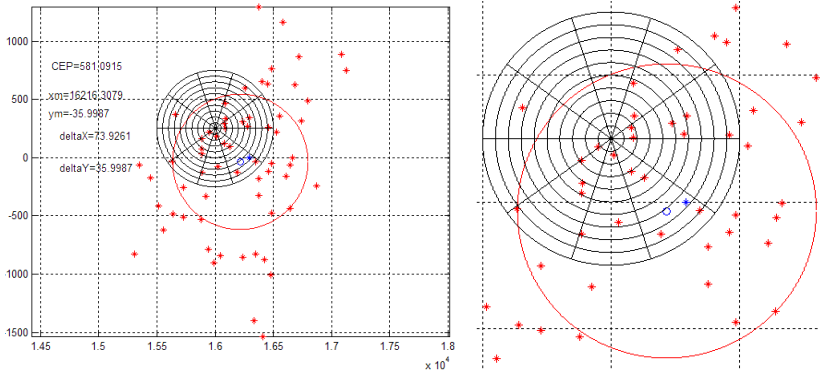


Figure 8. Large scale target with (10 x 10) parts

Matrix number of hit=	Matrix destruction proportion=	CEP= 581.0915 [m]
0 0 0 0 0 0 0 0 0 0	96 100 100 100 100 98 100 98 100 100	Median point along X= 16216.3079 [m]
2 0 0 0 0 1 0 1 0 0	70 84 90 90 88 80 84 80 88 90	Median point along Y= -35.9987 [m]
0 1 0 0 0 0 1 0 0 0	74 70 78 80 80 76 70 76 78 80	Hit probability= 0.34375
0 0 0 0 0 0 0 0 1 0	68 66 70 70 70 70 64 68 58 68	Number of part impacted= 19
1 1 0 0 0 0 2 0 1 0	46 48 58 60 60 56 40 54 48 58	number of hit= 22
1 0 0 0 0 0 0 0 0 0	36 46 50 50 50 50 46 48 48 50	Destruction percentage (%) = 6.9091
1 0 0 0 0 0 0 1 0 0	28 38 40 40 38 40 38 28 38 40	
0 0 0 0 1 0 0 1 0 0	28 28 30 28 20 28 28 18 24 30	
0 1 0 0 0 0 0 0 2 0	16 10 18 20 18 20 18 14 0 16	
1 0 0 0 0 0 1 0 0 0	0 6 10 10 10 8 0 8 6 10	

Figure 9. Results in the case of a large scale target with (10 x 10) parts

This model remains limited by its targets panel, it can only generate circular ones. Furthermore the dividing logic of the targets can be improved, likewise the general geometry. Another way of improving this model would be to realize a Probability to Kill study. For this purpose, the condition when the target is considered killed has to be established. Two kinds of conditions can be chosen. The first one would be hit on some vital points. The second would involve reaching one pre-decided destruction percentage from which the target is considered destroyed.

4. Conclusions

In this study we ran a physical analysis conducting to a final equation system whose parameters were included in a ballistic model. Implementing it on computer program by creating a code with an interface enabled us to find an approximate solution of the system thanks to Runge-Kutta method. It can simulate a trajectory whose order of magnitude in terms of range and velocity is matching with real launching parameters and results. This first code validates our previous ballistic theoretical system.

The last part of the study focused more precisely on validating an algorithm by analyzing multiple launchings [1] campaigns trajectories. This algorithm is able to simulate several launches sequences with initial conditions disturbed. This model aimed to describe the influence of perturbations in the initial conditions that could have big

consequences on their accuracy on impact [7]. It also described how the nature of the target according to its position and its capacity to endure direct hits influenced the final results of a multiple rocket launching. The various and precise data resulting from those tests also allowed us to validate this program.

This program can also be developed in several ways. The model describing the probability to kill if hit can also be implemented on the algorithm. In addition, the statistical model more generally used in this program fits with the simple type of target and could be modified according to more realistic parameters.

References

1. C. Aramă, C. Rotaru, M. Aramă, E. Mihai, A Comparative Analysis Between Two Types of Vehicles Which Could Be Used as UAV Launchers Mobile Platform, Review of the Air Force Academy, No. 3(30), 2015;
2. R. Brouchu, R. Lestage, Three-Degree-of-Freedom (DOF) Missile Trajectory Simulation Model and Comparative Study with a High Fidelity 6DOF Model, DRDCVALCARTIER-TM-2003-056, Technical Memorandum, Defence R&D, Canad-Valcartier, 2003;
3. M. Khalil, H. Abdalla, O. Kamal, Trajectory Prediction for a Typical Fin Stabilized Artillery Rocket, Proc. Of the 13th International Conference on Aerospace Science&Aviation Technology ASAT-13, pp.1-14, Cairo, Egypt, 2009;
4. C.E. Moldoveanu, S. Buono, P. Șomoiaș, Study of the Unguided Rocket Effectiveness, MTA Review, Vol. XXVI, No. 1, 2016;
5. C. Rotaru, G.C. Constantinescu, O. Ciuica, I. Cîrciu, E. Mihai, Mathematical Model and CFD Analysis of Partially Premixed Combustion in a Turbojet, Review of the Air Force Academy, No. 2(32), 2016;
6. C. Rotaru, R.I. Edu, Lift Cpability Prediction for Aerodynamic Configurations, Review of the Air Force Academy, No. 3(27), 2014;
7. T. Saileranta, A. Siltavuori, S. Laine, B. Fagerstrom, On Projectile Stability and Firing Accuracy, Proc. Of the 20th International Symposium on Ballistics, pp. 195-202, Orlando, FL, 2002.

Cristian-Emil MOLDOVEANU^{*)}
Pamfil ȘOMOIAȘ^{*)}
Thomas GADEN^{**)}

^{*)}Military Technical Academy of Bucharest, 39-49 George Coșbuc Avenue, Bucharest, ROMANIA
cristian.moldoveanu@mta.ro

^{**)}ECAM Strasbourg, Rue de Madrid, 67300 Schiltigheim, FRANCE,
thomas.gaden@ecam-strasbourg.eu

Abstract: By computing the useful information obtained with the internal and external ballistics, the theoretical trajectory of a bullet can be calculated. In order to get the most accurate values, preliminary knowledge is needed. So by using appropriate tools and software, a bullet's trajectory can be calculated if the correct values are provided (mass, diameter, initial angle, initial speed). Using the physical model for the trajectory and the experimental means we obtain the bullet impact and ricochet.

Keywords: Ricochet, impact, ballistics, accuracy

1. Introduction

In order to compute the trajectory of the bullet, the different forces and phenomena occurring during the flight need to be assessed. The most effective way to do that is to express all the forces applied to the bullet and to establish the equations of the movement. Some hypotheses are taken in account: the bullet is studied for a short-range; the Coriolis force is neglected etc. There following forces are considered to be applied to the system: weight (G) and drag (R):

$$G = mg \quad (1)$$

$$R = \frac{1}{2} \rho V^2 S C_x \quad (2)$$

with:

- ρ , density of the air [kg/m³];
- V , speed of the bullet [m/s];
- S , cross sectional area [m²];
- C_x , drag coefficient.

Next we can establish the equations needed to study the bullet movement. We use the fundamental principle of dynamics. The following equations are obtained:

$$\begin{cases} \frac{dV}{dt} = -\frac{1}{2m} \rho V^2 S C_x - g \sin \theta \\ \frac{d\theta}{dt} = -\frac{g \cos \theta}{V} \end{cases} \quad (3)$$

In order to obtain the bullet trajectory we use the following initial conditions:

- the initial speed $V_0 = 700$ m/s;
- the initial angle $\theta_0 = 5^\circ$;

- the initial position $(x_0, y_0) = (0, 0)$;
- the mass $m = 9$ g;
- the bullet diameter $d = 7.62 \times 10^{-3}$ m.

2. The computational program

Using the equations presented above we set up a computational program having the aim to calculate the single or multiple trajectories (fig.1). The impact points of the trajectories are obtained by taking in account some obstacles.

The interface is divided into several sections:

- Weapon's parameters:** Includes input fields for d (7.62 [mm]), m (7.9 [g]), tip_cx (1), ind (1.2), and V_0 (983 [m/s]). There are "Default values" and "Modify" buttons.
- Initial conditions:** Includes input fields for X_0 (0 [m]), Y_0 (0 [m]), Z_0 (0.5 [m]), $teta_{OH}$ (1 [°]), $teta_{OV}$ (2 [°]), n_x (1), n_y (1), n_z (1), $nteta_H$ (1), and $nteta_V$ (1).
- Obstacles:** Includes "Number of existing obstacles" (16), "Selected obstacle" (?), "Type of the obstacle" (y), and coordinate ranges for X , Y , and Z axes. There are "Add obstacle", "Display infos", and "Remove obstacle" buttons.
- Calculation:** Includes "Calculate trajectory" and "Calculate multiple trajectory" buttons, with a note to "Enter parameters in 'cond_ind' file".
- Figures:** Includes checkboxes for "Figures inline" (checked) and "Figures offline", and a "Clean figures" button.
- QUIT:** A large button at the bottom center.
- Plots:** Two empty coordinate systems with axes ranging from 0 to 1.

Figure 1. The interface of the computational program

In the **Weapon's parameters** section, the user can modify: the diameter of the bullet, the mass, the drag coefficient, and the initial velocity. In the **Initial conditions** section are the firing parameters: initial position (X_0, Y_0, Z_0) , the horizontal and vertical angles $(V_{\theta_{OH}}, \theta_{OV})$, and the number of different position for each parameter $(n_x, n_y, n_z, n_{\theta_H}, n_{\theta_V})$.

Two other buttons were also added: the **"Default values"** button will modify the values of the two section so that they correspond to the defaults conditions of firing ($d = 7.62\text{mm}$, $m = 7.9\text{g}$, $tip_cx = 1$, $ind = 1.2$, $V_0 = 983\text{m/s}$, $X_0 = 0\text{m}$, $Y_0 = 0\text{m}$, $Z_0 = 0.5\text{m}$, $\theta_{OH} = 0^\circ$, $\theta_{OV} = 1^\circ$, $n_x = n_y = n_z = n_{\theta_H} = n_{\theta_V} = 1$); the **"Modify"** button is used to save the weapon's parameters and the initial conditions before a simulation.

In the **Obstacles** section, the user can:

- see the details of every existing obstacles, by entering the number of the and then clicking on **"Display infos"**. The user will access to the type of the obstacle (perpendicular to the x-axis or y-axis), and the minimum and maximum coordinates along the different axis. If the entered value is above the number of existing obstacles, the program will

display the information of the last obstacle. If the entered number is null or negative, it will display the information of the first obstacle.

- create an obstacle, by entering its number, its type, and the minimum and maximum values of its coordinates and then clicking "**Add obstacle**". If the obstacle is an x-type, the X_{min} and X_{max} coordinates must be the same. If it is an y-type, Y_{min} and Y_{max} must be equal. The user can either create a new obstacle by entering a number above the number of existing obstacle, or replace one by typing the number of one already existing.

- remove an obstacle, by typing the number of the obstacle and then clicking "**Remove obstacle**".

In the **Calculation** section, the user has two choices: calculate one trajectory with the initial parameters entered in the "Initial conditions" section; calculate multiple trajectories on the same figure with the parameters entered in the "cond_init" file of the program's directory.

Finally, on the **Figures** section, the user can choose where to plot the figure: in the interface, in the two already existing graphs (by choosing "Interface Figures"), or in new appearing windows (by choosing "Outside Figures"). The two different options can be chosen at the same time.

3. Numerical results

We will use the computational program presented in Fig 1 in order to calculate the two distances d_1 and d_2 of the associated obstacles, for the following type of firing range (fig. 2). The aim is to obtain a best configuration for the firing range in order to avoid the ricochet and the impact points outside the area of the firing range.

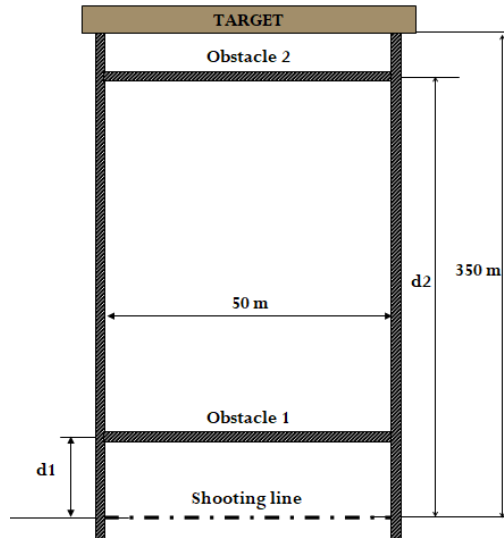


Figure 2. The firing range configuration

The bottom position of the obstacles is considered at 4m and the top is considered at 10m, and for the target wall the bottom is at ground level and the top at 10m.

The problem can be considered as a geometrical problem: the best disposition is made such as the first and second obstacles occupy the biggest surface possible. It also implies that, for a maximum efficiency, they need to only block specific trajectories and not trajectories that the other ones could block (fig. 3).

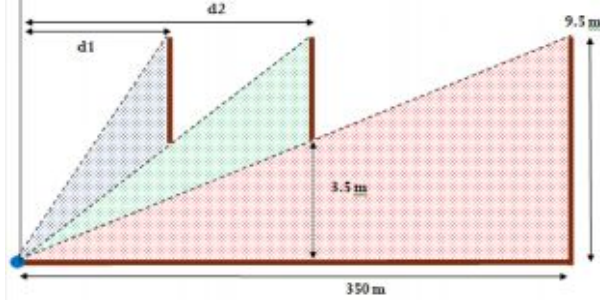


Figure 3. The geometrical problem of the firing range configuration

By running a simulation with the following parameters: $X_0 = Y_0 = 0m$, $Z_0 = 0.5m$, $\theta_{0H} = 0^\circ$, and by making θ_{0V} from 0° to 11.4° , are obtained the results presented in fig. 4.

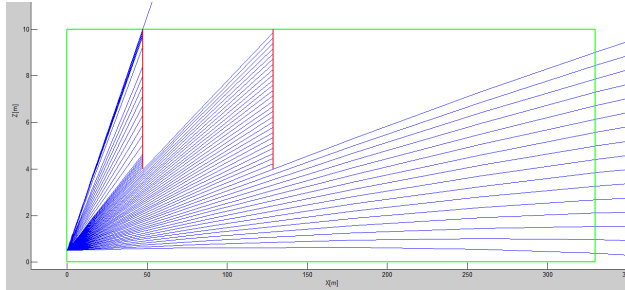


Figure 4. The trajectories obtained for the best firing range configuration

The set of two obstacles positions, respectively at 47.5m and 128.9m and the target wall placed at 350m, we can stop trajectories for $\theta_{0V} < 11.4^\circ$.

4. Experimental results

In order to study the velocity and the angle of the bullet ricochet, the following experiments were done (fig. 5). A gun, with a fixed location, will shoot at a target with a fixed angle. Then, if the ricochet phenomenon occurs, the bullet will impact at a cardboard panel. All along, a camera with fast recording (up to 3000 frame per second) will focus on the target area. That way, it will be possible to work with the recordings and gather data such as the initial velocity, the ricochet velocity, and the vertical ricochet angle. The time will be obtained using the Photron software: the time being obtained using each video frame (fig. 6),

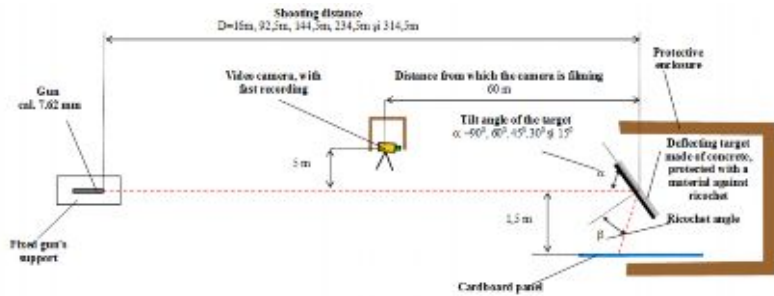


Figure 5. The experimental configuration

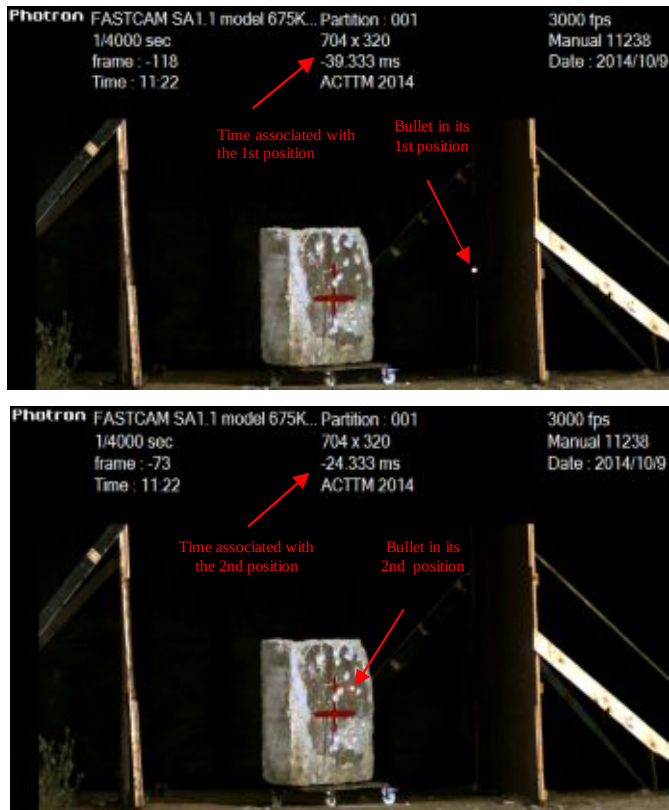


Figure 6. The velocity of the impact bullet calculation

We know the dimensions of the target, the distances between the camera and the target, and the angle between the trajectory of the bullet and the target. Using this data and

by assuming that the bullet hits the centre of the target, the impact angle can be calculated (fig. 7).

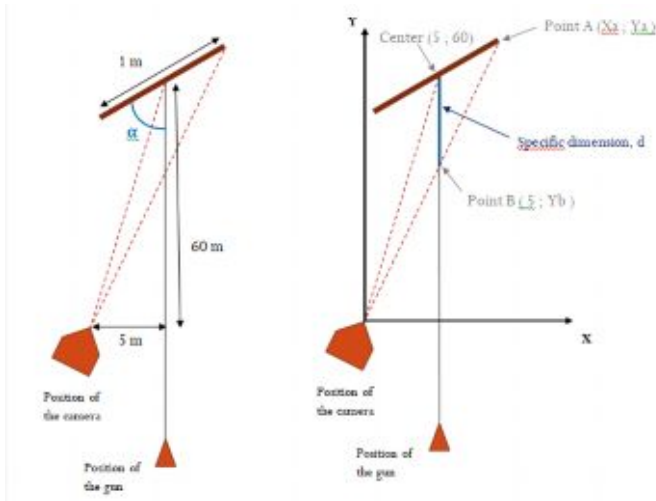


Figure 7. The angle of the impact bullet calculation

4. Conclusions

In this study we ran a physical analysis conducting to a final equation system whose parameters were included in a ballistic model for computing the ricochet parameters of the bullet. Implementing it on computer program by creating a code with an interface enabled us to find an approximate solution of the system using the Runge-Kutta method. It can simulate a trajectory whose order of magnitude in terms of range and velocity is matching with real firing parameters and results. This program can calculate the impact point using the different types of obstacles.

The experiments about the ricochet velocity of a bullet highlight a few points: the initial velocity of a bullet varying from one experiment to another, while the firing conditions are the same; the angle of the target has an important influence on the bullet ricochet angle and velocity: for high incident angles, the bullet will be deflected with a lower velocity.

References

1. R. Brouchu, R. Lestage, Three-Degree-of-Freedom (DOF) Missile Trajectory Simulation Model and Comparative Study with a High Fidelity 6DOF Model, DRDCVALCARTIER-TM-2003-056, Technical Memorandum, Defence R&D, Canad-Valcartier, 2003;
2. T. Saileranta, A. Siltavuori, S. Laine, B. Fagerstrom, On Projectile Stability and Firing Accuracy, Proc. Of the 20th International Symposium on Ballistics, pp. 195-202, Orlando, Fl, 2002.

PRELIMINARY NUMERICAL ESTIMATION OF SELECTED TERMINAL BALLISTIC EFFECTS PRODUCED BY EXPLOSION OF MORTAR PROJECTILE

Bartosz Fikus

Faculty of Mechatronics and Aerospace, Military University of Technology, Warsaw, Poland
bartosz.fikus@wat.edu.pl

Abstract: Results of theoretical modeling of mortar projectile's fragments propulsion were shown. In conducted investigations, due to dynamic character of whole phenomena characterized by extremely high values of strains, the meshless explicit approach was used (Smoothed Particle Hydrodynamics method implemented in AUTODYN software). Results were compared with simplified Gurney's formula, which provided high accuracy for the cylindrical part of the casing in which detonation is fully developed and resulted in higher values of relative discrepancy of initial velocity for the non – cylindrical region, especially where the detonation is not developed.

Keywords: Gurney's formula, mortar projectile, explosion, terminal ballistics, meshless methods

1. Introduction

The mechanisms of influence on enemy of different types of ammunition is strongly dependent on projectile's construction and conditions of its use. The most popular type of considered devices are fragmentation projectiles, in which the fragments are launched by products of detonation of high explosive. One of the crucial parameters for this case of projectiles is fragments' initial velocity, which significantly determines destructive potential of applied shell. Commonly, during estimation of lethal abilities of various systems, the Gurney's formula is used [1]. This simplified approach is based on one – dimensional model of the explosive system and works correctly especially in cases of regular geometries (cylinders, plates – Fig. 1), ensuring approximately 10 % accuracy [2].

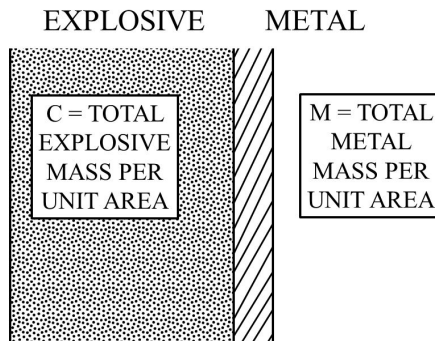


Figure 1. Open – faced sandwich [3]

For the cylindrical symmetry, Gurney assumed that the gases move radially outward from the central axis of the explosive charge. Moreover, he imposed that the radial velocity of gases varies directly with the distance from the axis to the casing [4]. In accordance with Gurney's model, the fragment's initial velocity is approximately equal to:

$$v_c = \sqrt{2E} \sqrt{\frac{\frac{C}{M}}{1 + \frac{C}{2M}}} \quad (1)$$

where E denotes kinetic energy per unit mass, C – mass of the explosive per unit length, M – mass of metal casing per unit length. The constants $\sqrt{2E}$ for various explosives is commonly available and its value depends on confinement conditions – it depends on thickness of casing and strength properties of casing material. For example, for the TNT the value of $\sqrt{2E}$ varies in range between 2.039 km/s (for thin case) and 2.505 km/s (for thick one). The relationship between initial velocity of fragments and ratio C/M for two presented values of $\sqrt{2E}$ have been shown in Fig. 2.

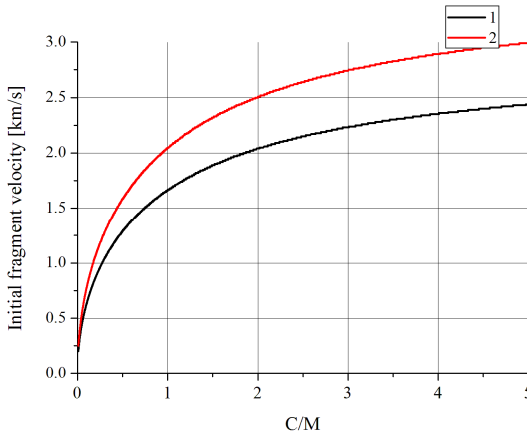


Figure 2. Comparison of initial velocities, predicted making use of Eq. (1) for two values of $\sqrt{2E}$ (1 - 2.039 km/s; 2 - 2.505 km/s), as the function of C/M

Taking into account, that in real conditions the Gurney's assumptions are not satisfied (especially for conditions of projectile's shapes different from cylinder and spheres), in presented work, the results of numerical estimation of fragments velocity produced by explosion of mortar projectile have been shown and compared with results obtained making use of Gurney's formula. This results are treated as the introduction to further works in under consideration area.

2. Numerical model

2.1. Numerical approach

Numerical modeling of extremely dynamic phenomena like materials launching by detonation products needs a special approach. The reason of difficulties during calculations is presence of large deformations (strain) of material, which results in impossibility of application of classical Lagrangian approach well – known in finite element analysis (method fails due to large distortion of elements).

One of the alternative ways in investigations of similar problems is application of meshless methods. Its efficiency was confirmed repeatedly [5]. During performed analyses commercial AUTODYN 3D explicit code was applied. In used software the Smoothed Particle Hydrodynamics (SPH) method was implemented. This approach is the specific case of Lagrangian method, in which classical elements were replaced by particles. Particles represented by points are characterized by so called “smoothing length” and each neighboring particle which is included into “area of interaction” defined by doubled smoothing length, affects the parameters at considered point. The influence of parameters of neighboring particles on parameters at point x_i has been shown in Fig. 3. The kernel function W has non – zero values for distance between “neighboring” particle and considered point is less than $2h$ (where h is the smoothing length).

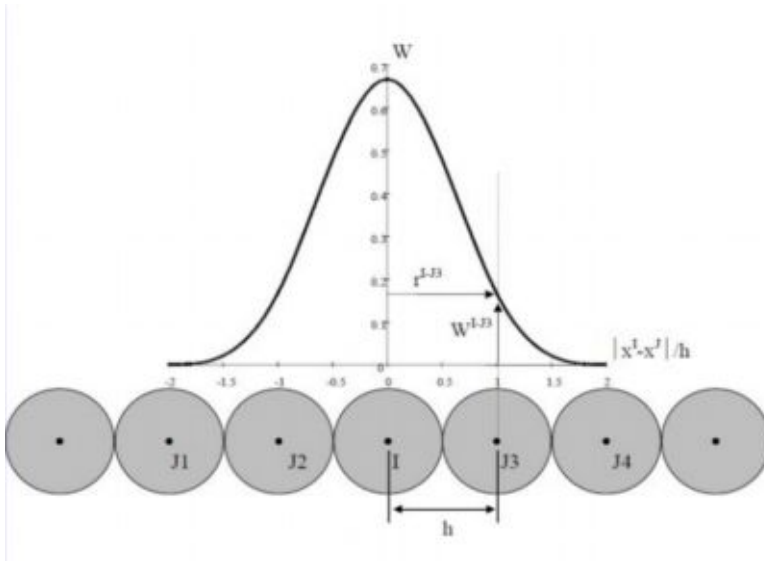


Figure 3. Geometrical representation of smoothing length [6]

The value of each “smoothed” field variable (density, velocity, energy) at the point x_i can be found using the following expression:

$$f_I = \sum_{J=1}^N m_J \frac{f_J}{\rho_J} W(x_J - x_I, h) \quad (2)$$

Using above presented approximation, the equations expressing conservation laws can be evaluated, as done in [7].

Unfortunately, this approach suffers from several disadvantages. The most important are particle inconsistency, inaccuracy at domain boundaries and instabilities at tensile stress state. As can be found in literature, the stability and accuracy of algorithm depends on particles density and sensitivity on this parameter should be analyzed in each case.

2.2. Geometry and material models

In this work, the projectile of 98 mm mortar was investigated. To ensure low computational cost of solution, the quarter of the full 3D model was considered, fulfilled by symmetry conditions. The geometry of under consideration object was shown in the Fig. 4. The whole projectile consists of four main parts: steel casing with fuse, high explosive (TNT) and fins made of aluminum alloy.

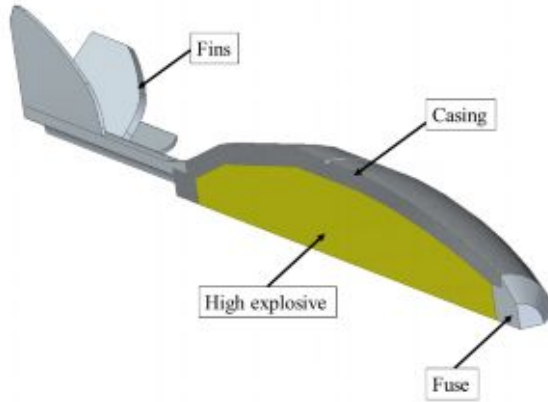


Figure 4. Geometry of investigated system

In order to model the behavior of high explosive, the Jones – Wilkens – Lee (JWL) equation of state was applied. For other materials the linear equation of state and the elastic – plastic material model was used, completed by Johnson – Cook strength and failure models (Johnson – Cook failure model for steel and maximum effective plastic strain failure model for aluminum alloy). Flow criterion was assumed to be in compliance with von Mises hypothesis.

In case of JWL equation of state, the pressure of detonation products is expressed by the following relation [8]:

$$p_{JWL} = A_{JWL} \left(1 - \frac{\omega\eta}{R_1} \right) \exp\left(-\frac{R_1}{\eta} \right) + B_{JWL} \left(1 - \frac{\omega\eta}{R_2} \right) \exp\left(-\frac{R_2}{\eta} \right) + \omega\rho_{DPe} \quad (3)$$

where A_{JWL} , B_{JWL} , R_1 , R_2 and ω are constants obtained in dynamic conditions, $\eta = \rho_{DP}/\rho_{HE}$ (ρ_{DP} – density of detonation products, ρ_{HE} – initial density of HE), e – internal energy of gases.

The linear equation of state, applied for metals, has the following form:

$$p_{Lin} \approx p_0 + K \left(\frac{\rho}{\rho_0} - 1 \right) \quad (4)$$

where K is the bulk modulus, ρ – material density and ρ_0 – initial material density referring to initial pressure p_0 .

Johnson - Cook expression describing dynamic yield stress was assumed as the following:

$$Y = \left[A_{JC} + B_{JC} \varepsilon_p^n \right] \left[1 + C_{JC} \ln \dot{\varepsilon}_p^* \right] \left[1 - T_H^m \right] \quad (5)$$

In above expressions ε_p is the effective plastic strain and $\dot{\varepsilon}_p^*$ is the normalized value of strain rate (divided by reference value $\dot{\varepsilon}_{p\text{ref}}$). Moreover, $T_H = (T - T_{\text{room}}) / (T_{\text{melt}} - T_{\text{room}})$, where T denotes material temperature, T_{melt} is its melting temperature, T_{room} – room temperature. The constants in Eq. (5): A_{JC} , B_{JC} , C_{JC} , n and m , are evaluated using experimental data.

The failure model introduces quantity, which defines level of failure of material:

$$D = \sum \frac{\Delta \varepsilon}{\varepsilon_f} \quad (6)$$

where

$$\varepsilon_f = \left[D_1 + D_2 \exp(D_3 \sigma^*) \right] \left[1 + D_4 \ln \left| \dot{\varepsilon}^* \right| \right] \left[1 + D_5 T^* \right]$$

and D_1 , D_2 , D_3 , D_4 are constants.

For the $D = 1$ material completely fails and, as assumed in calculation, is eroded.

In the Tables 1 and 2, material properties applied in calculations were summarized.

Table 1.

Parameters of models describing high explosive [9].

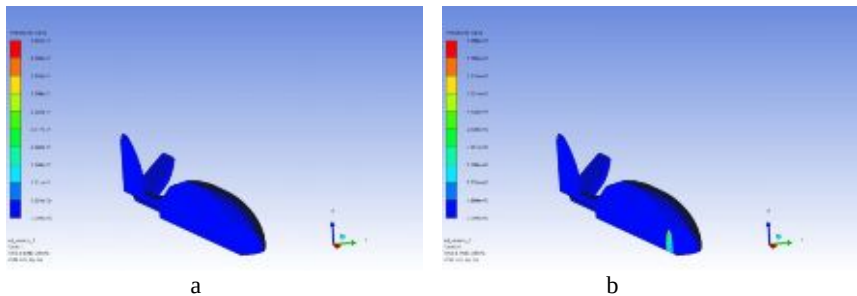
	Parameter	TNT
1	A_{JWL} [GPa]	373.769989
2	B_{JWL} [GPa]	3.747100
3	R_1	4.15
4	R_2	0.9
5	ω	0.35
6	Density of high explosive ρ_{HE} [kg/m ³]	1630
7	C-J pressure p_{CJ} [GPa]	21
8	C-J detonation velocity D_{CJ} [m/s]	6930
9	Energy of explosion e_0 [MJ/m ³]	6000

Table 2.
Parameters of models describing metals [10, 11].

	Parameter	Steel	Aluminum alloy
1	Density ρ_0 [kg/m ³]	7830	2770
2	Bulk modulus K [GPa]	159	70
3	Specific heat λ [J/(kg K)]	477	875
4	Shear modulus μ [GPa]	77	27.6
5	Quasi – static yield stress A_{JC} [MPa]	792	337
6	Hardening constant B_{JC} [MPa]	510	0.343
7	Hardening exponent n	0.26	0.41
8	Strain rate constant C_{JC}	0.014	0.01
9	Thermal softening exponent m	1.03	1
10	Melting temperature T_m [K]	1793	877
11	Reference strain rate $\dot{\epsilon}_{p\ ref}$	1	1
12	Damage constant D_1	0.05	not applied
13	Damage constant D_2	3.44	not applied
14	Damage constant D_3	-2.12	not applied
15	Damage constant D_4	0.002	not applied
16	Damage constant D_5	0.61	not applied
17	Effective plastic strain at failure ϵ^p_{eff}	not applied	0.3

3. Results

As the results of calculations, the pressure distributions and velocity of casing fragments, as the function of time, was obtained. In the Fig. 5, the spatial pressure distribution for several moments were presented. As can be seen, the maximum pressure at the front of detonation wave differs from Chapman – Jouguete pressure about 15 – 20 % (Tab. 1). The reason of this situation is difference between SPH “particles’ density” and thickness of reaction zone in detonation wave – in presented considerations the structure of detonation wave was not investigated. Basing on conducted calculations, can be concluded that acceptable distance between particles, for presented problem, is approximately equal to 1 mm.



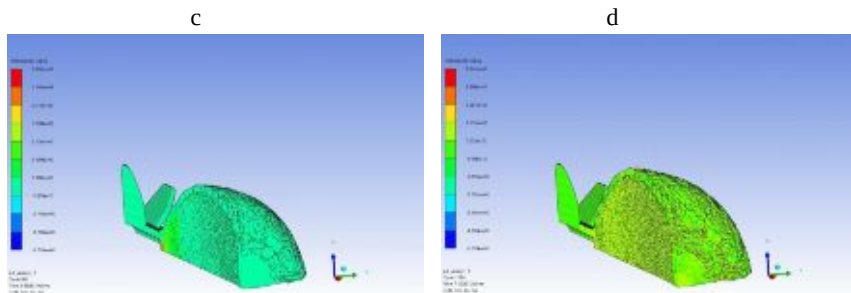


Figure 5. Pressure distribution for several moments of launching process

Moreover, the fragmentation process differs from real situation due to omission of stochastic inhomogeneity of material properties.

In the Fig. 6 the distribution of gauge points for velocity measurements was presented. In the Fig. 7 the velocity components as the function of time were shown. In Fig. 8 the resultant velocity as the function of time was sketched.



Figure 6. The distribution of gauge points on the projectile casing

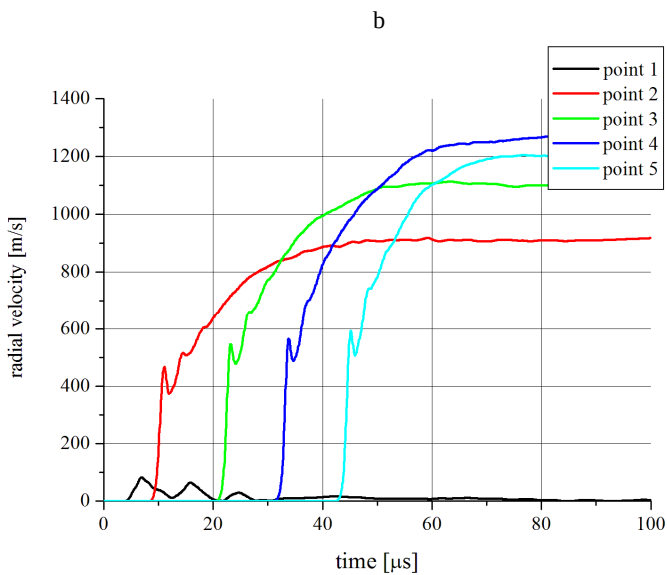
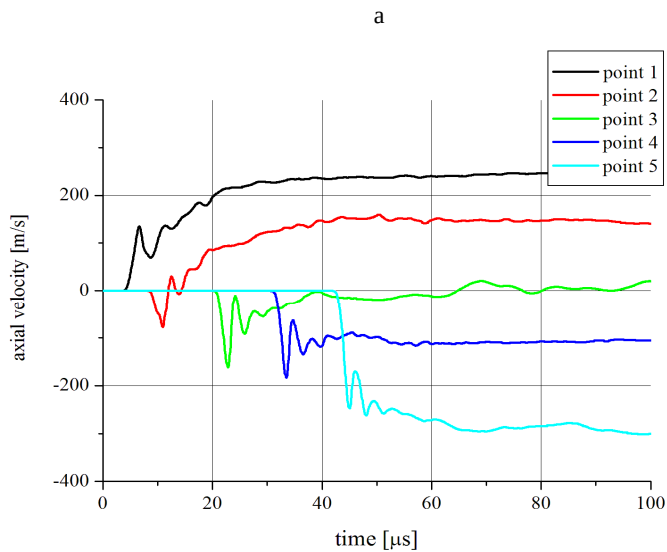


Figure 7. Values of velocity components as the function of time for gauge points

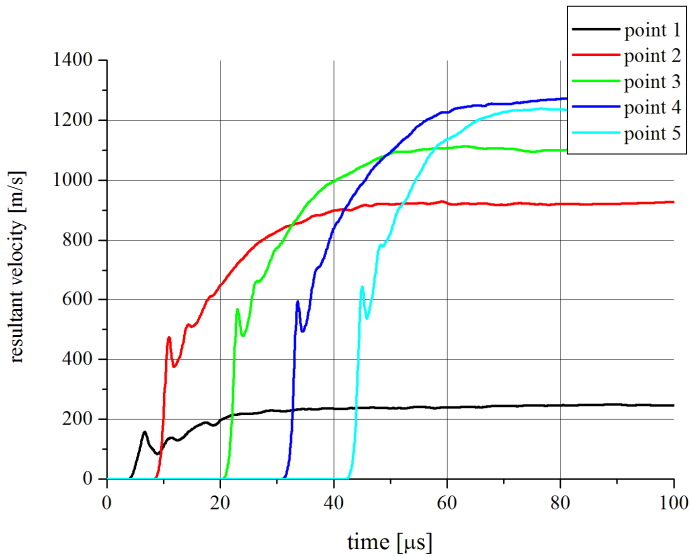


Figure 8. Values of resultant velocity as the function of time for gauge points

In order to compare results of numerical calculations with results of analytical considerations, the obtained values of velocity were summarized in table 3.

Table 3.
Comparison of the Gurney's velocity with the numerical results

Point No.	Estimated value of C/M	Gurney's lower value of velocity [m/s]	Gurney's higher value of velocity [m/s]	Resultant velocity from numerical model [m/s]	Relative discrepancy for lower Gurney's velocity [%]	Relative discrepancy for higher Gurney's velocity [%]
1	0.14	737	906	246	199	268
2	0.23	926	1137	918	1	24
3	0.385	1159	1423	1106	5	29
4	0.385	1159	1423	1265	8	12
5	0.23	926	1137	1199	23	5

Due to small value of casing thickness (approximately 10 mm), the lower value of Gurney's velocity should be taken as the correct value. As can be seen, the largest discrepancy is noticed for the region where the detonation process is not fully developed. The second region of higher values of relative error is the part of the projectile, where the diameter of the HE decreases (concentration of the parameters).

4. Conclusions

The presented results of calculations showed the correctness of applied algorithm and accordance of obtained values with analytical investigations. More serious divergence between these values was observed for the region of detonation development (in the vicinity of fuse) and in part where the diameter of HE changes. At the cylindrical fragment of the casing the relative error of analytical results was less than 10 %. Conducted verification of numerical model allows for further analyses of more complex terminal ballistics phenomena.

References

1. Andrews W. S., Jaansalu K. M., A First Order Method For Estimating Lethal Areas For Fragmenting Munitions, 29th International Symposium on Ballistics, Edinburgh, 2016.
2. Walters W.P., Zukas J.A., Fundamentals of shaped charges, John Wiley and Sons, New York – Chichester – Brisbane – Toronto – Singapore, 1989.
3. Włodarczyk E., Fikus B., The Initial Velocity of a Metal Plate Explosively – Launched from an Open – Faced Sandwich (OFS), Engng. Trans., 64, 3, 2016.
4. Initial Fragment Velocities From Hollow Warheads (U), Navweps Report 8282, U.S. Naval Weapons Evaluation Facility, New Mexico, 1964.
5. Jach K., Computer modeling of dynamic interaction of bodies with free points method (in Polish), PWN, Warsaw, 2001.
6. SPH User Manual & Tutorial, Revision 4.3, ANSYS Inc., Century Dynamics Inc., 2005.
7. Vesenjok M., Ren Z., Application Aspects of the Meshless SPH Method, Journal of the Serbian Society for Computational Mechanics, 1, 1, 2007.
8. www.sharcnet.ca/Software/Ansys/17.0/enus/help/exd_ag/ds_app_mat_models.html
9. Lee E., Finger M., Collins W., JWL Equations of State Coeffs for High Explosives, UCID-16189, 1973.
10. Johnson G.R., Cook W.H., Fracture Characteristics of Three Metals subjected to various strains, strain rates, temperatures and pressures, J. Eng. Mech. Vol. 21, 1985.
11. G.R., Johnson, W.H., Cook, Selected Hugoniot: EOS, LA-4167-MS, 7th Int. Symp. Ballistics., 1969.

Анатолий А. Маслак.

ИЗМЕРЕНИЕ ЛИЧНОСТНЫХ КАЧЕСТВ СТУДЕНТОВ

Анатолий Андреевич Маслак

353566 Россия, Краснодарский край, ул. Запорожская, 96/3-36
53566 Russia, Krasnodar krai, Slavyansk-on-Kuban, str. Zaporozhskaya, 96/3-36
e-mail: anatoliy_maslak@mail.ru, tel. +79094597449

MEASUREMENT OF PERSONAL TRAITS OF STUDENTS

Anatoly Andreyevich Maslak

Аннотация

В рамках теории латентных переменных измерены личностные качества студентов: «уровень тревожности», «уровень коммуникативности», «уровень лидерских качеств», «уровень одиночества». Результаты измерения использованы для сравнения студентов факультетов института на основе этих латентных переменных. Показана статистическая взаимосвязь между измеренными личностными качествами.

Ключевые слова: личностные качества студентов, измерение латентных переменных, статистическая взаимосвязь личностных качеств.

Постановка задачи

Целью исследования является измерение латентных переменных «уровень тревожности», «уровень коммуникативности», «уровень лидерских качеств», «уровень одиночества» у студентов первых курсов СГПИ и студентов, обучавшихся в «Школе лидеров», а также сравнение студентов факультетов на основе результатов измерения латентных переменных.

Качества личности рассматриваются как латентные, то есть скрытые, переменные, которые определяются операционально через наборы индикаторов. Измерение латентных переменных осуществляется с использованием методики измерения на основе модели Раша.

Данные

Для измерения исследуемых качеств личности использовались опросники характеризующие тревожность, коммуникативность, способность быть лидером и ощущение одиночества [1, 2, 5-8].

В опросе принимали участие 474 студента первого курса СГПИ, которые распределены следующим образом:

- факультет математики и информатики – 87 студентов;
- факультет истории и юриспруденции – 30 студентов;
- факультет биологии и химии – 36 студентов;
- факультет иностранных языков – 31 студент;
- факультет ПМНО – 51 студент;
- факультет технологии и предпринимательства – 52 студента;
- факультет физической культуры – 36 студентов;
- факультет филологии – 35 студентов;

- школа лидеров - 116 студентов.

Метод

В качестве программного обеспечения для измерения латентной переменной использовалась диалоговая система RUMM2020 (Rasch Unidimensional Measurement Models) [9].

При анкетировании учитывались следующие факторы - «факультет», «пол» и «возраст» студентов. Для определения значимости фактора использовался дисперсионный анализ.

Необходимо отметить, что значения латентной переменной студентов и индикаторы этой латентной переменной измеряются на одной и той же линейной шкале. Взаимное расположение этих двух наборов переменных для каждой латентной переменной представлено на рисунках 1 - 4.

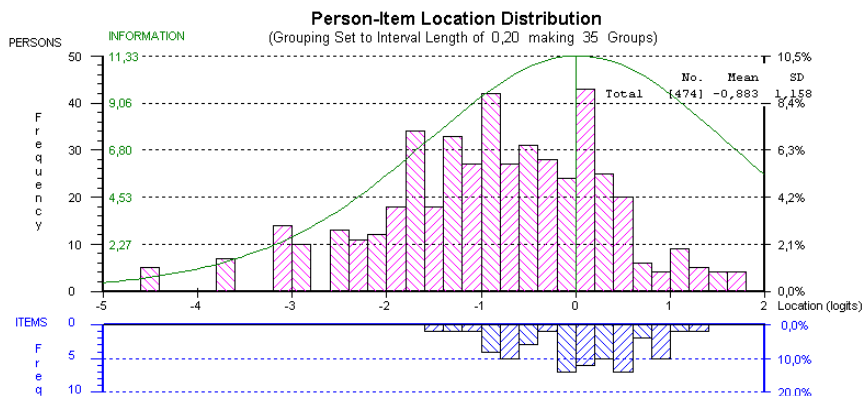


Рис. 1. Соотношение между уровнем тревожности студентов и индикаторов опросника «Шкала проявления тревоги»

Как видно из рис. 1, уровень тревожности испытуемых студентов распределен примерно по нормальному закону. Причем уровень тревожности варьируется в очень больших пределах: от -5 логит до +2 логит. Сами же индикаторные переменные распределены достаточно равномерно. Приведенная в верхней части диаграммы информационная функция свидетельствует о том, что данный набор тестовых заданий адекватен для оценки уровня тревожности большинства студентов.

Как видно из рис. 2, уровень коммуникативности испытуемых студентов также распределен по нормальному закону. Уровень коммуникативности также варьируется в очень больших пределах: от -4 логит до +3 логит. Сами же индикаторные переменные распределены достаточно равномерно. Приведенная в верхней части диаграммы информационная функция свидетельствует о том, что данный набор тестовых заданий адекватен для оценки уровня коммуникативности большинства студентов.

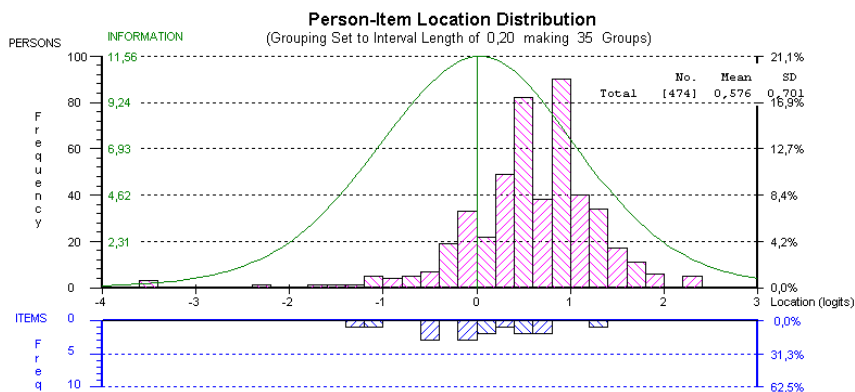


Рис. 2. Соотношение между уровнем коммуникативности студентов и индикаторов опросника «Коммуникативные качества личности»

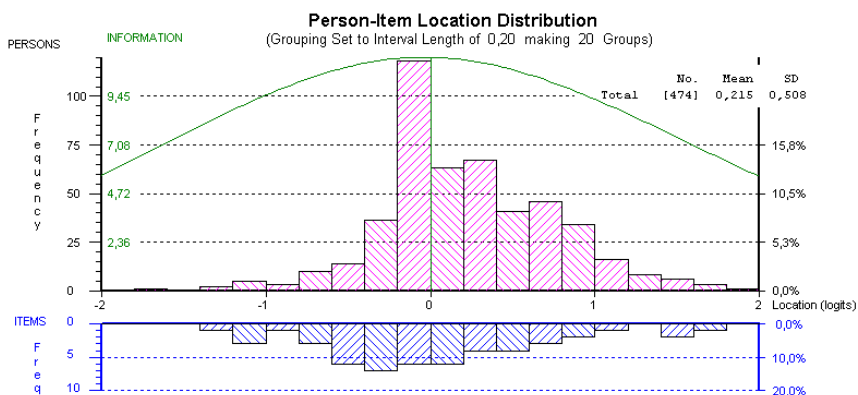


Рис. 3. Соотношение между уровнем лидерских качеств студентов и индикаторами опросника «Организаторские способности личности»

Как видно из рис. 3, уровень организаторских способностей испытуемых студентов распределен примерно по нормальному закону. Причем уровень организаторских способностей варьируется несколько в меньших пределах – всего от -2 логит до +2 логит. Сами же индикаторы распределены достаточно равномерно. Приведенная в верхней части диаграммы информационная функция свидетельствует о том, что данный набор тестовых заданий адекватен для оценки уровня организаторских способностей большинства студентов.

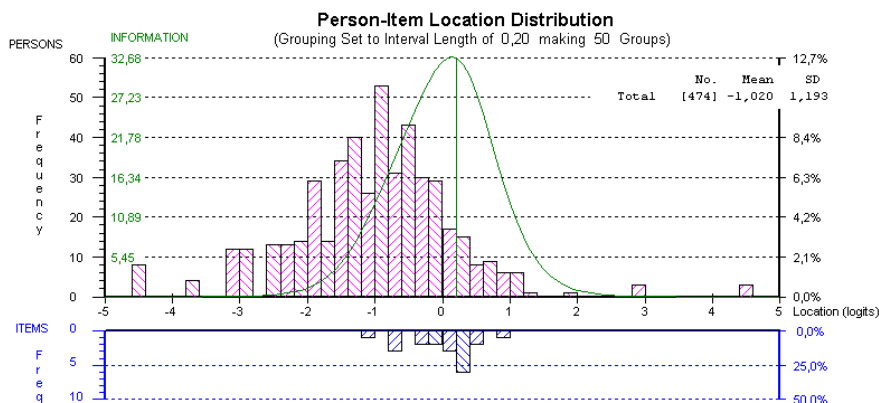


Рис. 4. Соотношение между уровнем одиночества студентов и индикаторами опросника «Шкала одиночества»

Как видно из рис. 4 уровень одиночества испытуемых студентов распределен примерно по равномерному закону. Причем уровень чувства одиночества варьируется в очень больших пределах: от -5 логит до +5 логит. Сами же индикаторы распределены достаточно равномерно. Приведенная в верхней части диаграммы информационная функция свидетельствует о том, что данный набор индикаторов адекватен для оценки уровня субъективного ощущения студентами своего одиночества.

Статистический анализ результатов измерения

Поскольку исследуемый фактор «факультет» является качественным, то в качестве метода статистической обработки результатов измерения всех латентных переменных выбран дисперсионный анализ [3, 4]. Результаты дисперсионного анализа представлены в табл. 1 - 4.

Таблица 1
Уровень тревожности студента в зависимости от факультета

Источник дисперсии	Сумма квадратов	Степени свободы	Средний квадрат	Fэксп	p
Факультет	58,55	8	7,32	5,91	<0,001
Ошибка	575,31	465	1,24		
Всего	633,86	473			

Из табл. 1 видно, что между факультетами существует статистически значимое различие (эмпирический уровень значимости $p < 0,05$). Средние значения уровня тревожности студентов факультетов и школы лидеров (в логитах) приведены в табл. 2.

Таблица 2

Средние значения уровня тревожности студентов

№ п/п	Факультет	Среднее значение	Стандартная ошибка
1	Педагогики и методики начального обучения	-0,361	0,82
2	Филологии	-0,398	0,84
3	Иностранных языков	-0,495	0,86
4	Биологии и химии	-0,577	1,16
5	Технологии и предпринимательства	-0,681	1,25
6	Физической культуры	-0,982	1,01
7	Истории и юриспруденции	-1,037	1,27
8	«Школа Лидеров»	-1,146	1,12
9	Математики и информатики	-1,327	1,28

Из табл. 2 видно, что самый высокий уровень тревожности у студентов факультетов педагогики и методики начального обучения (-0,361 логит), филологии и иностранных языков (-0,398 логит). Наименьшее значение уровня тревожности у студентов факультета математики и информатики (-1,327 логит) и участников «Школы лидеров» (-1,146 логит).

В табл. 3 приведены результаты дисперсионного анализа уровня тревожности студентов в зависимости от факультета.

Таблица 3

Уровень коммуникабельности студента в зависимости от факультета

Источник дисперсии	Сумма квадратов	Степени свободы	Средний квадрат	F-эксп	p
Факультет	20,12	8	2,51	5,50	<0,001
Ошибка	212,57	465	0,46		
Всего	232,69	473			

Как и в предыдущем случае, оказалось, что между исследуемыми факультетами существует статистически значимое различие (эмпирический уровень значимости $p = 0,001 < 0,05$). Средние значения уровня коммуникабельности студентов приведены в табл. 4.

Таблица 4

Средние значения уровня коммуникабельности студентов

№ п/п	Факультет	Среднее значение	Стандартная ошибка
1	«Школа Лидеров»	0,815	0,58
2	Математики и информатики	0,723	0,74
3	Технологии и предпринимательства	0,621	0,70
4	Истории и юриспруденции	0,565	0,55
5	Иностранных языков	0,481	0,42
6	Филологии	0,434	0,34
7	Биологии и химии	0,395	0,67
8	Педагогики и методики начального обучения	0,309	0,51
9	Физической культуры	0,178	1,26

Как и следовало ожидать, наиболее высокий уровень коммуникабельности у участников школы лидеров (0,815 логит) и у студентов факультета математики и информатики. Самый низкий уровень коммуникабельности у студентов факультета физической культуры (0,178 логит) и педагогики и методики начального образования (0,178 логит). В табл. 5 представлены результаты дисперсионного анализа уровня лидерских качеств студентов в зависимости от факультета.

Таблица 5

Уровень лидерских качеств студентов в зависимости от факультета

Источник дисперсии	Сумма квадратов	Степени свободы	Средний квадрат	F-ксп	p
Факультет	13,17	8	1,65	7,03	<0,001
Ошибка	108,80	465	0,23		
Всего	121,97	473			

Из табл. 5 следует, что между факультетами существует значимое различие (эмпирический уровень значимости $p < 0,05$). В табл. 6 приведен уровень лидерских качеств студентов в зависимости от факультета.

Таблица 6

Средние значения уровня лидерских качеств студентов
в зависимости от факультета

№ п/п	Факультет	Среднее значение	Стандартная ошибка
1	«Школа Лидеров»	0,470	0,55
2	Математики и информатики	0,268	0,46
3	Педагогики и методики начального обучения	0,162	0,50
4	Технологии и предпринимательства	0,128	0,45
5	Истории и юриспруденции	0,123	0,35
6	Иностранных языков	0,080	0,54
7	Филологии	0,061	0,49
8	Физической культуры	0,051	0,29
9	Биологии и химии	-0,033	0,53

Как и следовало ожидать, наибольший уровень лидерских качеств оказался у участников «Школы лидеров» (0,470 логит). Наименьшим уровнем организаторских способностей обладают студенты факультета биологии и химии (-0,033 логит) и студенты факультета физической культуры (0,051 логит). В табл. 7 представлены результаты дисперсионного анализа уровня одиночества студентов в зависимости от факультета.

Таблица 7

Уровень ощущения студентами своего одиночества
в зависимости от факультета

Источник дисперсии	Сумма квадратов	Степень свободы	Средний квадрат	F-ксп	p
Факультет	31,10	8	3,89	2,815	0,005
Ошибка	642,23	465	1,38		
Всего	673,33	473			

Из табл. 7 видно, что между исследуемыми факультетами также существует значимая разность и по ощущению своего одиночества (эмпирический уровень значимости $p = 0,005 < 0,05$). Средние значения уровня субъективного ощущения студентом своего одиночества приведены в табл. 8. Наиболее выражено ощущение одиночества у студентов факультета филологии (-0,696 логит), наименее выражено у студентов факультета математики и информатики (-1,337 логит) и у участников «Школы лидеров» (-1,276 логит).

Таблица 8

Средние значения уровня субъективного ощущения студентами своего одиночества

№ п/п	Факультет	Среднее значение	Стандартная ошибка
1	Филологии	-0,696	0,92
2	Биологии и химии	-0,758	1,17
3	Физической культуры	-0,758	1,88
4	Технологии и предпринимательства	-0,759	1,16
5	Педагогики и методики начального обучения	-0,826	0,88
6	Иностранных языков	-0,879	1,03
7	Истории и юриспруденции	-1,038	1,12
8	«Школа Лидеров»	-1,276	1,04
9	Математики и информатики	-1,337	1,28

Представляет интерес выявление статистической взаимосвязи между исследуемыми латентными переменными (табл. 9).

Таблица 9

Коэффициенты корреляции исследуемых латентных переменных

Латентная переменная	Тревожность	Чувство одиночества	Коммуникабельность	Лидерские качества
Тревожность	1	0,528	-0,514	-0,441
Чувство одиночества	0,528	1	-0,581	-0,356
Коммуникабельность	-0,514	-0,581	1	0,385
Лидерские качества	-0,441	-0,356	0,385	1

Результаты корреляционного анализа, приведенные в табл. 9, позволяют структурировать полученные результаты измерений латентных переменных:

- четко выделяются две группы переменных: первую группу составляют «тревожность» и «чувство одиночества», вторую группу – «коммуникативность» и «организаторские способности»;

- латентные переменные «тревожность» и «чувство одиночества» связаны прямопропорциональной зависимостью (коэффициент корреляции равен 0,528);

- латентные переменные «коммуникабельность» и «лидерские качества» также связаны прямопропорциональной зависимостью (коэффициент корреляции равен 0,385);

- между любой парой переменных из выделенных групп существует обратнопропорциональная зависимость.

Выводы

1. Представлены результаты измерения на линейной шкале латентных переменных «уровень тревожности», «уровень коммуникабельности», «уровень лидерских качеств», «уровень одиночества». Необходимо подчеркнуть, что эти латентные переменные определяются операционально – на основе наборов индикаторов.

2. Полученные результаты измерения использованы для сопоставительного анализа личностных качеств студентов, обучавшихся в «Школе лидеров», и студентов первых курсов СГПИ. Полученные результаты измерений обладают достаточно высокой разрешающей способностью: выявлена значимая разность между уровнем качеств личности студентов в зависимости от факультета.

Литература

1. Аванесов В.С., Анисимова Т.С., Маслак А.А., Семенцова О.А., Смирнова Г.И. Педагогические измерения. Тезаурус // Педагогические измерения. 2005. № 1. С. 28-32.
2. Батаршев А.В. Психодиагностика способности к общению, или Как определить организаторские и коммуникативные качества личности.— М.: Гуманит. изд. центр ВЛАДОС, 2001.— 176 с. — (Психология для всех).
3. Гласс Дж., Стэнли Дж. Статистические методы в педагогике и психологии. – М.: Прогресс, 1976. – 496 с.
4. Маркова Е.В., Маслак А.А. Рандомизация и статистический вывод. – М.: Финансы и статистика, 1986. – 208 с.
5. Маслак А.А., Анисимова Т.С., Осипов С.А., Давлетова А.И. Оценка качества опросника для измерения латентной переменной «толерантность» // Оценка эффективности образовательных инноваций и технологий: Материалы Шестой всероссийской научно-практической конференции. – Славянск-на-Кубани: Издательский центр СГПИ, 2004. – С. 25 – 35.
6. Маслак А.А., Поздняков С.А., Киряев К.П. Анализ качества опросника для измерения на линейной шкале уровня коммуникативности участников «зимнего колледжа прогрессивной молодежи» // Теория и практика измерения компетенций и других латентных переменных в образовании Материалы XIII Всероссийской (с международным участием) научно-практической конференции. Ответственный редактор А.А. Маслак. 2010. С. 125-134.
7. Немов Р.С., Практическая психология: Познание себя: Влияние на людей: Пособие для учащихся. – М.: Гуманит. изд. центр ВЛАДОС, 1999. – 320 с.
8. Щебетенко А.И. Тесты для делового человека и для всех. – Пермь: Алгол-Пресс, 1995. – 197 с.
9. Getting Started RUMM 2010. Rasch Unidimensional Measurement Models. – Perth: RUMM Laboratory Ltd, 2001. – 87 p.

GROWING IMPORTANCE OF CYBERSECURITY IN OTHER COUNTRIES

Lt.Col. Bartosz BIERNACIK, PhD Eng.

Bartosz BIERNACIK – b.biernacik@aon.edu.pl;; War Studies University,
al. Gen. Chruściela – Montera 103, 00-910 Warsaw, Poland

Abstract: *Cybersecurity is a grooving issue due to the more and more frequent examples of activity in cyberspace. The growing activity is unfortunately focused on cyber-terrorism, cyber-espionage, cyber hacktivist and more. To make it more complicated cyberspace is the place of almost full anonymity and it is hard to proof the guilty of the exact group or person. That is why plenty of countries are building its abilities to act in cyberspace. Some of them are willing to act only to protect themselves but other are officially declaring also offensive activities. This article is a presentation of current trends in cyberspace in some of the biggest players in it.*

Keywords: *cyberspace, cyber operations, cyber-hacktivist, cybercrime, cyber-terrorism, cyber-espionage, Internet of Thongs.*

Introduction

Cybersecurity has become the most important issue for last few years for the security specialists as a result of growing popularity of the Internet. Nowadays we do not talk about Internet anymore – now we are facing new, bigger, better and more sophisticated version – Internet of Things (IoT). Growing number of items connected with each other gives opportunity for the groups of people that wants to destabilize the situation in some places. Those places can be – group of people, social networks, cities or even countries. This is the problem of growing importance of cyberspace that must be protected by specialists against that kind of activities.

Cybersecurity problems had found respond in plenty of countries in a specialized organizations dealing with cybersecurity issues on a daily basis. This article will provide basic information about them as well as some of the most important for Europe security organizations.

NATO Cooperative Cyber Defense Centre of Excellence

NATO as a military organization is responsible to protect military part of cyberspace of all the member countries. Of course it is not possible to do such a thing by one organization. Therefore in NATO there is an organization named NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) which is the International Organization of the Military. It was accredited by the North Atlantic Council of NATO on 28 October 2008. The center is located in Tallinn, Estonia at the Estonian Battalion stationed Communications.

CCD COE's mission is to improve the capacity and potential of defense cooperation and information sharing among NATO members and their partners in the field of cyber defense through education, research, development, collecting experiences and consultations.

The aim of the CCD COE is to become the main source of knowledge and specialist skills in the area of cyber defense through the collection, production and dissemination of knowledge in this field among NATO members and their partners.

Cyber defense center in Tallinn is one of 21 accredited Centres of Excellence (COES), training for high-tech aspects of NATO operations.

The main tasks of the Centre are:

- improving interoperability within the framework of the Network Enabled Capability (NATO NNEC);
- developing doctrines and teaching methods and the development of concepts and their validation;
- increasing the security of information and education of cyber defense, raising awareness and training in the field of cyber-security;
- providing support for cybersecurity during the experiments / military exercises (including those conducted on the spot);
- analysis of the legal aspects of cyber defense.

The center has also other obligations, which include:

- contribution to the development of practice standards and cyber defense with NATO PfP candidates NATO and non-NATO countries;
- contribution to the development of security policy NATO cyber defense, to define the scope and responsibilities of the military in cyberspace;
- conducting cyber defense training, information campaigns, workshops and courses,
- developing and carrying out defense exercises in cyberspace.

To summarize activity of this organization we may say that this is not an organization that protect physically the cyberspace of NATO countries. It is an organization that co-operate with all of the member countries as well as PfP countries to build better standards and protection of the cyberspace. The responsibility of the active protection is still put on the country level, therefore NATO countries must strongly cooperate and work to build up cyber protection abilities, to avoid cyber-attacks.

European Network and Information Security Agency

The same approach as NATO was defined for other great but this time civilian organization – European Union.

The **European Network and Information Security Agency (ENISA)** is a Centre of Network and Information Security Expertise for the EU, its Member States, the private sector and Europe's citizens.

ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks.

ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Agency produces plenty of documents that are guidelines for civilian national agencies. Its library consist of hundreds' of books defining cyber security issues. It has its own strategy defining planning activity of ENISA. Latest was defined for years 2016-2020 (fig. 1).



Fig.1. ENISA Strategy 2016-2020.

Source: [4]

Agency produces also annual report (fig. 2) that contain main problems of cyber security and list of the biggest and the most important treats for each year (fig. 3).

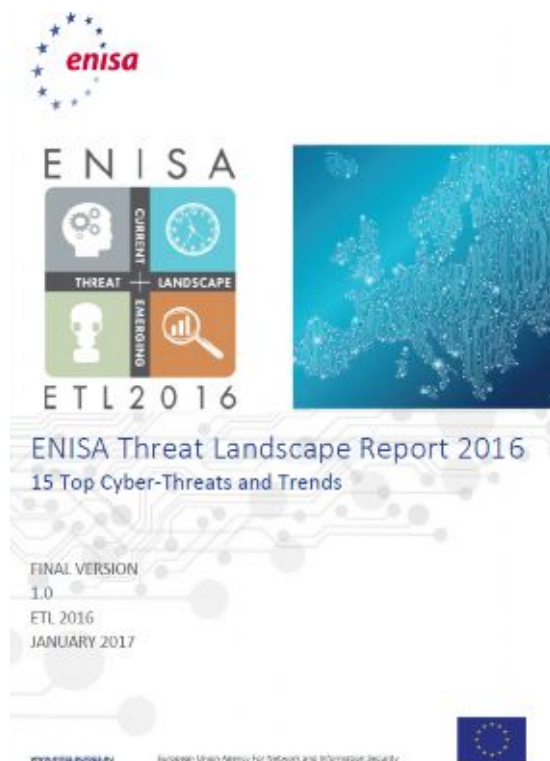


Fig.2. ENISA Annual report – ENISA Threat Landscape Report 2016.
Source: [4]

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware		1. Malware		
2. Web based attacks		2. Web based attacks		
3. Web application attacks		3. Web application attacks		
4. Botnets		4. Denial of service		
5. Denial of service		5. Botnets		
6. Physical damage/theft/loss		6. Phishing		
7. Insider threat (malicious, accidental)		7. Spam		
8. Phishing		8. Ransomware		
9. Spam		9. Insider threat (malicious, accidental)		
10. Exploit kits		10. Physical manipulation/damage/theft/loss		
11. Data breaches		11. Exploit kits		
12. Identity theft		12. Data breaches		
13. Information leakage		13. Identity theft		
14. Ransomware		14. Information leakage		
15. Cyber espionage		15. Cyber espionage		

Legend: Trends:  Declining,  Stable,  Increasing
Ranking:  Going up,  Same,  Going down

Fig.3. Top 15 threats in 2015 and 2016 from ENISA Threat Landscape Report 2016.

Source: [4]

ENISA is also responsible to conduct the exercise for the specialists. Latest – Cyber Europe 2016: was the pan-European exercise to protect EU Infrastructures against coordinated cyber-attack (fig. 4).



Fig.4. ENISA – Cyber Europe.

Source: [5]

The exercise is a flagship activity organized every two years. Realistic scenario is prepared for thousands of experts from all 28 EU Member States, Switzerland and Norway which are facing it this challenge.

Cyber Europe 2016 (CE2016) was the largest and most comprehensive EU cybersecurity exercise to date. This large-scale distributed technical and operational exercise started in April 2016, offering the opportunity for cybersecurity professionals across Europe to analyze complex, innovative and realistic cybersecurity incidents. On 13th and 14th of October ICT and IT security industry experts from more than 300 organizations, including but not limited to: national and governmental cybersecurity agencies, ministries, EU institutions as well as internet and cloud service providers and cybersecurity software and service providers were called upon to mitigate the apex of this six-month long cyber crisis, to ensure business continuity and, ultimately, to safeguard the European Digital Single Market [5]. Cyber Europe 2016 painted a very dark scenario, inspired by events such as the blackout in an European Country over Christmas period and the dependence on technologies manufactured outside the jurisdiction of the European Union. It also features the Internet of Things, drones, cloud computing, innovative exfiltration vectors, mobile malware, ransomware, etc. The exercise was focused on political and economic policies closely related to cybersecurity. This also took into account new processes and cooperation mechanisms contained in the Network and Information Security (NIS) Directive. For the first time, a full scenario had been developed with actors, media coverage, simulated companies and social media, bringing in the public affairs dimension associated with cyber crises, so as to increase realism to a level never seen before in cybersecurity exercises.

The Cyber Europe motto was expression: *stronger together*. Cooperation at all levels is key to the successful mitigation of major, borderless cyber incidents.

ENISA as an EU cybersecurity agency plays a key role in EU cyber preparedness.

The NIS Directive [6] is a major step forward the EU's abilities to deal with large cross border incidents that can lead to such crises. The CSIRT Network established by the Directive, along with work done so far for the EU Cyber Europe cycle, are key in providing decision makers with an overview of the situation and ultimately to respond to such complex threats.

ENISA, the European Commission and the Member States are investing in strengthening of an EU-wide cybersecurity crisis cooperation. The future of cyber crisis man-

agement in Europe - currently planned by the European Commission, concerns the drafting of a cyber crisis cooperation plan and the development of a cyber crisis management platform. ENISA's exercises provide a unique opportunity to test new developments, prepare for the future and develop further the sense of cooperation in the EU.

US CYBERCOM - United States Cyber Command

One of the most advanced in cybersecurity countries are United States of America. They have two main organizations dealing with cyber – NSA (National Security Agency) and US CYBERCOM (United States Cyber Command).

The National Security Agency (NSA) is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence. The NSA is responsible for global monitoring, collection, and processing of information and data for foreign intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT). The NSA is also tasked with the protection of U.S. communications networks and information systems.[1][3] The NSA relies on a variety of measures to accomplish its mission, the majority of which are clandestine.[4].

As part of the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD 54), signed on January 8, 2008, by President Bush, the NSA became the lead agency to monitor and protect all of the federal government's computer networks from cyber-terrorism.[3].

The second organization, dealing with cyberspace is one of the largest Cybernetic Army in the world, the Army of the United States, which has, consisting of:

- Army Cyber Command/2nd Army;
- The Network Technology Command/9th Signal Command Army (NET-COM);
- The 1st Information Operations Command Land (1st IO Command);
- The U.S. Intelligence and Security Command (INSCOM).

US CYBERCOM combines the full spectrum of operations the cyber US Department of Defense, plans, coordinates, integrates, synchronizes and implements the defense and protection of information networks Department of Defense (DoD), coordinates the operations of the DoD to support military missions by management networks for the themselves. Prepares, manages and runs the entire range of military operations in cyberspace. Command uses currently owned power and resources by building structures of cooperation and synchronizing effects of combat operations to combat threats in cyberspace.

USCYBERCOM combines the full spectrum of operations the cyber US Department of Defense (DoD), plans, coordinates, integrates, synchronizes and implements the defense and protection of information networks DoD, coordinates the operations of the DoD to support military missions by management networks. Prepares, manages and runs the entire range of military operations in cyberspace.

Command uses currently owned power and resources by building structures of cooperation and synchronizing effects of combat operations to combat threats in cyberspace.

The Americans intend to Create a fully developed forces to act in cyberspace (up to 2018) – Cyber Mission Force (CMF).

CMF is planned to have 133 specialized teams of protection, which are the first line of defense of the state against any threats in the sphere of cyber hacktivists, relating both to the activities of third countries, companies and individuals.

It is estimated that the number of these forces CMF will eventually be 6,200 US military and civilian operators. The process of preparing and equipping the necessary hardware facilities began in 2013.

So far, the United States can boast of 3100 the operators of this type, coming from the four branches of the military.

They operate in the existing 58 teams.

Until recently determined role of CMF is a three element as a set of tasks related to security, first of all, the Department of Defense, secondly, in the broad sense of the United States and the activities carried out for the needs of the individual commands combat.

According to the plan:

- 13 teams is to focus the defense of the United States and used by the state of critical infrastructure, susceptible to all kinds of cyber threats;
- 68 teams are directly responsible for the protection of the Department of Defense and its networks, which are targeted by foreign and American hackers;
- 27 teams are responsible for offensive part, subordinated, every day, commanders of combat;
- 25 teams - facilities and support, especially in the field of analytics for these teams to be another.

US DoD in the doctrine of Joint Publication 3-12 (fig. 5). Cyberspace Operations presented the principles of planning, preparation, conduct and evaluation of operations in cyberspace.

This document presents the operational activities in cyberspace at all levels of command and control.

Defined concepts, task areas and identifies relationships and connections in the combined operations conducted with the use of elements in the fight cyberspace.

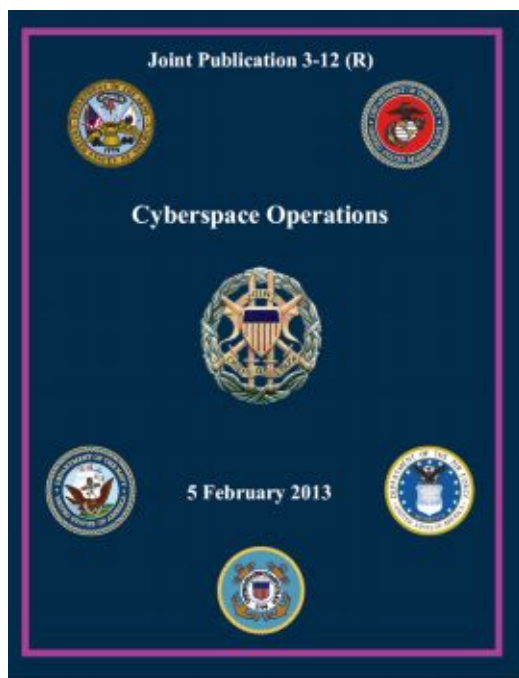


Fig.5. JP 3-12 (R) from 5th February 2013.

Source: [12]

Another very important document for the US is the latest Cyber Strategy (fig. 6) from April 2015 in which for the first time US officially confirm will of active offensive activities in cyberspace to protect America against the enemy.

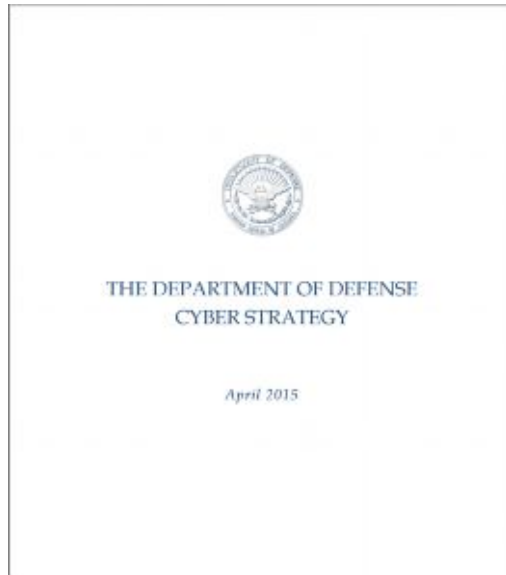


Fig.6. Cyber Strategy from April 2015.

Source: [2]

The Department of Defense Cyber Strategy 2015 defines 5 main goals:

- build and maintain ready forces and capabilities to conduct cyberspace operations;
- defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
- be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
- build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
- build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Great Britain activity

In 2010, Great Britain started to operate two cells involved in cyber security:

1. **Officer of Cyber Security (OCS)**, which conducts strategic consultancy in the field of cyber security for the UK government and is responsible for the creation and supervision of the government program for achieving strategic priorities of cyber security.

2. **Cyber Security Operations Center (CSOC)**, which has the task of monitoring and ensuring cyber security and incident response directed against users and data communications networks in the UK, as well as advising and informing about the dangers of both in the sphere of business and the public.

Great Britain has also developed its own cyber security (fig. 7).

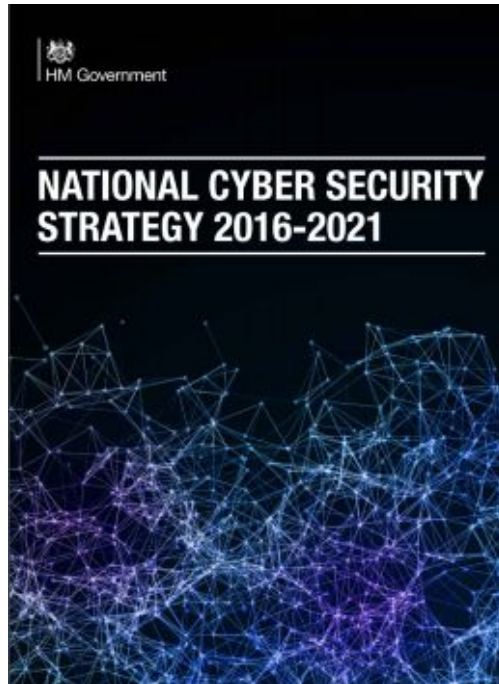


Fig.7. National Cyber Strategy 2016-2021.

Source: [13]

Germany activity

In Germany there are two main offices responsible for cybersecurity. Construction of the offices are similar to solutions made in Great Britain. One of them is **National Cyber Defense Center**.

NCDC in Germany is operating under the Federal Ministry of Internal Affairs since 16th June 2011 with the task of creating better safety standards and procedures for defense in the area of cyberspace for both the private and the state sector.

Center serves as a common platform for the rapid exchange of information and coordination of activities against the security event information.

The mission of the Center for cyber defense in Germany is quick and comprehensive assessment of security incidents in order to develop recommendations and a coordinated response.

To achieve this goal, it organizes the collection and analysis of information about vulnerabilities in the products and results of the analysis of security incidents and attacks, as well as proposals for protective orders.

The second organization is planned to be created a **National Cyber Security Council** acting under the auspices of advisors for German Chancellor dedicated to the ICT matters, with the tasks of securing the flow of information between government, industry, safety authorities, telecommunication companies.

The main tasks of these entities is to collect information and data concerning Internet security and to provide decision-makers with expertise in the management of IT security.

In addition, it was decided to create a powerful cell counterintelligence dedicated exclusively fending off attacks on government servers. The Federal Intelligence Service (BND) conducts a large-scale recruitment of new intelligence officers. Instead, agents are looking for the best computer scientists who specialize in the field of security.

Russian Federation

This article could not miss the second huge player in cyberspace, which open the Russian Armed Forces.

They build their own digital shield to protect against cyber threats. The Russian Ministry of Defense is planning in 2017, complete the creation of a special body whose main task will be to protect critical facilities of the Russian armed forces from hackers.

In Russia for a long time, there are cell information security and combating organized cybercrime. The structure has a FSB (Federal Security Service), which is to fight cyberterrorism in the channels public communications networks in the preparation of terrorist acts.

Russia had implemented its own security strategy (fig. 8).

Russian National Security Strategy, December 2015 – Full-text Translation

[Text of 31 December Russian Federation Presidential Edict 683 approving appended text of "The Russian Federation's National Security Strategy"]

EDICT OF THE RUSSIAN FEDERATION PRESIDENT

On the Russian Federation's National Security Strategy

In accordance with Federal Laws 390-FZ "On Security" dated 28 December 2010 and 172-FZ "On Strategic Planning in the Russian Federation" dated 28 June 2014, I decree:

1. The attached Russian Federation's National Security Strategy is to be approved.
2. The following are to be deemed no longer valid:

Russian Federation Presidential Edict 537 dated 12 May 2009 "On the Russian Federation's National Security Strategy Through 2020" (*Sobraniye zakonodatelstva Rossiyskoy Federatsii*, 2009, No. 20, Item 2444;

Point 27 of Attachment 1 to Russian Federation Presidential Edict 483 dated 1 July 2014 "On Amending and Deeming No Longer Valid Certain Acts of the Russian Federation President" (*Sobraniye zakonodatelstva Rossiyskoy Federatsii*, 2014, No. 27, Item 3754).

3. This Edict comes into force from its date of signing.

[Signed] Russian Federation President V. Putin

Moscow, the Kremlin

31 December 2015

No. 683

APPROVED by Russian Federation Presidential Edict 683 Dated 31 December 2015

Fig.8. Russia National Security Strategy from December 2015.

Source: [14]

China

Another example of countries are the most active and aggressive China, which officially confirmed the creation of cyber troops May 25, 2011, They are part of the Chinese People's Army - Liberation.

The creation of so-called. Blue Fighter Army spent probably about \$ 1.5 million. The main activity of this elite unit is "defending the interests of government and business in cyberspace China."

Currently, the unit has been included in the structure of the Military Command Center in the Chinese province Guangdong the south of the country.

In addition, within the framework of the reform of the Chinese army, created a new unit to specialize, among others, in hostilities on the Internet and cyber espionage.

Strategic Assistance Force (SSF) are to ensure that the Chinese army will be able to make the Internet more efficient and more advanced offensive and reconnaissance.

It also has to protect the government against cyber-attacks. The unit consists of three parts. The first is the "soldiers - hackers" responsible for cyber-attacks and cyber defense. The second will deal with military operations in space, focusing on reconnaissance and satellite navigation. The third is to deal with the conduct of the war in the network. It also has to interfere with the operation of the devices radar and communication opponent. The unit also has the use of civilian technology: cloud computing, artificial intelligence and nanotechnology.

North Korea

North Korean regime has created a team of approx. 3000 cyber warriors whose task is to build a network of support for state authorities, and above all for Kim Jong-un, as well as spreading among Internet southern properly crafted propaganda.

It has to be done using the comments placed on South Korean websites. The North Korean cyber unit includes, among others 200 agents with writing online comments aimed at southern neighbor.

The purpose of propaganda is to demoralize the enemy and to help in the task they have stolen from the South Koreans virtual identity.

Propaganda is promoted by using hosted 140 sites in 19 countries.

North Korea educates its cyber specialists in elite schools in Pyongyang, and the most aptitude hackers are then directed to the 10-year training in the Military Academy Kim Il Sung and other universities.

Only in June 2013 Cyborg Soldier regime blocked 65 South Korean websites, stole the data of 2.5 million members of the ruling in the Seoul Grand National Party, 300 thousand military and 200 thousand site users belonging to the president of South Korea.

South Korean military intelligence claims that North Korea has recently doubled from three to six thousand numbers of their "cyber forces" - special formations dealing with hacker attacks.

The task of the "Office 121" as the name of this unit is to attack targets in South Korea. As for interfering with the functioning of the South Korean armed forces, the government's work, calling the "psychological shock", causing "physical and psychological paralysis" of the South (the information the Defence Ministry in Seoul).

Probably, the "121 Office" has for years been expanded by the North Korean military intelligence. They work there the most talented computer experts. From the information provided by defectors from North Korea that "Office 121" can plan the attack, including a telecommunications facilities and power network in South Korea.

In 2013, Seoul accused North Korea of hacker attacks on computer systems of South Korean banks and broadcasters.

At the end of November 2013 Sony Pictures was the victim of cyber-attack, which the FBI was derived from North Korea.

The attack was connected with plans to introduce released comedy "The Interview" about a fictional plot to kill North Korean leader Kim Jong-un.

Following the threats of hackers Sony Pictures canceled shows, but soon after changed its position and the film was to hundreds of American cinema, and has been in the United States available online for a fee and cable networks in the context of video on demand.

Pyongyang denies it was behind the attack.

Summary

To summarize we have to mention again that nowadays we are living in the environment that is strongly connected with IT technologies and transformation of the Internet into Internet of Things is a fact. The fact is also that all of this is in the cyberspace which is growing issue for the whole Europe and most of the world.

The European ICT Industry is one of the most advanced in the world. Making the EU's single market fit for the digital age could contribute €415 billion per year to our

economy and create hundreds of thousands of new jobs. The pervasiveness of high-speed connectivity and the richness and quality of online services in the European Union are among the best globally. Such advantages have considerably increased the dependability of European citizens on ICT services. These two elements, quality of services and customer base, make this industry particularly appealing to global business. What if this important piece of the global economy becomes a target? Computer security attacks are increasingly used to perform industrial reconnaissance, lead disinformation campaigns, manipulate stock markets, leak sensitive information, tamper with customer data, sabotage critical infrastructures [5].

Problems of cybersecurity are growing nowadays and they will become the most important issue in near future. Future war fight will (rather already common war fight) are to be conducted in cyberspace. Cost of the operation in cyberspace is much lower than use of armed forces – and it is hard to prove who is guilty and who conducted the attack... Disruption in the economy of the attacked country is much bigger by using cyberspace rather than traditional forces.

Therefore we must as an European Countries try to do our best to improve our cybersecurity capabilities and prepare ourselves to conduct full spectrum of activities in cyberspace: defense as well as offensive operations.

Bibliography

1. "About NSA: Mission". National Security Agency. Retrieved September 14, 2014.
2. Cyber Strategy, (PDF File).
3. Ellen Nakashima (January 26, 2008). "Bush Order Expands Network Monitoring: Executive Order 13470 – 2008 Amendments to Executive Order 12333, United States.
4. https://www.enisa.europa.eu/publications#c5=2007&c5=2017&c5=false&c2=publicationDate&reversed=on&b_start=0.
5. <https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016>
6. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>
7. <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-role-in-the-european-digital-single-market-dsm>
8. <https://www.enisa.europa.eu>
9. https://en.wikipedia.org/wiki/National_Security_Agency#Mission
10. "Intelligence Agencies to Track Intrusions". The Washington Post. Retrieved February 9, 2008.
11. "Intelligence Activities, July 30, 2008 (PDF)
12. JP 3-12 (R), Cyberspace Operations (PDF File).
13. National Cyber Strategy 2016-2021 (PDF File).
14. Russia National Security Strategy. December 2015. (PDF File).

DEFENSE AND SECURITY

Krystian Frąciak,

POLISH SPECIAL OPERATION FORCES - DIRECTIONS OF DEVELOPMENT

LTC Krystian FRĄCIK, Ph.D.

Assistant professor,
Chief of Special Forces and Airborne Branch,
War Studies University, Warsaw

The use of advanced technology troops and combat undoubtedly will force changes in the terms and manner of execution of modern military operations. The process of implementation of modern automated systems of command, reconnaissance or destruction points to the ever increasing in today's battlefield importance of technical solutions and information technology. These factors, often now raised to the rank of the principles of war art, decide to obtaining an advantage, both informative and quality. Therefore, to achieve and maintain the advantage of modern weapons systems must be characterized by certain properties and combat capability commensurate with the challenges of modern multi-dimensional battlefield.

The effect of introducing new combat measures is to seek ways to best use. Among the key directions of development stands out among others the development of the concept of network operations. Generally seeks to combine the various combat platforms, both manned and unmanned as a single system. At the same time large scale systems are deployed soldier's individual equipment.

The paper presents the directions of development and degree of implementation of changes in the equipment subunits of Special Operations Forces (SOF) and the impact of new technologies on the capabilities and performance of combat tasks. Presenting the issues and concepts of the capacity of the soldier, infantry equipment, limiting the contribution of aspects of human factors in combat through the use of Unmanned Air Systems. The development also raises topics implementation of network data exchange systems and the related expected changes in the rules for the implementation of combat operations.

INTRODUCTION

Technical and scientific progress, new technologies, political and social changes in the world early twenty-first century functioning reevaluate assumptions and rules of conducting military operations and the need to enforce their fundamental overhaul.

Technological development and equipping of troops in the increasingly sophisticated means of destruction and transportation contribute to a change of views on the conduct of modern military operations. The most characteristic features of the modern battlefield include: a large increase maneuverability and fire power of troops, the dynamics of action and rapid change in the situation, increasing the possibility of impact on the full

depth of the combat structure, a quick transition from one struggle to another and the strong desire to gain and maintain the initiative. This highlights the dynamic and highly maneuvering nature of modern military operations.

Although due to the currently reigning in the world crisis in most countries is limited to expenditures for the modernization of army, that fact does not mean that they intend to resign from the key programs, developing new technologies and means of struggle.

In theory and practice more and there are new concepts for conducting military operations, are developed technologies and means of fighting, the growing importance of unmanned platforms and precision of destruction. These conditions indicate that based on current knowledge, including the issue of conducting military operations, there are many reasons to make inspiring multifaceted analysis, evaluation and identification of current status and determine the forecast changes.

Alignment with the conduct of military operations to modern battlefield conditions, new challenges and to maintain readiness to respond to new threats can be, inter alia, by implementing innovative techniques and technologies and the continual transformation of the armed forces. Indeed, they should still be characterized by high levels of mobility, technology and military equipment combat and have integrated automated systems of command, reconnaissance and logistical support. Integration and synergy of this type, interoperable systems of different types of troops and the armed forces, allows the efficient use of potential and combat capability.

Among the key directions of development of future systems is observed, inter alia, the implementation of the system equipment infantry soldier, the introduction of large-scale unmanned combat platforms, unmanned air vehicles (UAV) or lighter combat vehicles and robots. The equipment of the armed forces appear active measures to combat in space, which already can not be reduced only to the three basic dimensions, such as length, width and height. There is in fact another dimension in the form of information space, only a limited capability devices in the speed of digital data, voice or image.

Hypothetical predictions of changes indicate the need for modifying existing today, the concept of conducting military operations. In the unanimous opinion of many military theorists, in the foreseeable future activities will be conducted under conditions defined as network-centric environment. The emergence and development of the concept of acting in an network-centric environment been forced changes taking place mainly in the world of information technology and the growing importance of information as a factor which plays a unique role in contemporary armed conflicts. Development of the concept of network activity causes already at the lowest levels it seeks to combine a variety of platforms, both manned and unmanned as a single system - in one network.

The process of implementation of modern automated systems of command, reconnaissance or destruction points to the ever increasing in today's battlefield importance of technical solutions and information technology. These factors, often now raised to the rank of the principles of martial arts, decide to obtaining an advantage, both informative and quality. Therefore, to achieve and maintain the advantage of principles of conducting military operations should be characterized by certain properties commensurate with the challenges of modern multidimensional combat environment.

DETERMINANTS OF TECHNOLOGICAL CHANGES AND THE IMPLEMENTATION OF THE NEW MEANS OF COMBAT

Dynamically changing external conditions and internal state security system carries a number of challenges, including new risks with asymmetry and unpredictability create a new environment of military action. The conditions most characteristic features of contemporary conflict is the unpredictability of possible measures of size, time and place of its occurrence. Modern military operations are usually asymmetric and often blur the current distinction between internal and external security of the state. Today's armed forces often have to undertake tasks that go beyond their traditional missions¹.

These factors resulted in the greatly expanded the range of activities for which military forces are involved.

Analyzing the principles of conducting modern military operations, indicates that one of the main environments in which they are held in urban areas. The result is that because of limits on the effective use of heavy equipment, the main effort of its own activities rests with the infantry soldiers. There is therefore a need to provide them the best conditions for the tasks, mainly by equipping them with adequate equipment and weapons that will enable achievement of the objective measures with the least losses. Another argument for the implementation of the armed forces of modern technology is the use of civilians by the media to unfettered access to information about their activities, and thus maintaining an acceptable level by policymakers personnel losses. Public opinion forces the fact that losses among their own troops, as well as among the enemy civilian population to be minimized. This phenomenon necessitates the need for the soldier to the highest possible degree of protection and security.

Another determinant for enforcement need to modernize equipment a soldier is to advance information technology and telecommunications, which contributed significantly to the emergence of the concept of network operations. An element of this concept was created in the U.S.A the future combat system - *Future Combat System* - whose key element is to be the soldier along with his entire equipment and weapons.

In summary, the above factors resulted in the need for soldiers and information technological advantage by equipping them with the means of providing them the best opportunity for detection, identification and destruction enemy ballistic better protection, better conditions for the implementation of tasks, appropriate mobility, and above all understood as situational awareness, knowledge the action area (environment) and the location, operation, and the enemy's intentions, as well as its own forces. It being assumed that situational awareness is the soldier had seen as part of an information network, with the consequence will be equipped with equipment that allows him to communicate and exchange data with other elements of this network.

CONCEPTS OF INDIVIDUAL EQUIPMENT SOF

The scope of tasks performed by the soldiers forced the need to adapt their individual weapons and equipment to the nature of the mission performed.

Observing the development of systems concepts and technologies for individual soldier equipment, could be tempted to say that one of the most advanced systems, is American system - *Land Warrior*. The work and development - research started in 1990 when

¹ A. Topik, *Terroryzm i broń masowego rażenia w polityce NATO*, Zeszyty Naukowe AON 2003, nr 1(50)A, page 11.

it approved by the United States Armed Forces of the project identified the essential requirements for the future soldier and his equipment, and development trends. The idea of this concept was:

- provide infantry soldiers increased situational awareness;
- providing free communication and exchange of information between them and the elements of superiors;
- increase combat capabilities;
- vitality and soldier survivability.

Requirements for the new system are set out in five key areas:

- **vitality:** providing increased opportunities for observation in day and night conditions, to locate, identify, classify, identify and destroy enemy in every situation;
- **mobility:** reducing weight of equipment while ensuring increased combat capabilities, compatibility in the activities performed by different types of troops (airborne troops, air-assault, mechanized, and special forces);
- **survivability:** providing protection against direct fire, small arms, landmines and incendiary weapons, and also provide protection against the effects of the use of nuclear, biological, chemical, high-power microwave and directed energy. In addition, to provide hearing protection, prevention, disruption, or confuse the enemy detection system, warning devices provide a variety of threats present on the battlefield, providing high durability protective equipment, as well as supporting the sense of peripheral vision, hearing and touch;
- **command and control:** providing voice communication, including the exchange of confidential data, images, digital maps, graphics display, transmit and receive the location of the object, providing situational awareness and data concerning the current situation in the combat operations conducted;
- **maintenance of a soldier on the battlefield:** providing logistical support in the supply of energy resources supply (batteries), water, food and ammunition.

The Land Warrior Initial Capability system (LW-IC), consists of the following subsystems:

- **armament subsystem:** it means: 5.56 mm M-4 rifle (a lighter version of the assault rifle M-16), thermal sight (called Thermal Weapons Sight - TWS), a video camera (called Daylight Video Scope - DVS), and a device consisting of a laser rangefinder and a digital compass (Laser Rangefinder English/Digital Compass - LRF/DC) and azimuth determining the distance to the target. In conjunction with its location indicated on the GPS can pinpoint the location of this end, for the submission of the report about the situation for the purpose of fighting or fire support artillery fire during the call on fire.
- **integrated helmet:** consists of a helmet made from ballistic material, providing cover. On a helmet mounted display is connected electronically with other subsystems and with the master system in the network command. The display has a soldier graphic data, digital maps, reconnaissance information, location of other soldiers, as well as images of weapons mounted on the viewfinder and the camera daytime thermal image. This allows to keep fire from behind the corner of a building or obstacle. Foreland to observe through the viewfinder provides faster thermal capture distant, faint, characteristic features of the terrain and enemy positions, including in the event of smoke or other factors impair visibility.

- **subsystem of uniforms and personal protective equipment:** consists of a frame with a modern design, respectively, arching her body to move the backpack of a soldier and individual equipment attached to the frame. Included in the subsystem have improved ballistic shield plates for better protection against small arms. In addition, the equipment includes: protective clothing against biological impacts, gloves, boots and optional detector of weapons of mass destruction.



Based on: www.army-technology.com (2011.09.13)

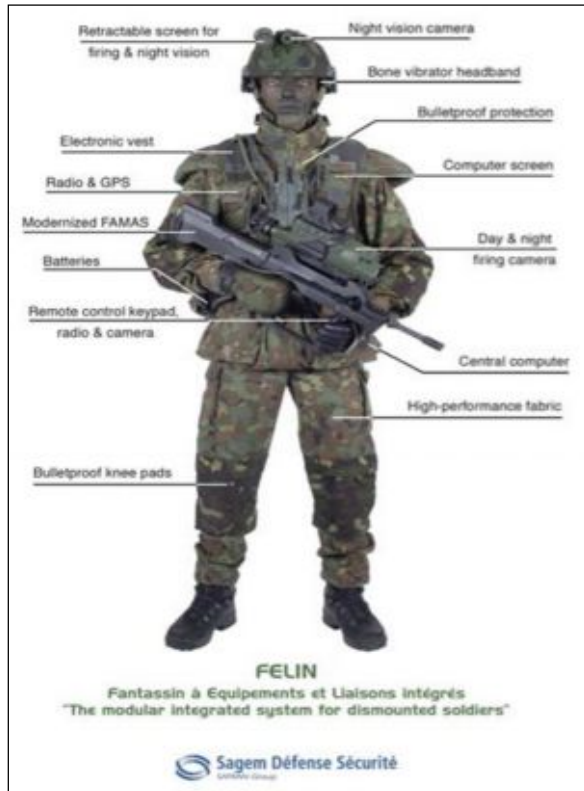
Land Warrior-Initial Capability system

- **PC module integrated with the radio:** characterized by a manual manipulator connected to the computer module. The manipulator is mounted on the breast of the soldier and acts like a computer mouse, and thanks to him, the soldier can change the displayed images, control buttons on the radio, change frequencies and send digital data. Some functions can be controlled via two buttons on the language of the gun trigger, allowing the soldier to keep weapons in combat position. Integration of GPS with a computer tenant has eliminated the need for a separate display and switches. CRS subsystem has an open architecture which allows for future conversion of both the software and components for later.

When the U.S.A. was working on a project of its Land Warrior system with a similar fate also began to develop the French engineers, who launched the project Feline (fr. *Fantassin a Equipement et Liaisons Integrees*).

FELINE system is a modular, with open architecture, which enables the use of specific modules, depending on conditions (in the day, at night, during acceleration or driving in the armored vehicle, flying plane, as well as during operations in urban areas, rural or open). Modular design is to allow the matching of equipment to the nature of the task

and to eliminate unnecessary burdens while maintaining the best possible protection. Uniforms are designed so as to not interfere with the natural movements performed during the movement of the soldier. The material is flame retardant uniforms, but also provides good ventilation and comfort measures at different temperatures. Optional equipment also protects the weapons of mass destruction. Large areas of the body are protected by soft ballistic materials, reinforced in places subject to wear, ceramic inserts. Special goggles, retractable inside the helmet, shield you from eyes that could blind him laser beam.



Based on promotional materials of SAGEM
FELIN system

The system offers configurations adapted to their functions, such as platoon leader, squad leader, sniper, machine gun sight or others. The architecture of the system can support different software versions, chosen for specific missions and tasks of soldiers - such as specialized programs for platoon leaders, snipers, anti-tank weapons handling. The system includes five following modules:

- vitality:
 - day-night sights for enhanced image;
 - control system components via buttons on the handles of weapons;
 - observation and maintenance of fire with the camera (mounted on the weapon) without tilting the body around the corner of a building or other object;
- mobility:
 - ergonomics of the system;
 - use of GPS tracking (positioning) of all units (soldiers) in the vicinity;
 - enhanced image sighting devices;
- C4I:
 - individual radio station with the possibility to exchange voice and digital transmission;
 - osteofon;
 - configuration of network radio and digital battlefield;
 - situational awareness closer to the real time;
- protection:
 - ballistic;
 - NBC;
 - against the negative factors of climate;
- power supply:
 - lithium-ion batteries;
 - portable and on-board charger;
 - sets for system integration with the vehicle.

Units equipped with FELINE have an element of the French system of network-centric information exchange *Bulle Opérationnelle Aéroterrestre* - BOA, whose purpose is to integrate various fighting systems of SOF and air component. It is assumed that the system will be integrated with vehicles, now considered a 8x8 VBCI infantry transporter, whose first models produced by Giat Industries in collaboration with Renault are in a testing phase. By the end of 2008 in a system equipped vehicles sixth Light Armored Brigade and the 2nd Armored Brigade. Plans call for installing the system on conveyances VBCI, combat infantry, chariots, and AMX-10P AMX-56 tanks Leclerc.

A little later the French design work on the weapons and equipment of the individual soldier, the British began. They proposed project *FIST* (Future Integrated Soldier Technology) and its subsequent variants V1 and V2.

Like other systems, the *FIST* system is a modular system that allows for the modernization of the individual components, depending on the tasks. The *FIST* V2 highlights five key components identified as:

- C4I - subsystem command, control, communications, computing and reconnaissance,
- vitality: arming devices with foresights,
- mobility: depends on the navigation, and the size and weight of equipment a soldier;
- viability: uniform, stealth technology, ballistic protection;
- maintenance: problems of logistics.

FIST communications system is to be provided to the company level. With higher levels has to be performed through an integrated communication system *BOWMAN*.

It is anticipated that each soldier will have a coded radio allows short-range communication between soldiers subunit. Sub-unit commander will have the ability to com-

municate with your supervisor or base (e.g. during patrol). Voice and digital data can be transmitted directly to the soldiers, or through communications with Headquarters relationships, which in turn may transmit the command, and have the information and images obtained from the observation posts, from other soldiers, unmanned air vehicles, sensors and remote-controlled by the assault reconnaissance aircraft or satellites.



Based on : <http://www.army-technology.com/projects/fist/fist1>. (2011.09.13)

FIST system

It is assumed that the soldier will be equipped with GPS, inertial navigation unit and a digital map depicted on the monitor display mounted on the helmet, or wrist, as well as the laptop managing the entire system. Thanks to the integrated GPS with digital compass, the soldier will have data as to its location, the location of other soldiers, but also subunit of the enemy forces, if they are detected.

Team equipped with a FIST system composed of eight soldiers and is intended as a unified platform. Each fire group (section) consists of commander, gunner and two

grenade riflemen. The primary weapon is a rifle assault troops 5.56 mm SA80, used in various configurations. This one is equipped with extensive observation and foresight device, which is connected electronically with the eyepiece mounted on the helmet sends images to allow lead to effective fire behind the obstacle, the corner of a building or other object. Rifleman has a 40 mm grenade launcher M203 suspended (UGL - Under Grenade Launcher), sniper rifle is equipped with SA-80 version with a long barrel, a gunner in a light machine gun. Other weapons adapted to the system includes a portable launcher *FIST* MBT LAW antitank, rocket JAVELIN antitank guided missiles and grenade HEFG (High Explosive Fragmentation Grenade). In this system of arms to hit behind the concealment will be possible after measuring the distance from the rangefinder and a data transfer control system coordinates the projectile (grenade), who directed more than an obstacle to explode over the target, causing its destruction.

Analyzing the current state of weapons and equipment which have soldiers the Army Armed Forces, the observation suggests that the situation in this area, much improved, especially since the Polish Armed Forces are involved in stabilization operations in Iraq and Afghanistan. This is a permanent process is also associated with the transformation of structures of the Armed Forces and their professionalizing.

Using the experiences of NATO countries in the implementation of the concept of the future soldier, in 2006 the Polish Army General Staff developed the operational requirements for development work on the Individual Combat Systems (IWS), code-named *TYTAN*. Armament Policy Department has established task teams, whose goal was to conduct work in four main areas of interest:

- integrated equipment;
- weapons and equipment foresights;
- electronics, optoelectronics and software;
- personal protective equipment (ballistic, climatic, mechanical, against weapons of mass destruction).

According to the assumptions *TYTAN* program includes:

- modernization of an individual equipment and adapt it to modern standards;
- a new generation of combat uniforms;
- a new generation of tactical equipment;
- works in the field of electronics and optoelectronics equipment;
- study of a new communications system;
- creating a new camouflage pattern;
- testing a new generation ballistic shields;
- collect data in order to develop the concept of the army a soldier twenty-first century.

On the basis of the results of theoretical work, supported by experiences from the mission in Iraq and Afghanistan, in 2008, developed the initial tactical and technical assumptions for the project. According to these basic equipment *TYTAN* will be composed of the following modules along with the forming of their constituent elements:

- combat uniform (battle suit, pants, underwear, hats, gloves, shoes, socks);
- protection system (body armor vest, flak jacket, gas mask, filter clothes, knee and elbow guards, protection devices for vision and hearing, protective clothing under the jacket);

- weapon system (automatic rifle with grenade launcher suspended, knife - bayonet, pistol, rifle-grenade launcher, sniper rifle, the ammunition, grenades);
- observation and reconnaissance equipment (reconnaissance and observation tool - binoculars, dating modular complex, helmet set, night vision goggles, personal torch, laser pointer);
- elements of the management of activities - C4I (personal computer with the display device information, personal radio station, hub - a hub, the device microphone - earphone, the positioning system, an identification system for their - the remote system health sensors soldier power source);
- mobile able system equipment (integrated with clothing handles and pockets for assembly and handling equipment and weapons soldier, a separate system for handling equipment and weapons);
- supplementary equipment (individual package of medical, chemical individual package, a set of survival).

The *ISW TYTAN* in addition to basic equipment to enable the soldier tasks under different conditions, have come further developed specialized packages: high intensity, high temperature, low temperature, very low temperature, precipitation, engineering, food, climbing, to fight in urban areas and training.

Furthermore, system *TYTAN* is to ensure:

- the ability to self-realization of the tasks in the conditions of confinement, without food and water refilling time to 24 hours;
- ability to function under conditions of industrial pollution, chemical and biological agents during the 24 hours;
- the possibility of independent action on the ground effectively:
 - open, lightly-wooded up to 1000 m;
 - in buildings and in densely-built up to 400 m;
 - outside the combat vehicle.

The individual project implemented a management system (C4I) applications should integrate all the electronic components, computer equipment optronic instruments soldier and ensure the exchange of image data and audio between soldier and elements of its environment, as well as cost-effective energy management.

The computer, part of the system is to enable the exchange of information between all peripheral devices in near real-time, including: sight, helmet set, observation and reconnaissance equipment, navigation, sensor system health soldier, display information (helmet, manual, constant) and functional integration with the other soldiers, the commander of the team, and the adjacent bands by the base vehicle, the higher-level command. According to the assumptions C4I management system should:

- ensure the acquisition, collection, processing and transfer of the necessary information to the soldiers of the team and/or to the higher command level;
- configuration command to enable communication in the team and decide on the type of information sent to the soldiers and the higher command post;
- enable receive and display information about their own position and objects and allied troops to prevent the conduct fratricidal fire.

When analyzing the current and projected state of equipment of the Polish Armed Forces soldier, do not forget about being in a test phase C3IS JAŚMIN system, in particular the possibility that presents one of its modules, namely module designed for the

individual soldier - DSS (*Dismounted Soldier System*). It consists of the following sub-systems:

- **Data Processing Subsystem.** His main device is a Tactical Computer Terminal, which is used to support decision making on the battlefield according to the concept of network capabilities of NATO;
- **Data Manipulation Subsystem.** Allows to enter data into the system and facilitates access to environmental data operations;
- **Sensors Management Subsystem.** Designed to connect the various sensors and information sources, such as LCD (Light Chemical Detector), GPS (Global Positioning System), inertial navigation and a video camera. It automatically controls the sensors, providing information, which after processing are distributed to other soldiers and commanders;
- **Power Management Subsystem.** Supplies the whole equipment ensures continuity of his work;
- **Information Presentation Subsystem.** Shows information on the various screens, such as the HMD (called Helmet Mounted Display) and the LCD panel. This subsystem is used during the practical implementation of the task, because obtaining the view field (space) does not involve direct combat arms and gives the user easy access to environmental data operations;
- **Data Distribution Subsystem.** Enables communication with other actors.

The main equipment is a transceiver subsystem that provides voice communication and data transmission technology, IP (Internet Protocol).

Summarizing the above considerations it can be concluded that in all pending projects, the key intention is to fulfill the principle that the fact that the soldier could efficiently perform tasks and achieve goals must have suitably higher level of technological superiority consisting in increasing the combat capabilities (the parameters affecting them) through the introduction of the latest, technologically advanced weapons and equipment items.

Another proposal concerns the level of subunit commanders situational awareness, which is not only dependent on the input of technology, but also the efficiency of the network command and data exchange. Therefore, it can be assumed that the commander, according to the concept of network operations, will have an appropriate level of situational awareness only when he will be an element of the system (network), which will have the possibility of obtaining information and its exchange with other users.

Because the future soldier is to be integrated into a future regime network-centric battlefield, while providing one of the most important of its components, it becomes necessary to provide it with proper weapons and equipment.

UNMANNED FLYING SYSTEMS

Another, no doubt a significant factor influencing the development of modern military operations is the use of unmanned flying systems – UFS.

To analyze the current state of development of the UFS and it is advisable to familiarize with developed in the U.S. Army Future Combat Systems document (FCS) 18 +1 +1 Systems Overview. White Paper. According to its assumptions of future combat system is to be connected (because it covers all types of troops and services) system of systems. It is assumed that it will build on eighteen separate systems, the network between these systems and the soldiers with their technologically advanced equipment. It

has, therefore, is to include a twenty (18 +1 +1) different systems. Under the assumptions of the system will consist of:

- system of ground autonomous sensors, (*UGS - unattended ground sensors*);
- two autonomous ammunition systems: launched (*NLOS-LS - Non-Line of Sight – Launch System*) and intelligent (*IMS – Intelligent Munitions System*);
- three classes of unmanned ground vehicles: ARV (*Armed Robotnic Vehicle*), SUGV (*Small Unmanned Ground Vehicle*), MULE (*Multifunctional Utility/Logistic and Equipment Vehicle*);
- eight systems of manned combat and support vehicles;
- network between these systems;
- soldiers and their equipment;
- four classes of UFS².

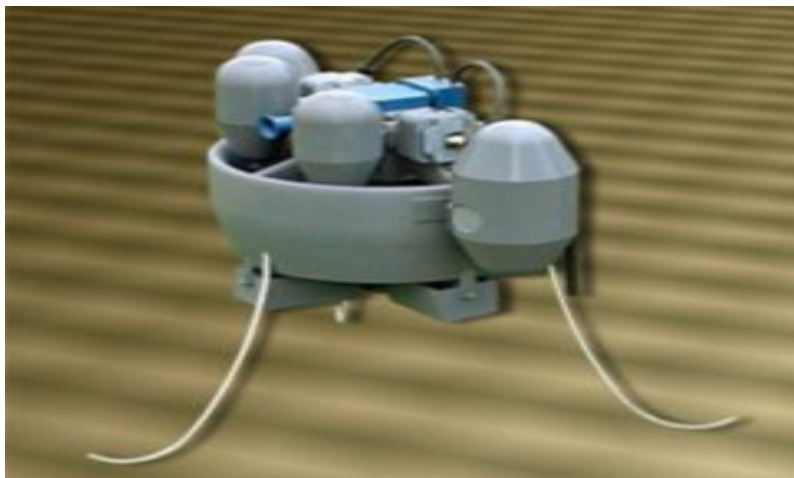
Unmanned Aerial Systems division has been made on the basis of level of command: for platoon - Class I, the company - Class II, the battalion - Class III, brigade - Class IV. In this paper I will consider a platoon- company level systems.

Unmanned Air Vehicle system Class I (Class I UAV) according to the assumptions FCS is intended to provide opportunities reconnaissance platoon soldiers, tracking and searching purposes (Reconnaissance, Surveillance, and Target Acquisition - RSTA). Its key element is the aircraft vertical takeoff and landing, both designed to operate in urban areas and wooded. Can be controlled by the operator, as well as fly autonomously. Moreover, in order to ensure optimal flow of information, it will be able to interact within the network created with selected ground and air combat platforms. With this possibility subunits platoon level reconnaissance will have available information on the conditions which limit the scope of the larger unmanned aircraft. In addition, UAV class I device to act as a translation in a difficult communications in the area difficult to access. This system shall consist of two aircraft (for platoon), the control unit (mobile station flight control) and security features. Its mass (about 18 kg) is to enable the transfer system by a single operator. It is also assumed that the ship is characterized by an 8 kilometer radius of the tactical and persist in the air for at least 60 minutes³.

System numbered among the first class is being developed by Honeywell Aerospace MAV system (Micro Air Vehicle), consisting of two miniature unmanned flying machines, batteries, flight control station, and video terminals. In accordance with the requirements of the whole system is made in a backpack carried by the operator. The system is built modularly and in addition to radio, and links for data exchange is equipped with a removable infrared camera, or daily, has also the possibility of installing other sensors equipped with an interface compatible with unmanned MAV system. The system allows recording video (10 minutes on the camera board and 60 minutes in the terminal ground flight control station). Provide on-board equipment to identify man-sized target at a distance of about 250 m and 125 m day night.

²*Future Combat Systems (FCS) 18+1+1 Systems Overview. White Paper, ver. 19, s. 2, <http://www.army.mil/fcs/> (15.09.2011)*

³ There, page 9.



<http://www.defense-update.com/products/h/honeywell-mav.htm> (2011.09.13)

Honeywell MAV (*Micro Air Vehicle*)

The system performs its tasks associated with the collection of information, mainly the method of hanging and stare (called Hover and Stare), or sit and stare (called Perch and Stare), since there is the possibility of placing it in a convenient place for observing the middle ground reconnaissance data collection .

Unmanned Air Vehicle system Class II (Class II UAV) is to have a wider range of possibilities than the UAV class I and twice the range of action. According to the assumptions, as a multipurpose aircraft should have the possibility of vertical takeoff and landing and to support company commander in the field of reconnaissance, security or early warning, detection and identification purposes (Reconnaissance, Security/Early Warning, Target Acquisition and Designation). Ships of this class will provide a system of measures that can be mounted on vehicles, so they can be delivered as close to the action area. This will provide increased surveillance and reconnaissance coverage. The system is to have the possibility of identifying targets in the day, at night and in poor visibility. It is assumed that this type of UAV is to be carried by two soldiers, operate within a radius of 16 km and persist in the air for at least 2 hours.

System currently meets the above requirements is the *Air Scout* and as a competitive project and the system under the name of OAV-II (*Organic Air Vehicle*). Until now, the third version of the already developed this system *GoldenEye 80*. The camera is a combination of technologies that use propulsion propeller arranged in a cylindrical hull (allows both vertical and horizontal flight device) with stealth technology, which uses a diesel engine drive. It uses sound damping system that causes the engine is quieter than helicopter cameras of similar size. The set of sensors on-board system includes a high resolution camera: day and thermal imaging and laser devices (the indicator targets and the laser beam detector). *GoldenEye 80* utilizes miniaturized navigation system and *GuideStar* flight control, which ensures the autonomy of the flight apparatus, while maintaining control and navigation during both vertical takeoff and landing, as well as hori-

zontal flight without the need for operator intervention. An additional advantage of this object is the ability to self-avoidance, avoidance of obstacles by quickly changing the direction of flight, as well as reliability in conditions of limited access GPS.

Another example of an unmanned flying class II system is a system of OAV-II ship-based unmanned vertical takeoff and landing with a blade placed in a cylindrical casing.



<http://www.piasecki.com>. (2011.09.13)

Prototype CClass II UAV Air Scout

The object will be equipped with cameras to allow observation of the forward and downward, which will send images to the ground terminal station flight control. Moreover, it can be equipped with various sensors and measures to detect mines and contamination of weapons of mass destruction.

In summary, having a UFS will provide its own source of reconnaissance aircraft, and this in turn will enable commanders to the lowest levels of self-command to collect information necessary for them in the field, especially in specific environment of the battlefield, in which the field of earth observation to be significantly reduced.

Opportunities of UFS presented in the paper reflect the level of requirements they must meet in relation to the information needs of the tactical level. These requirements meant that the reported structures are characterized by:

- the relatively small size;
- design modularity allows you to mount a set of sensors suitable for the mission;
- the use of stealth technology, making it difficult to detect by radar;
- low sound signatures;
- capability of vertical takeoff and landing (which excludes the need for a specially prepared landing sites and need to increase the mass of the system equipment, carried by soldiers with additional equipment startup and recovery of the vessel);
- surveillance capabilities in the day, at night, and in limited visibility conditions;

- resources and capability to detect: weapons of mass destruction, contamination, detection and identification purposes, to determine their distances, the laser beam detecting device sent by the enemy.

These requirements are designed to allow the fulfillment of the essential role of UFS which provide information from the battle space in near real-time. Thanks to them much faster than before the commander will have the knowledge about the situation in their immediate vicinity. Possessed information superiority will provide situational advantage, which in turn will obtain favorable action. However, due to the density of the battle all sorts of means, the use of unmanned aircraft systems will mainly be indicated in specific battlefield environments, such as built-up areas, mountainous or wooded.

Advantages of the use of UFS in military operations include the elimination of flying personnel losses, high combat effectiveness, reduce losses in the aerospace, economical operation (particularly servicing, fewer take-off landings, reducing the time constraints of the tasks by remote control, etc.)

Noteworthy is the fact that using of UFS is a demand not only from the army. Also, civilian users see them as the feasibility of various non-military tasks, particularly associated with high risk of losing life or health, for example, during the reconnaissance aircraft disaster areas, or natural disasters.

Most experts predict continued, vigorous development of unmanned aviation. It is assumed that in the third decade of the twenty-first century, unmanned aerial vehicles will utilize 50% of the airspace. Further development is also associated with new tasks that may arise against UFS, for example, air transport of large loads over long distances, providing supplies to the battlefield or evacuation of wounded.

NETWORK CENTRIC SUPPORT SYSTEMS COMMAND

The development of information technology caused the avalanche build-up of new, previously unknown ability to communicate and rapidly expanded their areas of application. Data transmission technologies (technologies used mainly on the internet) adapted to the needs of civilian users also gave new possibilities for systems used in the military. This allowed to increase the military capabilities of communications and IT systems for transmission, processing and data analysis. However, the challenge is how to organize a network of communication and appropriate sharing and making it available for common situational awareness.

The possibilities of using network-oriented access to shared information gave rise to the concept of network-centric battle. The network-centric concept emphasized a new quality, which is the environment in which the fight will be carried out, mainly fight news. The growing importance of operations other than war, the huge advances in technology and asymmetric forms of warfare led to the identification of the need to move away from the battlefield in favor of fighting the perception of the environment as an area of network-centric battlefield.

The essential purpose network-centric conception of the struggle is to design such a set of interconnected elements of space combat, so you can use an increased amount of available information that will be transformed into knowledge necessary resources and consequently will get an increase combat capability.

To ensure the success and efficiency of the activities in line with the concept of action in the network centric environment, it is necessary to ensure a high level of information exchange between its components and the appropriate level for their use.

With regard to the military structures of the base material and the functional systems of network is a global information network (Global Information Grid - GIG), understood as a network structure whose elements are the nodal network layer:

- sensor network as a set of technical means of reconnaissance and information gathering (called Sensor Grid);
- network servers understood as an organized command posts system of decision-making centers (called Grid Command and Control) network;
- effectors identified mainly with advanced weapons systems, and active measures fight (called Shooter Grid).

Determining the extent to which the use of network technology in the armed forces can contribute to improve their military capabilities, it is not easy. But it should be emphasized that the new tactics, techniques and procedures (TTPs), which use is made possible by drastically increasing the ability to share information in a huge affect on increasing the combat capabilities that extend the capabilities of commanders and enable them to communicate their intentions and decisions more quickly, accurately and precisely. The ability to continuously monitor the performance of tasks allows to change the decision according to the situation. An important advantage is the ability to share information to the command of the new approach, namely the use of a common battle space awareness to achieve a high degree of synchronization operations, while preserving the ability to immediately adapt to changing operational situation.

Dynamically changing external and internal conditions pose many challenges, mainly the new threats that are asymmetric and form a new space unpredictability of military operations. One of the many factors influencing this space is a significant expansion of the package of tasks performed by the army, resulting from participation in peace support operations - mainly in the Balkans, the stabilization operation in Iraq or counter-terrorism in Afghanistan.

Purpose and especially to perform the tasks envisaged by the army, require the use of a wide range of command support systems and simulation activities, which should greatly enhance the sharing of information, to enable rational decision making, and consequently result in more efficient use of forces.

These conditions became the impetus for a series of reviews and assessments carried out in various bodies. Their results led, inter alia, for use in a military exercise carried out in the NDU, the first time in the scale of the Polish Armed Forces, Command Support System JAŚMIN. System capabilities allow, inter alia, the graphical representation of the current situation and mapping of the planned activities, and the collection and processing environmental data of current activities. C3I JAŚMIN is able to perform and present:

- structure and equipment;
- display the current situation;
- alarm sensors display;
- planned activities;
- command/short orders and reports.

During the exercise was also used Action Tactical Simulator, which allowed a short time after entering the data to simulate the system planned by the command post personnel for action, and thus their evaluation and comparison of options under consideration of the course of action (COA). The simulator has been developed under a project implemented by the Cybernetics Department of Military Technical Academy and Management and Command Faculty of NDU.

The conclusions of the exercises and theoretical considerations allow to conclude that the use of command support systems will allow, inter alia, eliminate the inertia of the existing specific information, resulting from delays in the flow of data.

In an environment of network-command support systems, the actual picture of the situation will be much more extensive, and most of all current and close to the actual operations. Generate a shared picture of the situation of combat with the use of data and information transmitted in real time, will provide commanders with the knowledge and situational awareness at any time, anywhere, without needing to ask for information to other participants in the activities.

Under the conditions of application of modern IT infrastructure, commanders, and in particular the staff a command post functional cells, will have a clearer picture of the situation and the high level of knowledge of the totality of the conditions of its own activities. This will allow the implementation of the command of far greater degree of probability of success in action, than in conditions considered to be traditional.

SUMMARY

Summarizing the above considerations it is clear that the analysis and evaluation of the phenomena of contemporary and future battlefield indicate that new technologies and means of struggle undoubtedly will affect the rules for the use of troops, both in current and future operations. Application of modern combat systems will shape the image of military action, will force changes in how and when and where to use your potential. Network variety of related sensors at all levels and levels of information system will create conditions for the implementation of tasks in an environment previously unknown to have full knowledge of the phenomena and situations occurring on the battlefield in near real-time. Therefore becomes necessary verification number to date operating practices and assumptions.

Also anticipated that the effectiveness of military operations to increase significantly, mainly by increasing the timeliness, completeness and reliability of the information about the current status of space combat.

Noticeable is that the current emphasis on the growing importance of changes in the organizational - as a determinant of technical change and development of military operations, including operations other than war. It is anticipated that a change of tasks and how their conduct will require increased capacity and maneuverability for fire crews. Therefore, the aim is to equip them with modern means of combat and transport. In view of the large involvement of the armed forces in various operations outside the country, it becomes necessary to have highly mobile units, suitably equipped and capable to act in a relatively short time.

It should also be aware that today's challenge is to design and produce the modern means of combat, but their implementation and use in practice. For emphasis here should be that new technology brings with it increased demands on each of the user. The use of modern means of warfare should be extremely efficient and expedient, professionally carried out by appropriately trained staff for that.

BIBLIOGRAPHY

1. *5,000 Sagem Défense Sécurité FELIN Systems Ordered For French Army*, (w:) www.defense-aerospace.com.

2. Alberts David S., Garstka John J., Frederick P., *Network Centric Warfare. Developing and Leveraging Information Superiority*, CCRP Publication Series, 2000.
3. *FELIN soldier system*, (w:) www.sagem-ds.com/pdf/en/D978.pdf.
4. *FIST Assessment Phase*, (w:) www.defense-update.com/products/f/fist_sa.htm.
5. *Future Combat Systems (FCS) 18+1+1 Systems Overview. White Paper*, ver. 19.
6. *Future Combat Systems Overview*, (w:) www.army.mil/fcs.
7. Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, AON, Warszawa 2003.
8. *Informacja do aneksu Rozwoju Sił Zbrojnych RP na lata 2007 - 2012*, Sztab Generalny WP, Zarząd Planowania Strategicznego - P 5, Warszawa 2009.
9. Janczak J., *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, [w:] *Sieci teleinformatyczne w działaniach sieciocentrycznych*, (red.) J. Janczak, A. Wisz, AON, Warszawa 2007.
10. Konopka L., *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, „Myśl Wojskowa” 2004, nr 2.
11. Topik A., *Terroryzm i broń masowego rażenia w polityce NATO*, Zeszyty Naukowe AON 2003, nr 1(50)A.

NETOGRAPHY

1. www.army-technology.com (2011.09.13)
2. www.army-technology.com/projects/fist/fist1. (2011.09.13)
3. www.defense-update.com/products/g/goldeneye50.htm (13.09.2011).
4. www.globalsecurity.org/military/systems/ground/fcs.htm (2011.09.13)

В. П. Петров.

ВЪЗНИКВАНЕ И РАЗВИТИЕ НА ТРАНСГРАНИЧНАТА ОРГАНИЗИРАНА ПРЕСТЪПНОСТ В СВЕТА

Велико П. Петров

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen.

INCREASE AND DEVELOPMENT OF THE TRANSBOUNDARY ORGANIZED CRIME IN THE WORLD

Veliko P. Petrov

Abstract: *This report aims to familiarize readers with a very serious problem of our time, namely organized crime, which is one of the most serious forms of crime because of the high degree of public danger. This type of crime is a problem for humanity. The emergence and development of cross-border organized crime in different countries around the world is being considered. Organized crime is a set of crimes committed by individuals involved in sustainable, hierarchical, professional criminal organizations whose primary purpose is to extract profits in large amounts for extremely short periods of time by committing unlawful acts. Globalization has significantly increased the cross-border nature of organized crime, with modern means of communication creating the conditions for the construction of criminal organizations of a network type.*

Keywords: *organized crime, international organized crime*

Организираната престъпност е комплексно социално-правно явление, което съдържа широк диапазон от престъпления и не се ограничава в определени сфери. Тя няма единен модел, а динамични проявни форми, определени от национални, регионални и глобални процеси. Организираната престъпност е една от най-тежките форми на престъпност, поради високата степен на обществена опасност. Този вид престъпност е проблем за човечеството. Понятието организирана престъпност е синоним на понятието мафия. Националните законодателства формулират престъпността като противоправна дейност на организирани формирования осъществяващи престъпен бизнес на определена територия и в определена сфера.

В Европейската стратегия за сигурност е посочено „Европа е основна цел на организираната престъпност. Тази вътрешна заплаха за нашата сигурност има важно външно измерение: трансграничният трафик на наркотици, жени, незаконни мигранти и оръжия представлява значителна част от дейността на престъпните групи. Той може да бъде свързан с тероризма. Тези престъпни дейности често се свързват със слаба или липсваща държавност. Приходите от наркотици са способствали за отслабването на държавните структури в редица държави производители на наркотици. Приходите от търговията със скъпоценни камъни, дървен материал и

малки оръжия подхранват конфликти в други части на света. Всички тези дейности подкопават както правовия ред, така и самия социален ред“.⁴

Следва да се отбележи, че дори и в специализираните кръгове не съществува общоприето определение за понятието организирана престъпност.

Можем да определим като **престъпна организация** всяка структурирана група, съществуваща за определен период от време, съставена от повече от две лица, които действат съгласувано и целят, чрез упражняване на заплахи, пряко или косвено, придобиване на финансова облага или друг вид материална привилегия, която вреди сериозно на икономическото и социалното сближаване на Европейския съюз и неговите държави членки, както и на единния пазар⁵.

Организираните престъпни групи⁶ са незаконни предприятия, предназначени да генерират печалба. Те се занимават с разнообразна трансгранична дейност като трафик на наркотици, трафик на хора, незаконен трафик на оръжие и корупция, която генерира огромни печалби.

„**Организирана престъпна група**“ означава структурирана група от три или повече лица, която съществува за определен период от време и действа съгласувано с цел извършване на едно или повече тежки престъпления, предвидени в съответствие с тази конвенция, с цел получаването, пряко или косвено, на финансова или друга материална облага⁷.

Транснационална организирана престъпност е съвкупност от престъпления, извършени:

- в повече от една държава;
- в една държава, но значителната част от планирането, подготовката и ръководството или контрола се извършва в друга;
- в една държава, но от организирана престъпна група, чиято престъпна дейност се осъществява в повече от една държава;
- в една държава, но със значителен ефект в друга държава.

Групата **Fijnaut**, създадена през 1995 г. от холандската парламентарна комисия, определя организираната престъпност като „група или мрежа от хора, които се фокусират основно върху незаконно придобитите печалби и по систематичен начин извършват сериозни престъпления, с големи обществени последици. Тези групи или мрежи са способни ефективно да прикриват своите престъпления, по-специално чрез използване на насилие или средства за корупция“. Те също така се стремят да се разграничават организираната престъпност от професионалната, корпоративна престъпност и „бяли якички“. Тогава по същество, организираната престъпност попада в две отделни наказателни категории: доставката на нелегални потребителски стоки (наркотици) и услуги, както и проникването в законния бизнес, като например банкиране, бизнес с отпадъци, транспорт, строителството и т.н.⁸

Организирана престъпна група – чл.93 т.20 от НК – легално определение: структурирано трайно сдружение на 3 или повече лица с цел да вършат съгласувано в страната или чужбина престъпления, за които е предвидено наказание лиша-

⁴ Европейска стратегия за сигурност, сигурна Европа в един по-добър свят, Брюксел, 12 декември 2003 г., стр. 4, <https://www.consilium.europa.eu /uedocs/cmsUpload/031208ESSIIBG.pdf>

⁵ Работен документ относно организираната престъпност, Специална комисия по организираната престъпност, корупцията и изпирането на пари, Докладчик: Salvatore Iacolino, 1.10.2012

⁶ Предложение за Директива на Европейския парламент и на Съвета за обезпечаване и конфискация на облаги от престъпна дейност в Европейския съюз, Брюксел, 12.3.2012 г., COM(2012) 85 final, 2012/0036 (COD)

⁷ Конвенция на ООН за транснационалната организирана престъпност от 15 ноември 2000 г., член 2а

⁸ Jansen, E. & Bruinsma, J., 'Policing organised crime', European Journal on Criminal Policy and Research, vol. 5.4 (1997), pp.85-98.

ване от свобода повече от Зг., и чрез които се цели да се набави имотна облага. Сдружението е структурирано и без наличие на формално разпределение на функциите между участниците, продължителност на участието или развита структура.

Трансграничната престъпност е явление с глобален характер, което е познато в почти всички страни в света и последиците от нея не са еднакво значими за отделните държави. Различията се дължат главно на географското положение на държавите, като тази престъпност поразява освен страните, през които преминава, а и тези, които са крайни точки на канали на наркотици, трафик на хора и т.н., като основния „удар“ е върху последните.

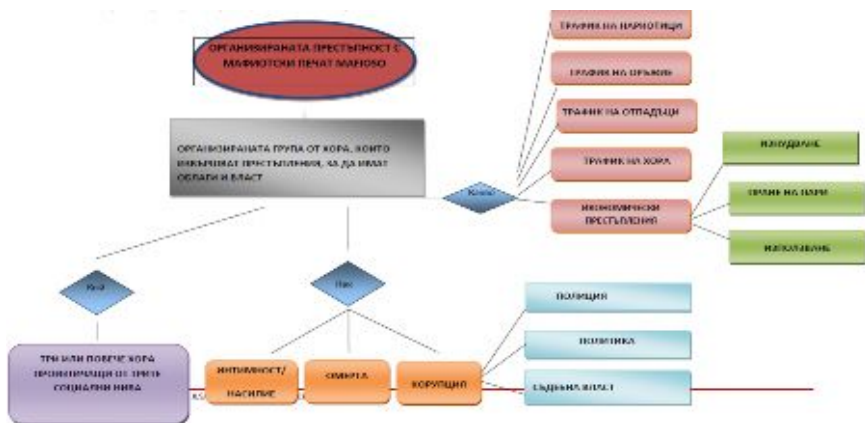
Трансграничната престъпност не влияе върху обема на престъпността като цяло, но пък значително влияе върху качествените характеристики на престъпността. Обемът на регистрираните трансгранични престъпления е сравнително нисък от регистрираната престъпност.

Експерти-криминолози на Интерпол разглеждат организираната престъпност като дейност на йерархично организирано съобщество, което чрез легалния и нелегалния бизнес, посредством изнудвания и корупция, създава по противоположен начин огромни капитали, а според руски криминолози организираната престъпност е функциониране на устойчиви, управляеми съдружия от престъпници, извършващи криминален бизнес, чиято система за самозащита от социалния контрол е корупцията.

Организираната престъпност се появява при определени исторически условия – дезорганизирано общество, насилие на собствената власт. За нейна родина се сочи Южна Италия и главно о-в Сицилия. Сицилианската мафия включва роднините си по пряка и сребрена линия и най-често те са 4-5 поколения. Като всички са подчинени на главата на мафията. Сицилианската мафия е модела, по който се изгражда и престъпната фамилия, която е винаги срещу Закона и установения ред.

При китайците организираната престъпност възниква като реакция на военна намеса и оцеляват само 5-ма. Това са и първите “Триади” от 17 век. При тези обществени условия се създават тайни организирани общества – затворени и подчинени на закона за мълчанието. За тях не се зане почти нищо (взаимоотношения вътре в организацията, броя на членовете, мащабите в които действа). Друга линия по която възникват престъпните организации е икономическата, появата и е резултат на развитие на търговията и новите икономически отношения. Като след време икономически интерес става основен фактор за реформиране на престъпните организации.

Фамилията – е характерна за италианската, американската и японската организираната престъпност. Ритуалите са задължителни за много от престъпните организации. Приобщаването на членове става по точно определен ритул – така е при Италианска мафия, Китайските “Триади” и Японската “Якуза”.



Фиг. 1. Организираната престъпност с мафиотски печат⁹

Италианската организирана престъпност е най-старата известна в света организирана престъпност, чиято дейност започва най-рано на о-в Сицилия, по времето когато там са били арабите, и присъствието на Френските войски през 13 век. Известни са няколко организации:

1) **Сицилианската мафия – Коза Ностра** – е с най-дългата история в света и Европа. Американската Коза Ностра е изградена по модел на Италианската. От 136 до 186 фамилии, има около 5 хил. мъже на честа, които са членове на Сицилианската мафия, поради участие в наркотрафик, хазарт, отвлечение и рекет.

2) **Неаполитанската организирана престъпност – Камора** – това е другата разновидност. Тя е най-буйната и е предимно в областта на кокаина. Над 130 фамилии с над 7 хил. членове. Нейните босове се занимават с рекет, отвлечение, изнудване. През 70-те год. избухва война м/у Сицилианската и Неаполитанската – побеждава Сицилианската, а Неаполитанската избягва в Мадрид.

3) **Калабрийската организирана престъпност “Норангета”** – те са натрупали пари и имат голяма мощ, те осъществяват политиката на големите наркотрафиканти и контрабандата на цигари. Калабрия предоставя възможност за развитие на мафията.

Има и две нови след 1990 г. – те са малки и се създават от членове на напусналите 2 големи но с разрешение на боса: Като “**Сакра Корона Унита**” – около 50 фамилии и “**Ластида/звезда**” – с около 1000 члена. Те имат спомагателен характер по отношение на големите.

Италианската мафия е проникнала във всички сфери на обществото и в политиката. Тя е модел по които се организира организираната престъпност и в други държави и най-вече в Америка. Италианската мафия има свои организации в целия свят.

⁹ Опознавателен преглед над проблематиките на законността в страните партньори в проекта ЕКЗ (европейска каравана за законност, на лат. ECL). Документът е разработен от експертна група по проекта ЕКЗ в Италия: Ирене Ферарио, Йоле Гарути, Омберта Инграши и Лаура Миани, European Caravan for Legality -No. JLS/2009/ISEC/AG/189 – 30-CE-0329861/00-73, стр.9.

Организираната престъпност в САЩ е една от най-мощните в света. Известна е с прозвището *Коза Ностра* и преминава през три периода. *Първия период* обхваща втората половина на 19 век до края на 1920 г. и е свързан с дейността на емигрантите. Няма ясно изградена физиономия, основното средство, което използват е рекет и корупционни практики. *Втория период* е известен с така наречения „Сух режим“ – забраняват се производството на алкохол и продажбата му. Те изнасят производства на островчетата нелегално и за кратко време натруват средства. Средата на 20-те години започват битките от Италия напускат хора от мафията и отиват в Щатите и там изграждат мафиите в САЩ по модел на Италианската мафия. Много време минава докато Американците разберат че убийствата и взривяванията не са в резултат на уличната престъпност, а на нововъзникнало явление по модел на Италианската мафия.

Организацията на организираната престъпност в САЩ в началото е наричана „Синдикат“, „Мафия“, а след това „Коза Ностра“. И при тях се приема фамилизъмът и сложното структуриране. В нея има строго разпределение на труда и специализация на отделните организации. Коза Ностра се ръководи от Боса – ръководителя на престъпната организация, той определя и наказания за членовете на „фамилията“, той винаги заслужава внимание. Съветника заема особено място и той се води като заместник на боса. На седмашко ниво са капитаните или наричани още „Глави на семейството“, на най-ниско ниво са войниците.

Третия период – Закона RICO, слага край на 2-рия период и поставя началото на 3-тия период, който продължава и до днес. Той регламентира и регулира нов тип престъпности, нови наказателно правни методи за контрол над престъпността. На мощността на К. Ностра се противопоставя мощността на държавата. Увеличават участието си в международния наркотрафик, което е и най-доходно, както и тясно сътрудничество със Сицилианската мафия, Колумбийските картели и Руските организации. Понастоящем Коза Ностра включва 25 фамилии с около 3 хил. мъже на честта и около 15-40 хил. асоциирани членове.

Китайски триади. Много малко се знае за нейната организация, тъй като тук дават отражение и философията и религията. Китайската организирана престъпност е една от най-добре структурираните, мобилни и ефективни. Триадите са базирани на три основни понятия – небе, земя и човек. Организацията и структурата на триадите отговаря на принципа на конспиративност. Изградени са приамидално – в основата са обикновените членове, а на върха е главата на дракона (ръководителя), като всички са подредени в строга ейрархия. На територията на Китайската република действа една триада „*Великият кръг*“, чийто числен състав не е известен. Най-големите триади са базирани в Хонконг и Тайван. „*Сун Йе Он*“ – е най-многочислената и мощна организация - тя има разклонения в Европа, Румъния, САЩ и Канада. „*14 Кв*“ – е най-многочислената и жестока и има около 30 клана с 25-30 хил. членове.

Това са основните най-големи триади. Характерното е че тяхната организация наподобява на колежанско общество. Плучават повиквателни да се явят в определен ден и време за изпълнение на операцията. След приключване на операцията те се прибират по местата си. Те са трудни за разкриване и са много мобилни. На о-в Тайван е „*Юнайтед Баму*“ и „*Бандата на 4-те морета*“ – те се занимават с пиратска дейност и имат добро разузнаване. Техните интереси са насочени в Азия, Тай-

ланд, а за трафик на дрога, проституция са насочени към Австралия. Имат и трайно присъствие в САЩ.

Японската организирана престъпност „Якуза“ е също от 18 век, изгражда се по модел на Италианската без да има връзка помежду им. Тя се организира на принципа на „фамилията“ (семейството), в нея основни са отношенията на „обуян“/бащата – „кобун“ – сина, което отразява взаимоотношенията в традиционното японско семейство. „Якуза“ се изгражда на принципа на пирамидата: На върха е обуян – бащата/бос, заместник на обуяна, офицери, членове и чираци.

Към членовете на престъпните организации има специални изисквания: да не разкриват тайните на организацията; да не употребяват наркотици и да са на подчинение на висшестоящите в организацията. Всеки един член има татуировка, която е отличителен белег на членовете на „Якуза“ – символа е „позлатен ромб“. За да се приеме някой за член на „Якуза“ се извършва определен ритуал, който наподобява на религиозна церемония.

Най-многочислената „Якуза“ е „*Ямагучи-гуми*“, която има 750 клана с около 23-25 хил. членове. Структурирана е под формата на пирамида и обединява криминалните класи в Япония т. нар. комарджии, амбулантни търговци, мошеници и хулигани. „*Ингава-кай*“ има 313 клана и м/у 6 и 7 хил. членове. Тя има сходна структура на „Ямагучи гуми“ – пирамидална. „*Суиомоши-ренго*“ – има 177 клана и 7000 членове - те са по-малочислени и по това се смята, че са по-лесни за управление. Основните зони в които са базирани: Азия и страните от Тихия океан, Корея и Филипините. Страните от Океания и Австралия. Северна Америка, Бразилия и Германия. Японската „Якуза“ се проявява по-скоро като криминална общност, липсва тясна обвързаност с икономиката на страната.

Колумбийска организирана престъпност. В много международни документи организираната престъпност в Колумбия се характеризира като „държава в държавата“, а това е характерно за държава в която организираната престъпност е навлязла във всички сфери на властта. Възниква през 60-те години, като страната става център за отглеждане на марихуана, така към традиционна кока се прибавя и нов наркотик търсен на пазарите. Със своето географско разположение и граничните със нея страни я превръщат в мост за трансфериране на наркотиците първоначално на Север, а по-късно и към Европа.

Основата върху която се изграждат и функционират организациите е икономическия интерес и оттам и наименованието *Картели*. Структурата на Картелите е пирамидална. Колумбийските картели са специализирани в трафик на кокаин и пране на парите от трафика. Дейността им е типично изразена в криминални прояви – грабежи, рекет, проституция. Колумбийските картели действат като предприятие с цел за извличане на максимална печалба. Те действат като организатори на своеобразна индустрия, в която са въввлечени огромен брой хора.

Нигерийска организирана престъпност. Това е относително нова организация създадена през 70-те год. на Африканския континент. Дейностите, които извършват са разностранни. Причините са икономически (свързани с производството на петрол). Организациите наподобяват мафиини формирования на американската Коза Ностра. Нигерийските групи представляват „клетка“, която се ръководи от шеф, има отговарящ за набиране на членове, лейтенанти и войници. Първоначално Нигерийските групи започват със спомагателни дейности на крупни международни организации, след което започват да се профилират в наркотрафик, изнудване,

фалшифициране на пари, документи, корупция. Членовете са и признати фалшификатори, изключително активни са и в трафика на героин.

Организираната престъпност в Русия. Руската мафия тръгва от Съветския съюз и сега има влияние по цял свят. Руската мафия е най-мощната престъпна мрежа в света. Това сочат анализите на експертите, които бяха оповестени в Лондон и Мадрид. Броят на членовете ѝ е между 100 000 и 500 000. Действат в Израел, Унгария, Испания, Канада, Великобритания, САЩ, Русия и др. Емигрират в Израел, Америка и Германия с фалшиви еврейски и немски самоличности. Дейността им включва разпространение на наркотици, търговия с оръжия, бомбени атентати, контрабанда, интернет измами и др. Едно от правилата им е никога да не си сътрудничат с властите. Ако някой от членовете е арестуван и проговори бива убит при освобождаването си. Известни са още с трафик на органи и поръчкови убийства. Руската организирана престъпност работи в сътрудничество със сицилианската Коза Ностра, колумбийските картели, а в последно време и с американската Коза Ностра.

Организираната престъпност от Мексико. Тя е създадена в затворите в САЩ от членовете на уличната престъпност и днес наброява около 30 000 души в САЩ. Те контролират каналите за наркотрафик, оръжие и проституция. Най-много пари печелят от нелегалната имиграция в САЩ и намирането на работа за имигрантите, които след това им „плащат гаранция сигурност“. Много пари печелят и от изнудване и рекет. Те действат на територията на Ел Пасо и Калифорния. Полицията нарича този град малкия Чикаго, защото напомня за Чикаго от времето на Ал Капоне. Членовете на мексиканската мафия се татуират с мексиканския национален символ върху горящ кръг с кръстосани ножове. Говори се, че има 150 затворника, които имат властта да заповядат убийство и около 2000, които са готови да изпълнят заповедта. Принуждават други групи и дилъри да плащат такса за защита и убиват тези, които откажат.

Организираната престъпност в Израел. Мафията в Израел извършва трафик на наркотици и проститутки в голям брой държави. Някога на тях е било гледано с респект, но днес са безскрупулни и убиват, без да им мигне окото. Руско-израелската мафия е толкова навътре в политическата система на САЩ, че силите на реда изобщо не успяват да постигнат някакъв прогрес в спирането им.

Организираната престъпност в Сърбия. Сръбската мафия действа в над 10 страни, сред които попадат Германия, САЩ, Великобритания и Франция. Извършват трафик на наркотици, контрабанда, убийства и кражба на информация. Състои се от три големи групи, които контролират останалите по-малки групи. Понастоящем в Сърбия групите на мафията са около 30-40.

Организираната престъпност в Албания. Албанската мафия се състои от голям брой престъпни организации, които освен в Албания, действат в САЩ и други европейски страни. Смята се, че албанската мафия се е разпространила на международно ниво през 80-те години. В САЩ и Великобритания мафиотите извършват трафик на жени и наркотици и са известни с това, че бързо си отмъщават.

Ямайските ганстери в Англия. Това са ямайци, които са емигрирали в Англия през средата на 20-ти век. Често са свързвани с организирана престъпност, като търговия на наркотици и сделки с оръжия. Не се намесват във високите етажи на властта, затова не се смятат за толкова силни като останалите мафиоти.

Организираната престъпност в страните от Америка, Африка и Азия.

Организираната престъпност в САЩ и Канада е сред най-развитите в съвременния свят и има не само локално но и глобано значение.

В *Канада* са се настанили едни от най-големите азиатски и европейски групи, които променят коренно криминалната обстановка. Основните сфери на дейност: са трафик на наркотици, пране на пари и измами, отвличане, а руските организации са се специализирали в извършването на поръчкови убийства. През последните години се настаняват и организации на японската „Якуза“, които се занимават с наркотици, пране на пари, проституция и измама. Банковата система в Канада е много добра и се използва за пране на пари. Перачите ги внасят в банките, а от там ги трансферираят към съответните страни.

На територията на *САЩ* е създадена огромна и сложна система от организирана престъпност от различни националности, които в конкурентната среда изграждат многонационални формирования. Присъствие има на Китайските „Триади“, които се занимават с нелегалния трафик на хора. Голямо влияние в САЩ има руската мафия, която присъства на черния пазар със суровини. Нигерийските престъпни групировки в САЩ изпълняват важни задачи в наркотрафика и кокаина. Виетнамските престъпни групировки се включват активно в трафика на героин, проституиращи жени и нелегална емиграция. В САЩ има силно развита организирана престъпност на улично ниво. Тези организации контролират трафика на наркотици и контрабандни стоки като алкохол и цигари.

Централна Америка обикновено се използва за бази и дистрибуция на наркотици, ембаргови стоки за Куба, контрабанда на стоки, трафик на хора. В района на Карибите е известен т. н. „Банка в банката“, които изпират милиарди долари, придобити чрез престъпления.

Южна Америка е точка за транснационалната организирана престъпност поради политическите си нестабилности, огромните пазари и възможности за инвестиране на мръсни пари, притежават суровини за производство на наркотици и други стоки, които имат значение за мафията. Поради своето разположение, предлагащо морски пътища за свързване със всички държави от континента.

Организираната престъпност в Африка. Този континент е слабо проучен и единствено изследователските програми дават представа за престъпността. Това е престъпност засягаща собствеността, насочена срещу живота и телесната неприкосновеност на човека. Съществуват различни предпоставки които обуславят развитието на организирана престъпност като:

1) благоприятните условия за отглеждане на разстения от които се произвеждат наркотици. Мароко е един от основните производители на канабис, а в района на Нигерия се отглежда кока;

2) засилена емиграция извън континента, като се развива и незаконния трафик на хора, който е един от основните дейности на организираната престъпност;

3) нелегалната търговия с оръжие и боеприпаси;

4) африканците се включват като носачи на наркотици и други контрабандни стоки по каналите на организираната престъпност.

Организираната престъпност в Азия се отъждествява с китайските „Триади“ и японската „Якуза“. Основното за тях е голямата им организираност и ролята им в съвременната транснационална престъпност. В Пакистан има развита система за трафик на наркотици и нелегални емигранти, като те работят в сътрудничество с турската мафия. Тук преминава и нелегалния път за трафик на жени и млади момичета.

чета, за така наречените сескиндустрии. Югоизточна Азия разполага с организирана престъпност която се занимава с грабежи, отвлечане, хазартни игри, проституция износ и внос на контрабандни стоки. В Азиатския континент действат и много центрове за пране на пари.

Организирана престъпност в страните от Океания – е сравнително по-слабо развита, тъй като възниква много по-късно. Австралия и Нова Зеландия са включени в глобализираната престъпност, тъй като на територията им са базирани най-големите многонационални престъпни организации (големи емигрантски колонии от Океания, присъствие има на китайските „Триади“ и японската „Якуза“, италианската мафия, както и руските групировки). В Австралия и Н. Зеландия е организиран пазар за героин, хашиш и кокаин, добре е развит и трафика на емигранти. Региона е един от световните центрове за пране на пари.

Организирана престъпност в страните от Европа. Организираната престъпност в *Западна Европа* от векове е традиционна привилегия на Италия. До 70-те години Европа е свободна от организирана престъпност, като постепенно се създават икономически, политически и културни предпоставки за развитието ѝ. След войните Европа се променя значително, като възниква сложна криминогенна обстановка. Последиците са: нарастване на общата престъпност; появяват се младежки неформални движения (рокери, хипита); появяват се терористични организации изградени на верски и расови предрасъди, развитие на мощна „черна“ икономика.

Създаването на Европейския съюз и на Западноевропейския съюз поставя началото на организираната престъпност в съвременните и аспекти. Развива се много бързо, а стремежа и е забогатяване в много нови форми на престъпност, и причиняването на големи материални щети на граждани и корпорации.

След 1989 / 90 г. възниква сложна обстановка в резултат на разпадането на Източния блок и най-вече на Съветския съюз. Западноевропейският пазар е цел за легална и нелегална икономика на страните от Централна и Източна Европа, както и към неразвятия пазар на ОНД – насочват се малко легални инвестиции и много представители на международната О.П.

Източна Европа – организираната престъпност в Източна Европа, Руската федерация и страните от ОНД е относително ново явление, което се появило при определени обществено-икономически и политически условия:

1) Премахване на тоталитарното управление в страните от бившия Източен блок и преминаване към демократично политическо управление;

2) Преминаване от централизирано планово управление в свободно пазарно стопанство - трансформация на собствеността от държавна в частна. Този процес на трансформация поражда уникална възможност за пораждаване на огромен криминогенен потенциал. За кратко време организираната престъпност придобива огромни размери, много международни престъпни организации влизат във взаимодействие с национални групировки и се занимават с трафик на наркотици и хора, контрабандни стоки, трафик на откраднати автомобили и стратегически суровини.

Организирана престъпност в Балканския полуостров възниква сравнително по-късно. Този процес съвпада с разпадането на Източния блок. Страните на Балканите имат и големи различия – Турция и Гърция са най-добре икономически развити, Гърция е член на ЕС и НАТО, а Турция на НАТО, останалите страни се ползват като транзитни за трафик на наркотици и контрабандни стоки. Албанската мафия е една от най-организираните. Добре изградена организирана престъпност

има и в Косово, Македония, Сърбия, България и Румъния. Дейността на престъпните организации е улеснена от корупцията. Основните дейности на престъпните организации на Балканите са: трафик на наркотици; трафик на крадени автомобили; трафик на хора; трафик на културни и исторически ценности и други.

Съвременната организирана престъпност в своето непрестанно развитие вече е извън традиционните схващания за йерархичност и корупция. В резултат на трансграничното и развитие и технологичния прогрес тя използва недостатъците и ограниченията на правните системи, като нанася сериозни щети на индивидуалното имущество и оказва изключително вредно влияние върху социално-политическата и икономическата система и нарушава правни ценности като човешкия живот, икономиката, общественото здравеопазване и др.

Най-общите характерни особености на организираната престъпност са следните:

- монопол върху определени престъпни дейности (наркотици, проституция, пране на пари и др.);
- системно използване на насилие срещу лицата, дръзнали да оспорят този монопол или вътрешната дисциплина на организацията;
- възможност организираната престъпна група да продължи дейността си и при отстраняването по каквато и да е причина на неин член;
- йерархична и бюрократизирана структура с разпределение на функциите;
- придобити знания в областта на правото, финансите и счетоводството;
- транснационализация на някоя от дейностите на организираната престъпна група;
- възможност да въздейства върху политическите, административните и съдебните процеси¹⁰.

Противозаконните дейности на транснационалната организирана престъпност са: контрабанда; международен трафик на наркотици и наркоиндустрия; контрабанда на нелегални мигранти; незаконна търговия с оръжие; незаконна търговия с ядрени материали; търговия с хора и човешки органи; кражба и контрабанда на автомобили; кражба и контрабанда на предмети с историческа и културна стойност; фалшифициране на пари и ценни книжа; порнография; пиратство; хазарт; лихварство; пране на пари и други форми на престъпност срещу международния икономически ред.

Изводи:

1. Организираната престъпност представлява съвкупността от престъпленията, извършени от лица, участващи в устойчиви, йерархични, професионални престъпни организации, чиято водеща цел е извличането на печалби в големи размери за изключително кратки срокове чрез извършване на противозаконни деяния.

2. Организираната престъпност е комплексно социално-правно явление, което съдържа широк диапазон от престъпления и не се ограничава в определени сфери. Тя няма единен модел, а динамични проявени форми, определени от национални, регионални и глобални процеси. Организираната престъпност е изградена от сложни корпоративни структури с развити мрежи от филиали, което и позволява да реализира стратегии за противодействие на правоохранителните органи и бързо да

¹⁰ Четирисет и първо Народно събрание. Комисия по правни въпроси и Комисия по вътрешна сигурност и обществен ред. Кръгла маса на тема: "Необходими законодателни промени за противодействие на организираната престъпност и корупцията", София, 3.05.2010 г., Адвокатски преглед 4-5/2010, стр.9.

натрупва капитали, съчетавайки насилствена и коруптивна престъпност с икономическа активност.

3. Една от характерните черти на съвременната организирана престъпност е нейното масово разпространение във всички райони на света и установения от нея тотален контрол върху всички сфери на обществено-политическия и икономическия живот на държавите. Глобализацията значително повиши трансграничния характер на организираната престъпност, като съвременните средства за комуникации създават условия за изграждане на престъпни организации от мрежов тип.

Литература:

1. Работен документ относно организираната престъпност, Специална комисия по организираната престъпност, корупцията и изпирането на пари, Докладчик: Salvatore Iacolino, 1.10.2012,

2. Предложение за Директива на Европейския парламент и на Съвета за обезпечаване и конфискация на облаги от престъпна дейност в Европейския съюз, Брюксел, 12.3.2012 г., COM(2012) 85 final, 2012/0036 (COD)

3. Конвенция на ООН за транснационалната организирана престъпност от 15 ноември 2000 г.,

4. Наказателен кодекс на Република България, в сила от 01.05.1968 г., Обн. ДВ. бр.26 от 2 Април 1968г., изм. ДВ. бр.13 от 7 Февруари 2017г., посл. доп. ДВ. бр.54 от 5 Юли 2017г.

5. Jansen, E. & Bruinsma, J., 'Policing organised crime', European Journal on Criminal Policy and Research, vol. 5.4 (1997), pp.85-98

6. Теми по организирана престъпност, http://znanieto.net/index.php?option=com_virtuemart&func=downloadRequestFree&page=shop.browse&product_id=4483

7. Публикувано във факти.бг на 28 Май, 2017 г. „Топ 10 на най-големите мафии в света“, <https://fakti.bg/life/239194-top-10-na-nai-golemite-mafii-v-sveta>

8. Четиридесет и първо Народно събрание. Комисия по правни въпроси и Комисия по вътрешна сигурност и обществен ред. Кръгла маса на тема: “Необходими законодателни промени за противодействие на организираната престъпност и корупцията”, София, 3.05.2010 г., Адвокатски преглед 4-5/2010, vas.bg/files/Adv4-5_2.pdf

9. Опознавателен преглед над проблематиките на законността в страните партньори в проекта ЕКЗ (на лат. ECL), Документът е разработен от експертна група по проекта ЕКЗ в Италия: Ирене Ферарио, Йоле Гарути, Омберта Инграси и Лаура Миани, European Caravan for Legality -No. JLS/2009/ISEC/AG/189 – 30-CE-0329861/00-73

10. Европейска стратегия за сигурност, сигурна Европа в един по-добър свят, Брюксел, 12 декември 2003 г., <https://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIBG.pdf>

В. П. Петров,

ЦИКЪЛ НА ПОЛИТИКАТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА БОРБА С ОРГАНИЗИРАНАТА И ТЕЖКАТА МЕЖДУНАРОДНА ПРЕСТЪПНОСТ

Велико П. Петров

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen

POLICY CYCLE OF THE EUROPEAN UNION TO COMBAT WITH THE ORGANIZED AND SERIOUS INTERNATIONAL CRIME

Veliko P. Petrov

Abstract: *This report aims to familiarize readers with a very serious problem of our time, namely organized crime, which is one of the greatest threats to the security and stable economic development of the countries of the European Union. The so-called cycle of EU policy to combat organized and serious international crime is being considered. It aims to ensure effective co-operation between Member States' law enforcement agencies, EU institutions and agencies, which should lead to coherent and robust operational actions addressing the most pressing criminal threats facing the EU. Each cycle lasts four years and optimizes coordination and co-operation on selected priorities in the fight against crime. Crime threats are determined on the basis of criminal intelligence data and then confirmed at political level. The report looks at the approved eight threats of crime as priorities in the EU's policy cycle to combat organized and serious international crime for the period 2018-2021: cybercrime, drug-related crime, organized crime affecting property, trafficking in human beings, Trafficking in firearms, VAT fraud and environmental crime.*

Keywords: *organized crime, fight against international organized crime*

От началото на 90-те години на миналия век организираната престъпност е гореща тема в обществения дебат, политическата и научна сцена. Съвременните интеграционни процеси в рамките на ЕС, наред с многото положителни промени, които донесоха на европейския континент, засилиха и усещането за несигурност и дори безнаказаност на организираната престъпност с транснационален елемент, която бързо се възползва от различното законодателство на държавите-членки на Европейския съюз.

Една от най-големите заплахи за сигурността и стабилното икономическо развитие на държавите от Европейския съюз е организираната престъпност. Изпълнителният директор на бюрото на ООН за мониторинг на престъпленията и наркотиците (UNODC) Юрий Федотов¹¹ заяви по време на конференция, посветена на проблема с трансграничната престъпност, която се проведе във Виена през октомври 2012 г. „Способни сме да изчислим печалбата на организираната престъпност в световен мащаб, тя е 870 млрд. долара. Но не можем да пресметнем нещастieto и страданията, причинени на милиони хора от тези нелегални дейности”.

¹¹ <https://profit.bg/svetat/organizirana-prestapnost-po-sveta-s-870-mlrd-dolara-godishna-pechalba/>

Все по-силно се откроява значимостта на сътрудничеството между държавите и международните организации за ефективно противодействие на организираната престъпност. Резултатното сътрудничество в борбата с международната организирана престъпност в значителна степен зависи от сближаването на националните правни системи с цел ефикасно и оперативно взаимодействие между държавите. Това е основна задача на вътрешните законодателства, включително на страните от Европейския съюз.

С приемането на Хагската програма за укрепване на свободата, сигурността и правосъдието в ЕС през 2004 г. Съветът на ЕС определи противодействието и превенцията на организираната престъпност като приоритет в политиката на Общността. В плана за изпълнение на програмата и в Съобщението на Комисията до Съвета и Европейския парламент от 2 юни 2005 г. се предвижда разработването на стратегическа концепция за борба с организираната престъпност, основаваща се на проактивно събиране на информация и разузнавателни данни, превенция и сътрудничество между правоприлагащите и съдебните органи, трети страни и организации. Така се поставя началото на *европейската оценка на заплахите от организираната престъпност* (на англ. съкратено ОСТА), изготвена за първи път в края на 2005 г. от Европол¹². ОСТА е документ, насочен към бъдещето, който поставя акцент върху качествената оценка на многоаспектния феномен организирана престъпност. Според изводите на Хагската програма ОСТА на Европол трябва да се превърне в ключов елемент на европейския проактивен модел за борба с престъпността (European Crime Intelligence Model).

На 5 октомври 2010 г. Постоянният комитет за оперативно сътрудничество в областта на вътрешната сигурност (COSI) постигна съгласие за установяването на цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност и набеляза отделните стъпки, необходими за пълното му прилагане. Заклученията на Съвета относно създаването и прилагането на *цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност* бяха приети от Съвета на 8 ноември 2010 г.¹³.

Цикълът на политиката е методология, възприета от ЕС през 2010 г., за справяне с най-значимите криминални заплахи. Всеки цикъл продължава четири години и оптимизира координацията и сътрудничеството по подбрани приоритети в борбата с престъпността. Заплахите от престъпления се определят въз основа на данните от криминалното разузнаване и след това се потвърждават на политическо равнище. В хода на цикъла всички съответни служби и заинтересовани страни на национално и европейско равнище се приканват да заделят средства и да съдействат за взаимното укрепване на усилията. Следят се и възникващи заплахи с цел ефикасно реагиране.

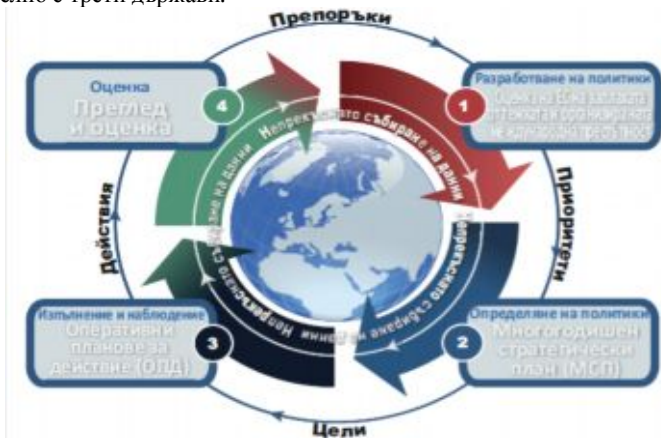
Целта на т. нар. *цикъл на политиката на ЕС* е да се осигури ефективно сътрудничество между правоприлагащите органи на държавите членки, институциите и агенциите на ЕС, което следва да доведе до съгласувани и стабилни оперативни действия, насочени към най-неотложните криминални заплахи, пред които е изправен ЕС. Това е основан на факти процес, който започва с представянето от страна на Европол на *оценката на заплахата от тежката и организираната престъпност (EU SOCTA)*, която включва набор от препоръки относно основните заплахи

¹² Оценка на заплахите от тежка организирана престъпност 2010г.-2011г., Център за изследване на демокрацията, София 2012 г., стр.10

¹³ док. 15358/10

от престъпност, пред които е изправен ЕС. EU SOCTA служи за основа на обсъжданията между държавите членки относно приоритетите за преодоляване на заплахите от престъпност на равнището на ЕС. След това приоритетите се приемат от Съвета по правосъдие и вътрешни работи, след което се отразяват в трансграничните оперативни действия на равнището на държавите членки, по-специално чрез съвместни действия между държавите членки и агенциите на ЕС с подкрепата на Европейската мултидисциплинарна платформа за борба с криминални заплахи¹⁴. Комисията е предоставяла и продължава да предоставя финансова подкрепа за изпълнението на цикъла на политиката на ЕС и за 2017 г. са отпуснати 4 милиона евро в допълнение към финансирането в размер на 9 милиона евро през 2015 и 2016 г.

Като цяло настоящият цикъл на политиката на ЕС (2013–2017 г.) се изпълнява успешно. Независима оценка¹⁵, възложена от Комисията, стигна до заключението, че той е постигнал основната си цел за подобряване на сътрудничеството между държавите членки в борбата с тежката и организираната престъпност¹⁶. Цикълът на политиката на ЕС е довел до по-добър обмен на информация и на добри практики и до започването на много съвместни разследвания и операции от страна на държавите членки. Той също така е допринесъл за изграждането на отношения и доверие, включително с трети държави.



Фиг. 1. Цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност¹⁷.

Етапи в цикъла на политиката:

1) Оценка на заплахата от тежката и организираната престъпност (SOCTA). Европол изготвя SOCTA въз основа на данни от правоприлагащите органи на държавите членки, на собствените си бази данни, на данни от други агенции

¹⁴ <https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact>

¹⁵ Проучване за оценка на цикъла на политиката на ЕС за борба с организираната и тежката международна престъпност за периода 2013–2017 г., окончателен доклад, 30.1.2017 г.

¹⁶ Настоящият цикъл на политиката на ЕС има 9 приоритета: подпомагане на незаконната имиграция, трафик на хора, фалшифицирани стоки, измами с акцизи и ДДС, кокаин и хероин, синтетични наркотици, незаконен трафик на огнестрелни оръжия, организирана престъпност, засягаща собствеността, и киберпрестъпност.

¹⁷ Съвет на ЕС, Цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност, www.consilium.europa.eu/bg/documents-publications/.../2015/.../qc0114638bgn.pdf/

на ЕС, като Frontex, Евроюст и ЕЦМНН, от трети държави – партньори на Европол, и трети частни партньори, както и въз основа на данни от отворени източници. SOCTA съдържа:

- анализ на настоящите и бъдещите заплахи за ЕС, породени от тежката и организираната престъпност;

- препоръки за приоритети в борбата с престъпността.

2) **Избор на приоритети в борбата с престъпността и многогодишни стратегически планове (МСП).** Постоянният комитет за оперативно сътрудничество в областта на вътрешната сигурност (COSI) разглежда препоръчаните в SOCTA приоритети. На тази основа министрите на правосъдието и вътрешните работи приемат приоритетите на ЕС в борбата с престъпността за съответния цикъл на политиката (т.е. за следващите четири години), като вземат предвид бележките на държавите членки, агенциите и Комисията, както и други имащи отношение оценки и политики. Впоследствие Комисията свиква среща на представители от държавите членки, агенциите в областта на правосъдието и вътрешните работи и институциите на ЕС за изготвянето на 4-годишен МСП (за всеки приоритет по един МСП). МСП съдържа списък на общите цели („стратегически цели“), които трябва да бъдат постигнати по време на цикъла. Тези МСП се одобряват от COSI.

3) **Оперативни планове за действие (ОПД) и отчитане на ръководителите.** МСП се изпълняват посредством оперативни планове за действие (ОПД) – по един за всеки приоритет и за всяка година. Те се изготвят от представители на участващите държави членки, на институции и агенции на ЕС. Тези ОПД се одобряват от COSI. ОПД включват съвместни действия на държавите членки/агенциите, както и действия на агенции и национални действия. Съвместните действия се осъществяват под формата на проекти на Европейската мултидисциплинарна платформа за борба с криминални заплахи (ЕМРАСТ). Тази рамка предоставя платформа за структурирано сътрудничество на съответните държави членки, институции и агенции на ЕС, както и трети партньори. За изпълнението на всеки ОПД отговаря „ръководител“ от държавата членка, изразила желание да оглави работата по приоритета, а за изпълнението на национално равнище следят националните координатори на ЕМРАСТ. Звеното за подпомагане на ЕМРАСТ към Европол осигурява административна и логистична подкрепа за проектите на ЕМРАСТ и наблюдава техния напредък. Европол определя и отговорници по подпомагането на ЕМРАСТ, които да осигуряват оперативна подкрепа за всички приоритети в борбата с престъпността. COSI одобрява ОПД и следи тяхното изпълнение въз основа на шестмесечни доклади от ръководителите чрез звеното за подпомагане на ЕМРАСТ.

4) **Преглед на Комисията и междинна оценка.** Ежегодното докладване на ръководителите и междинната оценка на Европол позволяват при необходимост адаптиране/видоизменение на МСП или на приоритетите. Всяка година Комисията запознава COSI с актуалното състояние, а в края на цикъла на политиката прави задълбочена и независима оценка. Направените в резултат на тази оценка изводи захранват следващия цикъл на политиката.

Приоритети на ЕС в борбата с престъпността за периода 2014–2017 г. (приети през юни 2013 г.):

- съдействието за незаконна имиграция, особено в изходните страни, при основните входни пунктове на ЕС, по основните маршрути, по алтернативни канали, и свързаните с това злоупотреби със законни канали за миграция;

- трафика на хора, особено с цел трудова и сексуална експлоатация, и свързаните с това злоупотреби със законни стопански структури;
- производството и разпространението на фалшифицирани стоки, с които се нарушават нормите в областта на здравеопазването, безопасността и храните, както и на стоки, които не отговарят на стандартите;
- измамите с акцизите и вътреобщностните измами с липсващ търговец;
- производството и трафика на синтетични наркотици в ЕС;
- трафика на кокаин и хероин в ЕС и разпространението им в ЕС;
- киберпрестъпленията, и по-специално онлайн измамите и измамите с разплащателни карти, сексуалната експлоатация на деца онлайн и кибератаките, които засягат критична инфраструктура и информационни системи в ЕС;
- незаконния трафик на огнестрелни оръжия;
- организираните престъпления срещу собствеността, извършвани от мобилни организирани престъпни групи.

Новият цикъл на политиката започна с представянето от Европол на 9 март 2017 г. на доклада EU SOCTA за 2017 г. В доклада се разглеждат потенциалните **връзки между тежката и организираната престъпност и тероризма**, а именно това, че организираната престъпност може да подхранва тероризма чрез дейности като трафика на огнестрелни оръжия и производството на фалшиви документи или чрез постъпления от контрабандата на наркотици. Това е подходът, предложен в Европейската програма за сигурност, който е застъпен в Съобщението на Комисията относно изпълнението на Европейската програма за сигурност с цел борба срещу тероризма и подготвяне на условията за ефективен и истински Съюз на сигурност¹⁸.

В EU SOCTA за 2017 г. се препоръчва вниманието да се съсредоточи върху петте приоритетни заплахи от престъпност: 1) **киберпрестъпност**, 2) **производство, трафик и разпространение на наркотици**, 3) **контрабанда на мигранти**, (4) **организираните обири и кражби** (организирана престъпност, засягаща собствеността) и 5) **трафик на хора**. В доклада се препоръчва също така да се разрешат три взаимосвързани проблема, които способстват или насърчават всички форми на тежката и организираната престъпност: а) документните измами, б), финансирането на престъпления, включително изпирането на пари, и в) онлайн търговията с незаконни стоки и услуги.

Въз основа на EU SOCTA за 2017 г. Комисията и председателството на Съвета са в процес на изготвяне на своите предложения за приоритетите на новия цикъл в политиката на ЕС за периода 2018-2021 г. за справяне с престъпността, които ще бъдат обсъдени в рамките на Постоянния комитет за оперативно сътрудничество в областта на вътрешната сигурност и одобрени през юни 2017 г. от Съвета по правосъдие и вътрешни работи.

С оглед на определянето на бъдещите приоритети на ЕС за борба с тежката и организираната престъпност Комисията подкрепя петте приоритетни заплахи от престъпност, идентифицирани от Европол. Освен това Комисията счита, че на равнището на ЕС следва също да се отделят особено внимание и финансови ресурси за преодоляване на следните три заплахи от престъпност: 6) **трафик на огнестрелни оръжия**, 7) **измами с ДДС** и 8) **престъпления против околната среда**.

Тези три области следва също така да бъдат приоритетни заплахи от престъпност в рамките на новия цикъл на политиката на ЕС.

В EU SOCTA за 2017 г. е подчертан следния ключов проблем, а именно **използването на нови технологии от престъпниците**. За почти всички видове организирана престъпност престъпниците разширяват обхвата на технологиите и ги приспособяват все по-умело и с все по-голямо въздействие. Използването на интернет за всички видове незаконна търговия със стоки и услуги се увеличи значително. Това налага правоприлагащите органи да бъдат оборудвани с подходящи средства за борба с този вид онлайн престъпност и да се обучават и учат заедно. Агенцията на Европейския съюз за обучение в областта на правоприлагането ще изиграе ключова роля при осигуряването на подходящо обучение за правоприлагащите служители на първа линия в съответствие с приоритетите на политиката и установените заплахи.

В EU SOCTA за 2017 г. се подчертава, че съществува и важно **външно измерение на тежката и организираната престъпност**. Хора от над 180 различни националности - пребиваващи в ЕС или извън него, участват в организирана престъпна дейност в рамките на ЕС. Около 40 % от заподозрените лица не са граждани на държавите членки. Основните пътища за трафик, свързани със заплахите от организираната престъпност, тръгват от държави извън ЕС. Работи се за преодоляване на заплахите от организираната престъпност във външен план¹⁹. Важно е да се отговори на заплахите от тежката и организираната престъпност, като се продължи осигуряването на връзки между вътрешната сигурност на ЕС и външната му дейност, включително чрез сътрудничество на Европол с трети държави.

Приоритетите за периода 2018–2021 г. на ЕС в борбата с тежката и организираната престъпност са:

1) Киберпрестъпност. Кибератаките се увеличават по интензитет, обем и качество. По своето естество киберпрестъпността е международна: жертвите, престъпниците и доказателствата често се намират в различни държави и са под различни юрисдикции. Държавите членки проявиха жив интерес към приоритета киберпрестъпност, както е видно от броя на оперативните планове за действие²⁰, създадени в областта на кибератаките, сексуалната експлоатация на деца онлайн и измамите с разплащателни карти. На равнището на ЕС значителен принос в борбата с киберпрестъпността²¹ има Европейският център за борба с киберпрестъпността на Европол (EC3). Евроюст работи в тясно сътрудничество с EC3 чрез командироването на експерт и членство в съвета на програмата. EC3 също така е домакин на съвместната работна група за борба с киберпрестъпността. Неговата мисия е да насърчава координираните действия, основани на разузнавателна информация, срещу ключови заплахи в областта на киберпрестъпността чрез трансгранични разследвания и операции със своите партньори.

19 Това включва проекти, финансирани от ЕС (например в Западните Балкани и региона Сахел), мисии по линия на общата политика за сигурност и отбрана (като например EUNAVFOR Med операция Sophia, която изрично е разработена така, че да се разруши също бизнес моделът на контрабандистите), както и мисиите за управление на границите в трети държави.

20 Оперативните планове за действие (ОПД) са разработени за всеки един от приоритетите на Европейската мултидисциплинарна платформа за борба с криминални заплахи (EMPACT) с цел координиране на действията от страна на държавите членки и организациите на ЕС срещу идентифицираните заплахи. Що се отнася до киберпрестъпността, през 2015 г. и 2016 г. бяха стартирани 114 оперативни плана за действие.

21 От създаването си EC3 е участвал в десетки знакови операции и в над 200 мисии за оперативна подкрепа на място. В резултат на това бяха направени стотици арести и анализирани над 800 000 файла, за по-голямата част от които бе доказано, че са зловредни.

По-нататъшните стъпки включват проучване на възможните решения за отстраняване на пречките пред наказателните разследвания на киберпрестъпността, като се определят конкретни инициативи за достъп до доказателства и информация. Сътрудничеството за борба с киберпрестъпността трябва да запази акцента си върху идентифицирането и защитата на жертвите въз основа на действащите права на жертвите, установени в законодателството на ЕС, и настоящите най-добри практики²². Сътрудничеството в борбата със сексуалната експлоатация на деца онлайн трябва да продължи и да се засили допълнително. Що се отнася до измамите с разплащателни карти, необходимо е съществуващото сътрудничество в областта на правоприлагането да се разшири към по-широк кръг от престъпни дейности, чийто обект са непаричните платежни средства. Както беше посочено в плана за действие с цел засилване на борбата с финансирането на тероризма, Комисията в процес на изготвяне на актуализация на рамковото решение от 2001 г. относно борбата с измамата и подправянето на платежни средства, различни от парите в брой.

2) Производство, трафик и разпространение на наркотици. Пазарът на незаконните наркотици продължава да е най-големият престъпен пазар в ЕС. EU SOCTA за 2017 г. показва, че повече от една трета от престъпните групи, действащи в ЕС, участват в производството, трафика или разпространението на различни видове наркотици. Пазарът на наркотици за търговия на дребно в ЕС възлиза на поне 24 милиарда евро годишно. Трафикът на наркотици също така подпомага неформалната икономика, а неговите странични ефекти са проявите на насилие и други незаконни дейности, създаващи сериозни социални проблеми.

ЕС предприема действия срещу трафика на наркотици в рамките на Стратегията на ЕС за борба с наркотиците за периода 2013-2020 г., които са насочени към намаляване както на търсенето, така и на предлагането на наркотици. На 15 март Комисията предложи проект на нов план за действие на ЕС по отношение на наркотиците за периода 2017-2020 г. С цел да се даде възможност ЕС да реагира по-бързо и по-ефективно спрямо новите психоактивни вещества през декември 2016 г. Съветът постигна съгласие по общ подход във връзка с нов законодателен пакет за справяне с новите психоактивни вещества и за установяване на контрол на вредните вещества на равнището на ЕС.

3) Контрабанда на мигранти. Контрабандата на мигранти не само стимулира незаконната миграция към ЕС, като по този начин подкопава сигурността на границите и управлението на миграцията, но също така представлява тежка форма на престъпност, която във все по-голяма степен излага мигрантите на риск от насилие, експлоатация и смърт. Контрабандата на мигранти към ЕС понастоящем е една от най-бързо разрастващите се форми на организирана престъпност²³.

В Европейската програма за миграцията, както и в Плана за действие на ЕС срещу контрабандата на мигранти е установена необходимостта от това да се даде приоритет на по-успешното предотвратяване на контрабандата на мигранти и борбата с нея, включително на намаляването на незаконната миграция и на човеш-

22 Например проектът „NoMoreRansom“ — <https://www.nomoreransom.org/>, под ръководството на Европол и с участието на правоприлагащите органи и частни организации за подпомагане на жертви на зловреден софтуер, с който са криптирани техните данни (софтуер за изнудване); по линия на този проект на жертвите се предоставят необходимите инструменти, с които да декриптират своя софтуер и да възстановят информацията.

23 По данни на Европол поне 90 % от всички мигранти и лица, търсещи убежище, които стигат незаконно до ЕС, са ползвали услугите на контрабандисти за тази цел. През 2015 г. мрежите за контрабанда на мигранти, които предлагат спомагателни услуги за пристигане в ЕС или придвижване на неговата територия, са генерирали печалба, оценявана между 4,7 милиарда евро и 5,7 милиарда евро.

ки загуби в Средиземно море. Увеличаването на подкрепата от страна на Европол, включително чрез създаването на специален Европейски център за борба с контрабандата на мигранти, има за цел да спомогне за преодоляването на тези предизвикателства. Отчетът за неговата дейност през първата година от създаването му показва цялостната подкрепа, която Центърът предоставя на европейските полицейски органи и на органите за граничен контрол в координирането на изключително сложните трансгранични операции за борба с контрабандата. Евроюст определи също и съдебни точки за контакт на „горещите точки“ в Гърция и Италия с цел насочване на съответната информация и случаи към националните бюра на Евроюст за последващи съдебни действия и координация на равнището на ЕС. Борбата с контрабандата на мигранти също така е важна дейност по маршрута през Централното Средиземноморие, както е предложено в съвместното съобщение от 25 януари 2017 г.²⁴.

4) Организирана престъпност, засягаща собствеността. Организираната престъпност, засягаща собствеността, обхваща широк набор от различни престъпни деяния, извършвани от високоспециализирани мобилни групи на организираната престъпност, действащи в ЕС, по-специално чрез организирани обيري, кражби, грабежи и престъпления, свързани с моторни превозни средства²⁵. Тя обаче често не се разследва в достатъчна степен, тъй като отделните инциденти често се класифицират като дребни престъпления. Увеличаването на броя на обирите на жилища, което се дължи на пътуващи престъпни групи с произход главно от Югоизточна и Източна Европа, е основен проблем в областта на правоприлагането. За противодействие на тази форма на престъпност с висока степен на мобилност е приоритет²⁶ сътрудничеството между правоприлагащите органи в рамките на ЕС, но и с държавите партньори в съседство.

5) Трафик на хора. Трафикът на хора е заплаха, на която ЕС отдава приоритет от повече от десетилетие, който трябва да се запази и през следващия цикъл на политиката. Това е една от най-тежките форми на организирана престъпност и грубо нарушение на човешките права, но също и един от най-печелившите престъпни пазари²⁷. Трафикантите често разчитат в огромна степен на документни измами за целите на трафикантската си дейност²⁸. ЕС е разработил ефективна и всеобхватна правна и политическа рамка за справяне с трафика на хора, по-специално Директива 2011/36/ЕС относно предотвратяването и борбата с трафика на хора и защитата на жертвите от него и Стратегията на ЕС за премахване на

24 JOIN(2017) 4 final, 25.1.2017 г.

25 В EU SOCTA за 2017 г. се отчита постоянно покачване на броя на регистрираните обيري през последните години, като оценките сочат, че на всеки 1,5 минути в ЕС се извършва обир, а в някои държави членки се регистрират по 1000 обира дневно.

26 Пример за трансгранично сътрудничество в областта на правоприлагането е операция „Turnstone“, проведена през май 2015 г. срещу тежката трансгранична организирана престъпност, засягаща собствеността, в региона на Балтийско море. Близко 80 000 субекта от списъците на пътници и фериботни линии, действащи в Балтийско море, бяха проверени както в националните бази данни, така и базите данни на Европол, в резултат на което бяха открити 325 цели с висока стойност. Нарушителите бяха арестувани след интензивна операция за наблюдение, при която заподозрените.

27 Според доклада на Европол от 2015 г. относно финансовия бизнес модел на трафика на хора прогнозната печалба в световен мащаб от всички форми на трафик на хора е 29,4 милиарда евро годишно. Средният годишен доход на един трафикант на хора е около 70 000 евро. Прогнозната годишна печалба в световен мащаб от трафика на хора, свързан със сексуална експлоатация, е 25,8 милиарда евро и съответно 3,5 милиарда евро от трафика на хора, свързан с трудова експлоатация.

28 През декември 2016 г. Комисията прие план за действие за укрепване на европейския отговор по отношение на измамите с документи за пътуване (COM(2016) 790 final, 8.12.2016 г.). На 27 март Съветът прие заключенията, с които се подкрепя планът за действие, и призова за бързото му изпълнение.

трафика на хора за периода 2012-2016 г.²⁹. Понастоящем Комисията разглежда какви действия са необходими за политическата рамка за периода след 2016 г. въз основа на съществуващата рамка и на оценка на резултатите от нея.

6) Трафик на огнестрелни оръжия. Националните черни пазари са основният източник на огнестрелни оръжия за терористите и престъпниците. Този пазар се захранва чрез кражби или отклоняване от законни оръжейни пратки и депа. Понастоящем най-разпространеният начин за трафик на огнестрелни оръжия в ЕС е чрез продажба онлайн в тъмната мрежа и доставка с обикновена поща и колетни услуги. Броят на случаите, свързани с разследвания на трафик на огнестрелни оръжия в тъмната мрежа, нараства (2 % през 2014 г., около 6,5 % през 2015 г. и 9 % през 2016 г.). Разглеждането на трафика на огнестрелни оръжия като приоритет в настоящия цикъл на политиката на ЕС показва резултати предвид по-голямата ангажираност на държавите членки (от 12 на 22 участващи държави) и по-широкото участие от страна на митническите органи³⁰. Налице е също така нарастващо сътрудничество с международни партньори (Интерпол, СНПООН) и регионално сътрудничество (по-специално в Западните Балкани), което доведе до средно 17 действия годишно през последните три години³¹. За да пресече доставките на оръжие, които са на разположение на престъпниците и терористите, Комисията счита, че този приоритет следва да бъде запазен в настоящия цикъл с цел допълване на постигнатото през март съгласие за затыгане на контрола върху законно притежаваните огнестрелни оръжия, включително разширяването на обхвата на забраните относно най-опасните оръжия³².

7) Трансгранични измами с ДДС. Организираните престъпни групи причиняват годишни загуби от приходи от ДДС в размер между 40 и 60 милиарда евро чрез трансгранични измами с ДДС, а 2 % от тези групи са отговорни за 80 % от вътреобщностните измами с липсващ търговец. Схемите за измами са изключително сложни и трудни за откриване, поради което е необходим координиран подход от страна на данъчните администрации и правоприлагащите органи. На равнището на ЕС Eurofisc - мрежа от данъчни служители - предоставя бърз и многостранен обмен на целева информация за борба с тежките трансгранични измами, свързани с ДДС. Тя обработва разузнавателна информация от първостепенно значение във връзка с измамниците и новите тенденции в измамите. Като се имат предвид финансовите загуби, дължащи се на трансгранични измами с ДДС, организирани от престъпни групи, Комисията счита, че това е въпрос, който следва да се включи в новия цикъл на политиката на ЕС. Както беше обявено, Комисията ще представи предложение през септември 2017 г. за преминаване към единно пространство на ЕС по отношение на ДДС, като се премахнат основните слабости на системата, за да се намалят значително трансграничните измами³³. След създаването на Европейската прокура-

29 COM(2012) 286 final, 19.6.2012 г.

30 Включени са 22 държави членки (BE, BG, DK, EL, ES, FI, FR, MT, NL, PT, RO, SI, SE, UK, LU, PL, HU, SK, AT, HR, DE и CY). Участват девет институции, агенции и мрежи: Комисията, Европол, CEPOL, Евроюст, ЕСВД, Европейската група на експертите по огнестрелни оръжия (EFE), Интерпол, Frontex, EU-LISA и трети страни: Швейцария, US-ATF.

31 Действията варират от сближаването на националното законодателство и създаването на централизирани, координационни органи („национални координатори“) до подобряването на обмена на информация и разузнавателни данни, обучения или съвместни транснационални разследвания и операции по правоприлагане (в Западните Балкани, насочени към газометеосигналните оръжия, видеоизменените оръжия и онлайн търговията или доставката на колетни пратки).

32 COM(2015) 750 final, 18.11.2015 г.

33 План за действие относно ДДС: към единно пространство на ЕС по отношение на ДДС - Време за избор (COM(2016) 148 final, 7.4.2016 г.

тура³⁴ тя ще бъде основният фактор в борбата с престъпленията, засягащи финансовите интереси на Съюза. Европейската прокуратура ще има правомощия да разследва и да преследва такива престъпления в целия ЕС, включително сериозни трансгранични измами с ДДС, свързани с щети в размер на най-малко 10 милиона евро. Това важи особено за схемите за верижна измама и за измама с липсващ търговец, които често са свързани със структури на организираната престъпност.

8) Престъпления против околната среда. Престъпленията против околната среда са на стойност между 91 и 258 милиарда щатски долара годишно и нарастват 2-3 пъти по-бързо от темпа на световната икономика. Поради това те представляват четвъртата по големина престъпност в света след трафика на наркотици, фалшифицирането и трафика на хора. ЕС е пазарът на произход (напр. незаконен трафик на отпадъци) или на местоназначение (напр. защитени видове, незаконен дървен материал) и/или разпределителният център за транзитен трафик към други региони (напр. продукти от дивата фауна и флора като слоновата кост)³⁵.

Значимостта на престъпленията против околната среда бе призната на равнището на ЕС чрез приемането на Директивата относно престъпленията срещу околната среда³⁶. Наказателните кодекси на държавите членки бяха приведени в съответствие с нейните изисквания за санкциониране на различните категории престъпления против околната среда, включително престъпленията, свързани с третирането на отпадъци и със защитените видове. През февруари 2016 г. ЕС прие също План за действие на ЕС³⁷ срещу трафика на екземпляри от дивата флора и фауна, който понастоящем е в процес на изпълнение. Комисията също така подкрепя и си сътрудничи с мрежи на ЕС от полицейски служители, прокурори, инспектори и съдии, специализирани в борбата с престъпленията против околната среда³⁸. Предвид тяхното икономическо отражение, това, че представляват сериозна заплаха за сигурността, и пагубното въздействие върху природата, Комисията счита, че престъпленията против околната среда следва също да бъдат включени в новия цикъл на политиката на ЕС.

Целият цикъл EMPACT се стреми да осигури приемственост в борбата срещу международна организирана престъпност чрез сътрудничество между националните правоприлагащи органи, институциите и агенциите на ЕС и други заинтересовани партньори.

В началото на цикъла на политиката SOCTA предоставя аналитични констатации, които информират политическите приоритети, стратегическите цели и оперативните планове за действие. Той идентифицира и оценява заплахите за ЕС и анализира точките на уязвимост към престъпления, както и възможностите, които престъпниците създават, за да ги ангажират.

34 На 3 април 16 държави членки уведомиха трите институции на ЕС за своето намерение да започнат засилено сътрудничество за създаване на Европейската прокуратура.

35 През 2015 г. Европол координира глобална операция за борба с престъпленията срещу дивата природа COBRA III, в която взеха участие 25 държави — членки на ЕС, Интерпол и Евроюст в рамките на групата за правоприлагане в търговията с видове на дивата флора и фауна. Операцията бе насочена главно срещу контрабандистите на слонова кост и на рогове от носорози, които осъществяват дейност по маршрута от Африка през Европа към азиатските пазари (основно китайския и вьетнамския пазар). Тя включваше 70 сложни разследвания в 25-те участващи държави и 600 изземвания, включително на големи количества лекарства от алтернативната медицина, съдържащи екстракти от защитени растения, и на няколко хиляди килограма защитен дървен материал. Вж. Преглед на Европол за 2015 г.

36 Директива 2008/99/ЕО относно защитата на околната среда чрез наказателно право (ОВ L 328, 6.12.2008 г., стр. 28).

37 COM(2016) 87 final, 26.2.2016 г.

38 EnvCrimeNet, Европейска мрежа на прокуратурите за околната среда (ENPE), Мрежа на Европейския съюз за изпълнение и правоприлагане на правото в областта на околната среда (IMPEL) и Форум на съдиите от Европейския съюз за околната среда (EUFJE).

При подготовката на SOCTA Европол анализира тенденциите и моделите в актуалните данни за престъпността, но също така да се провери средата и за други фактори, които може да се очаква да повлияят на извършването на престъпления и способността на правоохранителните органи да ги спре. Това осигурява основата за прогнозата на бъдещи заплахи за вътрешната сигурност на ЕС.

SOCTA се изготвя от Отдела по операции на Европол, който се основава на широк принос от външни партньори, включително държави-членки, трети държави и организации: Eurojust (Евроюст) и Frontex (Фронтекс)

Програмата за сигурност определя три приоритета за действия на ЕС, като се насочва към областите, в които съюзът би могъл да има значителен принос:

1) Тероризмът и радикализацията са значителни заплахи за вътрешната сигурност на ЕС;

2) Организираната престъпност има огромна човешка, социална и икономическа цена – в това число незаконното превеждане на хора през граница, трафика на хора, трафика на огнестрелни оръжия, наркотици, екологичните, финансовите и икономическите престъпления;

3) Киберпрестъпността предлага огромна потенциална печалба за престъпниците, тъй като животът ни, в това число търговията и банкирането, се преместват в онлайн пространството. Подобрването на ответните действия на правоприлагащите и съдебните органи спрямо киберпрестъпността е приоритет в Европейската програма за сигурност.

За справяне с тези заплахи програмата има за цел да укрепи и да повиши ефективността на обмена на информация и на оперативното сътрудничество между държавите членки, агенциите на ЕС и сектора на информационните технологии. Европейската програма за сигурност трябва да бъде обща програма. Тя ще доведе до резултати в борбата с тероризма и трансграничната престъпност само ако всички участници в процеса положат по-големи усилия за по-добро сътрудничество, в това число институциите на ЕС, държавите членки, агенциите на ЕС и съответните участници от гражданското общество.

Изводи:

1. Задълбочават се политиките, които ЕС може да осъществи по отношение на основните области на действие на организираната престъпност и по-конкретно: търговията с хора и тяхната експлоатация; международният трафик на наркотици; трафикът на оръжие; изпирането на пари и финансовите престъпления; корупцията, взаимно проникване и взаимно съществуване на организираната престъпност, политика и публична администрация и отклоняване на обществени средства (по-специално европейски средства) от страна на организираната престъпност; екомафия и престъпления спрямо околната среда; киберпрестъпност; фалшифициране на стоки и свързан с тази дейност трафик; изнудване и лихварство.

2. Чрез т. нар. цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност се цели да се осигури ефективно сътрудничество между правоприлагащите органи на държавите членки, институциите и агенциите на ЕС, което следва да доведе до съгласувани и стабилни оперативни действия, насочени към най-неотложните криминални заплахи, пред които е изправен ЕС. Всеки цикъл продължава четири години и оптимизира координацията и сътрудничеството по подбрани приоритети в борбата с престъпността. Заплахите от престъпления

се определят въз основа на данните от криминалното разузнаване и след това се потвърждават на политическо равнище.

3. Оценката на заплахата от тежката и организираната престъпност от 2017 г. е добра основа за определяне на приоритетите на ЕС в борбата с престъпността за следващите четири години. Одобрени са следните осем заплахи от престъпност като приоритети в цикъла на политиката на ЕС за борба с организираната и тежката международна престъпност за периода 2018-2021 г.: киберпрестъпността, престъпността, свързана с наркотици, организираната престъпност, засягаща собствеността, трафика на хора, трафика на огнестрелни оръжия, измамите с ДДС и престъпленията против околната среда.

Литература:

1. Заключение на Съвета относно създаването и прилагането на цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност (док. 15358/10)

2. Заключение на Съвета за определяне на приоритетите на ЕС в борбата срещу тежката и организираната престъпност за периода 2014–2017 г. (док. 12095/13)

3. Мандат на ЕМПАСТ (док. 14518/12)

4. Работен документ относно организираната престъпност, Специална комисия по организираната престъпност, корупцията и изпирането на пари, Докладчик: Salvatore Iacolino, 1.10.2012.

5. Доклад на комисията до Европейския парламент, Европейския съвет и Съвета, Шести доклад за напредъка по създаването на ефективен и истински Съюз на сигурност, Брюксел, 12.4.2017 г. COM(2017) 213 final

6. Интегрирана стратегия за превенция и противодействие на корупцията и организираната престъпност, www.strategy.bg/FileHandler.ashx?fileId=968

7. Проучване за оценка на цикъла на политиката на ЕС за борба с организираната и тежката международна престъпност за периода 2013-2017 г., окончателен доклад, 30.1.2017 г.

8. Европейско сътрудничество за борба с организираната престъпност, Венета Кокалова, София, 2009г.

9. Съвет на ЕС, Цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност, www.consilium.europa.eu/bg/documents-publications/.../2015/.../qc0114638bgn_pdf/

10. Оценка на заплахите от тежка организирана престъпност 2010г.-2011г., Център за изследване на демокрацията, София 2012 г.

11. Доклад относно организираната престъпност в Европейския съюз, (2010/2309(INI)), Комисия по граждански свободи, правосъдие и вътрешни работи, (A7-0333/2011), Европейски парламент 6.10.2011 г.

12. Съобщение на комисията до Европейския парламент, Европейския съвет и Съвета, изпълнение на Европейската програма за сигурност с цел борба срещу тероризма и подготвяне на условията за ефективен и истински Съюз на сигурност, COM(2016) 230 final, 20.4.2016 г.

К. К. Казаков,

ПРИНЦИПИ НА РАЗУЗНАВАТЕЛНИЯ АНАЛИЗ И СИНТЕЗ

Константин К. Казаков

Университет по библиотекознание и информационни технологии, гр.София
бул.“Цариградско шосе“119, e-mail: kkazak@mail.bg

PRINCIPLES OF INTELLIGENCE ANALYSIS AND SYNTHESIS

Konstantin K. Kazakov

Abstract: In this paper, it has shown that the analysis-synthesis process proceeds from intelligence analysis to operations analysis and then to policy analysis. The knowledge-based intelligence enterprise requires the capture and explicit representation of such models to permit collaboration among these three disciplines to achieve the greatest effectiveness and sharing of intellectual capital. Also it has shown the basic concepts of reasoning and approaches to explicitly model intelligence topics and targets. A collaborative intelligence analysis-synthesis process requires such explicit modeling.

Keywords: Intelligence, Analysis and Synthesis

Неопределеността и повишената динамика на промените в съвременната среда за сигурност генерират нови предизвикателства към разузнавателните служби и към системата за защита на национална сигурност, като цяло. Ясното дефиниране и изучаване на процесите в разузнаването спомагат за повишаване на тяхната ефективност и адаптивност към новите условия. От друга страна добре структурираните описателно – обяснителни модели на процесите в разузнавателната дейност позволяват по – ефективен граждански контрол върху системата за защита на националната сигурност.

Разузнавателният анализ и синтез е част от стойностната верига на информационния процес започващ от придобиването на данни и цели създаването на ново знание за средата за сигурност, което да се използва за взимане на управленски решения.

В основата на създаването на знание стоят мисловни процеси, които се базират на известното към даден момент за неизвестното преди този момент. За разузнавателния анализ това е процес, чрез който доказателствата (всички данни, които се определят като релевантни към даден проблем) се използват за извличане на знание, необходимо за взимане на управленски решения. Трябва да се отбележи, че обикновено в практиката наличните данни са недостатъчни, неподредени във времето, двусмислени и дори подвеждащи.

Разузнавателният анализ използва функциите на анализа и синтеза за да създава разузнавателни продукти. Анализът и синтезът разграничават процесите на изследване на доказателствата, за да се обяснят целите на изследването. Анализът е процес на декомпозиране на разузнавателните данни (доказателства) на съставните им части. Целта е да се изследват взаимоотношенията между тях и да се открият

липсващите данни, като винаги фокусът е върху проблема, който трябва да се реши. Синтезът е процес на сглобяване на възможни решения (хипотези) от компонентите на доказателствата.

Разузнавателният анализ като част от информационния процес за взимане на решения

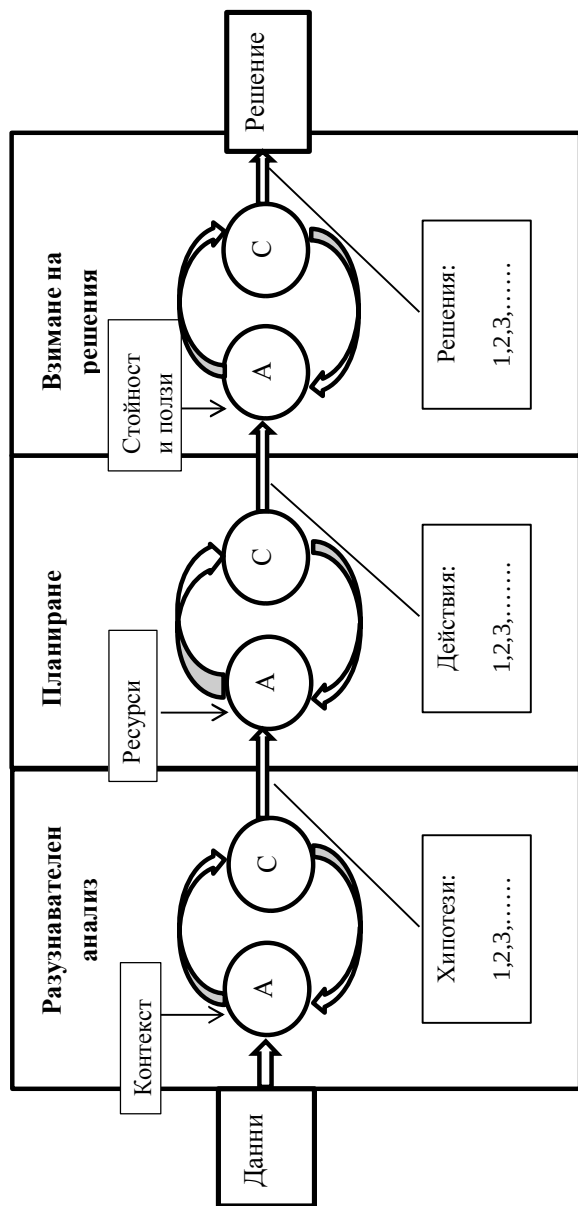
Разузнавателният анализ е част от верига от процеси за анализ и синтез, които водят до управленски решения и действия в държавата. Тези процеси са разделени на разузнавателен анализ, планиране на операции и взимане на решения (създаване на политики). (фиг.1).

- Разузнавателен анализ. Разузнаването събира и анализира данни, ръководени от контекста на проблема, разлагайки всички елементи на данните ги организира във временни, пространствени и функционални рамки. От тези данни се синтезират хипотези, обяснения или модели, които се отчитат в разузнавателен доклад;
- Планиране. Операциите приемат разузнавателния доклад и анализират последиците от хипотезата за ситуацията, преди да синтезират (планират) изпълнимите действия, които зависят от наличните ресурси;
- Взимане на решения. Създателите на политики разглеждат възможните действия в контекста на определени стойности, като цена, риск и т.н. Целта е да се определи ефекта на всяка алтернатива и въз основа на рационална селекция да се вземат решения с най-голяма ползност за обществото.

Посочените процеси се изпълняват задължително от различни организации, като във всяка от тях се използва цикъл на анализ и синтез. Изпълнителите трябва да си сътрудничат за да създадат стойностен продукт, необходим на вземащите решения. От друга страна дефинирането на трите процеса спомага за тяхното разделяне и запазване на границите между тях. Много важно е разузнаването да бъде много близко до планирането на операции и създаването на политики, но не бива да се смесва с тях за да не се загуби обективността на разузнавателните оценки.

Процесът на разсъждение, който анализира данните и синтезира обяснения изработва изводи и заключения. Те се характеризират, като процес и продукт.

- Процес. Изработването на изводи се определя от начина по който вярванията се потвърждават. Процесът може да се предвижда от специфичните (конкретни) вярвания към по-генерални, или обратното.
- Продукт. Степента на вярност на изводите, като разузнавателен продукт се определя от две категории: сигурни и с различна степен на вероятност, но по-ниска от единица.



Фиг. 1

Пътят на разсъжденията е процес, който започва от набор от данни и заявка от потребителите за да се достигне до взимане на решения. Процесът на анализ и синтез съчетава всички начини на разсъждения и мислене за да обработва наличните данни, като първо ги изследва и декомпозира, а след това ги организира в стройни доказателства. Процесът създава хипотетични обяснения на структурираните данни и ги използва за потвърждаване или опровергаване на хипотезите, които обясняват фактите и събитията.

Анализът и синтезът като процес на моделиране

Основните процеси на разсъждение се прилагат в различните практически анализи, извършвани от анализаторите, като:

- Обяснение и описание. Намират се и се свързват сродни данни, за да се обяснят обекти и събития в реалния свят;
- Откриване на отклонения. Разпознаване и идентифициране на наличието на обекти и събития, в които се откриват потенциално важни отклонения и аномалии спрямо "нормалното" или "очакваното" състояние;
- Откриване на нови модели. Откриване наличието на досега неизвестни модели в данните, които се отнасят до обекти и събития;
- Оценка. Оценява се текущото качествено или количествено състояние на обектите или събитията;
- Прогнозиране. Предвиждат се бъдещи събития въз основа на откриването на известни показатели. Екстраполира се текущото състояние, проектират се ефектите от линейни фактори или се симулират ефектите от сложни фактори, с цел синтез на възможни бъдещи сценарии и разкриване на възникващи очаквани и неочаквани събития.

Във всеки от тези случаи процеса на анализ и синтез може да се разглежда, като процес на декомпозиране на наличните данни и изграждане на модел. Целта на този процес е да сортира и организира данните след това да ги синтезира в свързани и ясно представени доказателства. Така се създава хипотетичен модел на обекта (разузнавателната цел).

Моделът се използва за събиране на доказателства, оценява логическата аргументация и предоставя инструмент за обяснение на това как наличните доказателства най-добре съответстват на заключението на анализатора. Моделът служи и за да помогне на анализатора да разбере какви доказателства липсват, както и кои доказателства подкрепят модела и кои не. Разузнавателната цел може да бъде описана от няколко модела, всеки от, които с множество хипотези. В този процес е присъщо експлицитно моделиране на разузнавателните цели, както и множеството хипотези, описващи тяхното състояние и поведение. Съвместният процес на синтез и анализ в разузнаването изисква такова експлицитно моделиране. Спонтанните мисловни (тацитни) модели в съзнанието на отделните специалисти (анализатори) трябва да бъдат изрично изяснени, и задължително споделени за съвместен анализ. Когато спонтанните умствени модели са изложени само, като обосновка за окончателните разузнавателни преценки, те стават недостъпни при независим контрол върху разузнавателните продукти и увеличават вероятността за грешки и пропуски. Изричните представяния на моделите осигуряват инструмент за тяхното съвместно изграждане, поддръждане, декомпозиране и критичен преглед на доказателствата. Тацитното и експлицитно моделиране са допълващи се инструменти на анализато-

рите и задължително трябва да се приложи обективна преценка за балансирано използване и на двете.

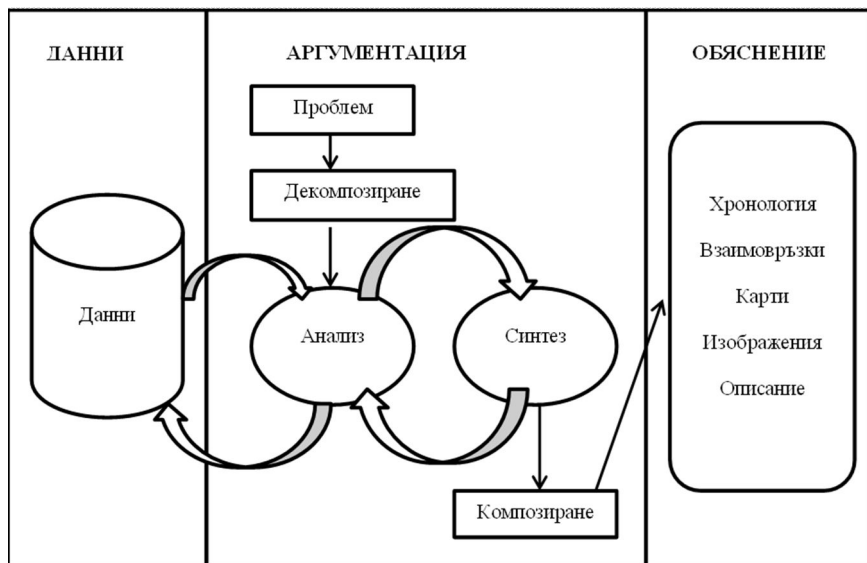
Моделирането осигурява по-дълбоко структуриран и по-широк съвместен анализ: Моделът е абстрактно изображение, който обслужва две функции:

- Моделът като хипотеза. Въз основа само на частични данни или предположения, моделът може да бъде представен с конкретни примери, като възможно предположение, което трябва да бъде оценено, като хипотеза;
- Моделът, като обяснение. Когато доказателствата се сглобяват в общата рамка на модела за да формират хипотеза, различния оглед на конкретния модел осигурява нови обяснения на тази хипотеза.

Процесът на прилагане на декомпозиране на данните (анализ) и конструктивен преглед на модела (синтез) може да бъде изобразен в три фази или работни процеси (фиг.2):

1. Събиране и съхраняване на данни. В тази фаза събраните данни се индексират и натрупват. Индексирането по време, източник, тема на съдържанието и други фактори се извършва за да се даде възможност за последващо търсене и достъп до различни доказателства;

2. Аргументация. Данните се преглеждат. Избраните елементи от потенциално значими данни (доказателства) се групират и сглобяват в осъществими категории обяснения, формиращи набор от хипотези, които обясняват наблюдаваните данни. Този процес прилага изчерпателно търсене в наличните данни, като приема някои от тях, а други отхвърля, като неподходящи. Целта на тази фаза е откриването на модели в данните. Тези модели водят до създаването на хипотези. Изследването на данните може да доведе до създаване на хипотези чрез предположения, въпреки че няма данни, подкрепящи хипотезата в този момент. Изследват се хипотезите, за да се определи какви данни ще се изискват за подкрепа или отхвърляне на всяка от тях. Хипотезите се класират по отношение на вероятността и необходимите данни за потвърждаване или опровергаване. Моделите са тестват и всяка хипотеза се преценява за пълнота, достатъчност и осъществимост. Това изследване може да доведе до заявка за допълнителни данни, усъвършенстване на настоящите хипотези или създаване на нови хипотези.



Фиг. 2

3. Обяснение. Различните тествания на модела предоставят обяснения, които артикулират хипотезата и свързват подкрепящите доказателства. Докладът на разузнаването може да включва един модел и обяснение, които най-добре съответстват на данните или алтернативни конкуриращи се модели, както и подкрепящите ги доказателства и оценка на последиците от тях.

Формата на модела е функция на поставения проблем. Най-често използваните модели в разузнаването са:

- Модел на организация. Описват се и се оценяват вертикалните и хоризонтални връзки в структурата на социалните организации;
- Финансов модел. Описват се и се оценяват финансови потоци, транзакции, бюджети, приходи и разходи;
- Модел на връзки между обекти и събития. Описват се и се оценяват връзките обект - обект, обект - събитие и събитие – събитие;
- Модел на физически обект. Описват се и се оценяват физически структури, способности, състояния и комуникации;
- Модел на съчетание на събития, хронология и последователност на оперативни процеси. Описват се и се оценяват причинно следствени връзки, динамика, повтораемост и продължителност на процеси и събития;
- Модел на движение на обект. Описват се и се оценява кинетичното поведение на физически обекти.

Моделът може да има много гледни точки или перспективи за обяснение. Хипотезата е единично обяснение на разузнавателния обект, позоваващо се на набор

от възгледи или модели. За една разузнавателна цел може да се създадат и разгледат няколко конкуриращи се хипотези, всяка от които с пълен набор от модели.

Моделите помагат на анализаторите да определят данните, необходими за разграничаване на хипотезите. Също така те се използват при представянето на разузнавателните продукти на потребителите. Основните потребители са, както взимащите решения с цел изготвяне на политики, така и право прилагашите и право раздавателните органи, при събрани данни за престъпление.

Моделиране на разузнавателните цели в средата за сигурност

Основният инструмент за създаване и поддържане на информационно превъзходство в сферата на сигурността е способността за осъществяване на ефективни информационни операции. Информационните операции са тези действия, които се предприемат за засягане на информацията и информационните системи на противника, като същевременно защитават собствените информация и информационни системи. В „Съвместната визия 2020“ на САЩ крайната цел на информационните операции е да улесни и защити процесите за взимане на решения в САЩ и в условията на конфликт да възпрепятства тези на противника.

Разузнавателните цели могат да бъдат обекти, събития и динамични процеси или комбинации от тях. Разработването на информационни операции поставя ударението върху разузнавателните цели, които съществуват не само във физическата реалност, но и в сферата на информацията (автоматизирани информационни системи и мрежи) и в сферата на човешките решения.

Съществуват две оперативни концепции за информационните операции. Първата е свързана с използване на информационните операции за наблюдение и ориентация в средата за сигурност. При втората освен наблюдение и ориентация в средата за сигурност се извършват и действия, които създават условия за информационно превъзходство над противника. В основата на тези концепции е, че информационните операции изискват координирани действия на разузнаването, насочени в три основни области на средата за сигурност. Разузнавателните цели трябва да бъдат моделирани и в трите основни области (домейни):

1. Физически домейн. Обхваща материалния свят от средата за сигурност. Основните целеви обекти в тази област са съоръжения, техника и персонал. В моделите се изобразяват обекти от физическия свят;

2. Информационен домейн. Абстрактната символична област от средата за сигурност съставена от думи, цифри и изображения, които представят физическия свят. Елементите се съхраняват и предават в електронен формат, чрез радио и телевизионни сигнали, интернет и вестници. Това е домейн, който се разширява с безпрецедентни темпове и в тази област се представят глобални идеи, съобщения и описания на света. Домейнът включва кибер пространството, което се е превърнало в основното средство, чрез което хората оформят своето възприятие за света;

3. Когнитивен домейн. Това е сферата на човешката мисъл, имаща отношение към средата за сигурност. Това е крайната цел на всички информационни потоци. Тази сфера се формира от индивидуалните и колективни мисли на правителствени лидери и населението като цяло. В тази когнитивна област се формират възприятия, концепции, мисловни модели и решения. Това е уязвима област, където несигурността, страховете, паниката и терорът могат да повлияят и променят поведението на обществото.

Ясното формулиране на принципите на разузнавателния анализ и синтез подпомага изучаването им, с цел повишаване на тяхната ефективност и надеждност и от друга страна повишава прозрачността в системата за защита на националната сигурност, като цяло.

Литература:

1. Davis, J., "The Kent-Kendall Debate of 1949," CIA Studies in Intelligence, Vol. 36, No. 5, 1992, p. 93.
2. U.S. DoD Joint Chiefs of Staff J-5, Joint Vision 2020, Washington, D.C.: Government Printing Office, May 24, 2000, p. 28.
3. Waltz, E., "Knowledge management in the intelligence enterprise" ARTECH HOUSE, INC., 2003;
4. Waltz, E., "Data Fusion in Offensive and Defensive Information Operations," Proc. of National Symposium of Sensor and Data Fusion, San Antonio, TX, June 2000, Vol. 1, pp. 219–232.

Ж. С. Йорданов

ПОДХОД ЗА ИЗСЛЕДВАНЕ НА ВЗАИМОДЕЙСТВИЕТО МЕЖДУ ВЪОРЪЖЕНИТЕ СИЛИ И ИНСТИТУЦИИТЕ, УЧАСТВАЩИ В СИСТЕМАТА ЗА ЗАЩИТА НА ВЪТРЕШНАТА СИГУРНОСТ НА СТРАНАТА

Живко С Йорданов

Военно формирование 32300 - ВАРНА
GSM: +359887881809 и +359895456954

EXAMINATION APPROACH OF INTERACTION BETWEEN THE ARMED FORCES AND INSTITUTIONS INVOLVED INTO THE COUNTRY'S INTERNAL SECURITY SYSTEM

Zhivko St Yordanov

Abstract: Security environment analysis present the increasing number of crimes, migratory pressure to the border as well as the worldwide terrorism increased threat for internal security. This environment required an objective assessment of interaction between the departments for protection to internal security, who will be at joint operation in a complicated operating environment.

Keywords: National security, Interior security, Counter terrorism, Defense, Interaction, Joint operations, Law Enforcement.

Поради факта, че **вътрешната сигурност** на страната обхваща всички аспекти на обществения живот, всички **министерства и ведомства** от държавната администрация имат отношение по нейната защитата. Водещите институции в това отношение са МВР, ДАНС, ДАР и Въоръжените сили. Тези институции обаче представляват отделни системи, които при нормални условия на обстановката функционират относително самостоятелно и едновременно са включени в системата за защита на националната сигурност. Анализът за средата на сигурност показва, че поради нарастващия брой престъпления, миграционния натиск по границата както и засилената заплаха от тероризъм в световен мащаб, заплахите за вътрешната сигурност стремително нарастват. Това може да доведе до криза, която да създаде необходимост от изключително бързи и решителни съвместни действия на различните институции при максимално напрежение на силите с цел отстраняване на заплахите и ликвидиране на последствията.

Тези обстоятелства налагат да се направи обективна оценка на взаимодействието между тях, за да се покаже текущото състояние на системата и да бъдат посочени насоки за нейното подобряване. За поставяне на обективна оценка взаимодействието между отделните елементи на системата е необходимо да бъде извършено емпирично социологическо изследване на взаимодействието между институциите.

Емпиричното социологическо изследване може да се определи като **основно средство за набиране на социологическа информация със съответните качества/актуалност, комплексност, представителност, достоверност и т.н.т./**, която

представлява надеждна основа за актуални теоретични обобщения и практически изводи, насочени както към усъвършенстване на теорията, така и към прогресивно изменение на социалната практика.[2] То представлява сложен, многостранен и продължителен изследователски процес със своя логика, методика и организация.[2] Този тип изследване може да се раздели на четири главни етапа:

- подготовка на изследването;
- провеждане на изследването;
- обработка на получените данни;
- анализ на социологическата информация;

Подготовката на изследването е най - голям по обем на извършваните дейности и най - продължителен етап, който включва в себе си следните три подетапа: програмиране на изследването, методика на изследването и проект за обработка на данните.

Програмата за провеждане на изследването е основен подетап на подготовката на изследването. В зависимост от качеството на провеждането на този подетап зависи цялостната подготовка на изследването, а от там и качественото провеждане на цялото изследване и събиране на достоверни емпирични данни.

Програмирането на изследването съдържа в себе си следните елементи:

1. Формулиране на темата, целите и задачите на изследването:

Без съмнение първата стъпка в изследването е формулирането на неговата тема. Темата на настоящото изследване произлиза от проблематиката на усъвършенстването на взаимодействието между въоръжените сили и другите държавни институции при защита на вътрешната сигурност. Следователно е необходима емпирична оценка на състоянието на взаимодействието между въоръжените сили и останалите институции, затова темата на изследването следва да бъде **"Оценка на взаимодействието между въоръжените сили и другите държавни органи участващи в защита на вътрешната сигурност"**.

От така формулираната тема на изследването следва, че целта на изследването е **да се събере представителна, точна и достоверна информация относно състоянието на системата за защита на вътрешната сигурност и механизмите за взаимодействие между нейните подсистеми и елементи.** Тази информация ще послужи за анализ на системата и набелязване на мерки за усъвършенстване на взаимодействието, между нейните елементи и неговото бъдещо подобряване. Постигането на тази цел може да се изпълни чрез решаване на следните основни **задачи**:

- на основата на емпиричната социологическа информация да се разкрие реалната картина на системата за защита на вътрешната сигурност на страната;
- да се изучат тенденциите в отношенията свързани с взаимодействието между въоръжените сили и държавните институции;
- да се определят най-съществени обективни и субективни фактори, способстващи за подобряване на взаимодействието между въоръжените сили и институциите;
- формулиране на практически изводи за състоянието на системата и набелязване на мерки за усъвършенстване на взаимодействието, и подобряване на системата за защита на вътрешната сигурност;

2. Определяне на обекта, предмета и обхвата на изследването

Обектът на изследването може да се определи като реална съществуваща същност в обективния свят, а предметът на изследването се определя като специфичен аспект, от който се изучава даден обект [2]. В конкретното изследване взаимодей-

твие то между институциите и между въоръжените сили е част от обществените отношения, които възникват при защита на вътрешната сигурност на страната.

Следователно като **обект** на настоящото емпирично изследване може да се определи **обществените отношения** свързани със защита на вътрешната сигурност на страната, а като негов **предмет** се определя **взаимодействието** между Въоръжените сили и другите държавни институции при защита на вътрешната сигурност на страната.

3. Разработване на теоретичен и социологически модел на процеса на изследване.

В конкретното изследване съставянето на теоретичен модел започва с дефинирането на елементите на системата за защита на вътрешната сигурност. След това е необходимо да се очертае правната рамка. Това са всички нормативни и административни актове, които регламентират дейността и правомощията на институциите, участващи в защитата на вътрешната сигурност.

След като се определят участващите институции и се очертае правната рамка следва да се провери работата на системата за защита на вътрешната сигурност като се проверят взаимовръзките между подсистемите, участващи в нея. Това може да се извърши, като се използва методът на сценариите.

Като цяло, методът на сценариите е надежден и подходящ, като позволява цялостно да се разгледа дейността на различните институции и взаимодействието между тях при разкриване и противодействие на заплахите за вътрешната сигурност при едни бъдещи възможни събития, в условията на изключителна неопределеност.[5]

За целта на изследването могат да се разработят различни сценарии, съобразени със заплахите за вътрешната сигурност в страната, които евентуално могат да възникнат в резултата на съзнателна човешка дейност или форсмажорни обстоятелства. Като пример за това могат да бъдат посочени следните четири оперативни сценария:

А. Терористична атака срещу обект от критичната инфраструктура от терористични групи на територията на България. - при този сценарий група терористи планират атака срещу някои от особено важните обекти в страната като между тях са пристанищата в Бургас и Варна, нефтено пристанище Росенец, летищата София, Пловдив, Бургас и Варна, Лукойл – Нефтохим – Бургас, Соди – Девня и други обекти, чието поразяване може да доведе до изключително големи щети за територията на страната, морските пространства и трудно ликвидиране на последствията. Задачата на институциите е да разкрият предварително намеренията на групата и нейните действия да бъдат пресечени още в самото начало или на по-късен етап да бъде проведена съвместна контртерористична операция.

Б. Трафик на оръжие, наркотици и стоки с двойна употреба от транснационална престъпна групировка - транснационална организирана престъпна група, изключително добре организирана, търгува с оръжия и стоки с двойна употреба. Задачата на институциите е да разкрият групировката и да извършват операция по пресичане на каналите на групировката.

В. Бежанска вълна на държавната граница - в следствие на задълбочаващата се кризисна обстановка в близкия изток хиляди цивилни граждани на различни страни от близкия изток се опитват да достигнат до Европа. Задачата на институциите е да предотвратят нахлуването на бежанци на територията на България и да облекчат натиска върху държавната граница.

Г. Групово нарушаване на обществения ред - малцинствена група е недоволна от решението на кмета на населен пункт за събаряне на незаконни постройки, което довежда до групово нарушаване на обществения ред като към безредиците се присъединяват и хора от околните на града населени пунктове. Задачата на институциите е чрез съвместна операция да ограничат последиците и да пресекат груповото нарушаване на обществения ред.

4. Формулиране на основните хипотези;

След като се създаде теоретичен модел за функциониране на системата за защита на вътрешната сигурност, се формулират основните хипотези на изследването.

Следвайки основните изисквания към хипотезите: да съдържат понятия, които могат да бъдат измерени; да бъдат прости и ясни; да могат да бъдат проверени, могат да бъдат формулирани две основни хипотези:

- **Хипотеза 1** - Теоретичната постановка и досегашната практика от изпълнението на съвместни действия между Въоръжените сили и институциите по защита на вътрешната сигурност показва, че съществуват добре урегулирани обществени отношения, с точни правила за взаимодействие, здрави взаимовръзки и ясни правомощия на различните органи и въоръжени сили.

- **Хипотеза 2** - Теоретичната постановка и досегашната практика от изпълнението на съвместни действия между Въоръжените сили и институциите по защита на вътрешната сигурност показва, че не съществуват добре урегулирани обществени отношения, поради което няма точни правила за взаимодействие и ясни правомощия на различните органи и въоръжени сили.

И двете хипотези са проверяеми и допускат алтернативност на ситуацията. Това ще рече, че в хода на изследването, в зависимост от получените емпирични резултати могат да се появят вторични хипотези, които да бъдат производни от основните две.

5. Скалиране. Разработване на специфични скалограми:

Под измерване най-общо се разбира намиране на числово значение за измерваната величина, т.е. такава процедура, при която измерваният обект се сравнява с някакъв еталон и получава числено значение.[2]

Най-удачният вариант за измерване на явленията свързани с взаимодействието и придаването им на цифрова стойност е тяхното измерване, чрез цифрови скали. **Скалата** е система от числа за подреждане на количествени признаци (метрично скалиране, т.е. измерване), или система от знаци, характеризиращи определени социални свойства, за подреждане и оценка на качествени признаци и техните разновидности (неметрическо скалиране, т.е. квалификация и квантификация).[2]

В настоящото изследване ще се използва неметрическото скалиране като най-широко ще бъдат използвани тристепенната интервална скала от типа:

вярно *невярно* *не мога да преценя*
1 2 3

и петстепенната номинална скала:

изобщо не много рядко понякога често много често
1 2 3 4 5

6. Изготвяне на инструментариума на изследването:

В инструментариума се включват всички документи, с помощта на които се набират необходимите данни. В него намират място въпросите, които интересуват изследователя, и които логически и по необходимост произлизат от теоретичния модел и определените емпирични индикатори. Практически, всеки емпиричен индикатор се представя в съответния документ с няколко въпроса. [2]

От формулираните хипотези могат да бъдат изведени следните емпирични индикатори:

- познаване на нормативната база за функциониране на системата за защита на вътрешната сигурност на страната;
- познаване на участващите структури в системата за защита на вътрешната сигурност на страната;
- познаване на правомощията, функциите и задачите, както собствените така и на останалите участници в системата за защита на вътрешната сигурност;
- наличие на единни планове за съвместни действия на институциите, при противодействие на кризи и заплахи за вътрешната сигурност на страната;
- подходяща организационна структура на различните подсистеми;
- съществува ли постоянен обмен на информация между взаимодействащите структури;
- наличие на единно командване и управление;
- съществуване на единни тактики, техники и процедури, които да бъдат ясни за всички участници в конкретната съвместна операция;
- провеждане на предварителни поетапни съвместни учения за проиграване на тактиките, техниките и процедурите при разрешаване на криза по защита на вътрешната сигурност;

Чрез емпиричните индикатори следва да се провери дали са изпълнени основните изисквания на взаимодействието и дали са спазени неговите принципи. Проверката на индикаторите ще се извърши чрез следните инструменти:

А. Въпросник

Въпросникът е основен инструмент в инструментариума или основен документ в документацията на емпиричното изследване.[2] Въпросникът е съставен съобразно темата и характера на изследването. Въпросникът следва да съдържа въпроси, които имат за цел да изведат цифрово значение на определените по-горе емпирични индикатори, чрез които да се оцени взаимодействието между институциите при защита на вътрешната сигурност.

Количественото определяне на първите три индикатора ще даде възможност да се провери дали са изпълнение две от основните изисквания на взаимодействието - нормативна определеност на взаимодействието и определяне на правата и задълженията на системите.

Цифровото измерение на първия индикатор **познаване на нормативната база за функциониране на системата за защита на вътрешната сигурност на страната** се определя от първите въпроси във въпросника. Чрез тях се проверява до каква степен се познават законите, правилниците, наредбите и инструкциите на различните ведомства, които определят техните функции и задачи. По този начин следва да се провери дали анкетираните познават законовата база, която регламентира техните действия.

Вторият индикатор **познаване на участващите структури в системата за защита на вътрешната сигурност на страната** се измерва чрез проверка дали анкетираните познават структурите участници в системата за защита на националната сигурност, структурите в които работят (служат), както и структурите, с които би следвало да си сътрудничат в съвместна операция.

Индикаторът **познаване на правомощията, функциите и задачите**, се измерва с въпроси, чрез които се проверява дали анкетираните познават своите правомощия и правомощията на своите колеги от другите структури.

Спазването на останалите изисквания на взаимодействието: трайност и непрекъснатост; организационна широта и пълнота на взаимодействието и комплексност на взаимодействието се проверява, чрез измерване на следващите емпирични индикатори:

Индикатор, **наличие на единни планове за съвместни действия на институциите**, се определя като се проверява съществуват ли конкретни планове за взаимодействие и дали анкетираните познават вече съществуващи планове на централно и местно ниво.

Постоянен обмен на информация и наличие на единна комуникационно-информационна система е индикатор, чрез който се дава отговор на въпроса дали съществува устойчив обмен на информация между институциите и по какъв начин се осъществява той. Последните въпроси дават цифров вид на индикаторите: **наличие на единно командване и управление; съществуване на единни тактики, техники и процедури; провеждане на предварителни поетапни учения за проиграване на съвместните действия.**

Б. Анкетна карта

Анкетната карта съдържа въпроси, които имат за цел събиране на обща информация за индивида, така че да бъдат събрани следните данни за него: възраст; години служба; длъжността, която заема към момента; професионален опит; участие в съвместни операции с въоръжените сили или други институции; отношение към работата като цяло;

Целта на събирането на данни е да се определят различни фокус групи, с определен коефициент K_t . Това има за цел максимално да минимизира субективното възприятие на индивида относно изследваните дейности.

Например, служител с повече от 20 години стаж, изпълнявал една и съща дейност и не участвал в съвместни операции, ще има едно виждане по въпроса, докато съвсем по друг начин тези дейности ще бъдат възприети от човек, който е със същия или близък до неговия стаж, но заемал повече от една длъжност и участвал в съвместни операции с други органи и институции.

В. Беседа

Този инструмент в изследването има за цел контрол на достоверността на получените данни. Тя ще се провежда групово, в началото преди попълване на въпросника, така че анкетираните да бъдат запознати с правилата за попълване на въпросника както и да бъдат получени отговори на следните въпроси:

- Какво е субективното отношение на групата към другите институции от системата за национална сигурност?
- Участвали ли са в съвместни операции с други органи и ведомства?
- Какви проблеми са срещнали по време на изпълнение на съвместни дейности?
- Какви са техните съвети и препоръки?

Събраните по време на изследването данни следва да се обработят и за да се получи крайният резултат.

На първо място се обработват резултатите от анкетната карта.

Резултатите от анкетната карта следва да се определят от отговорите, които са дадени от служителите (военнослужещите) като всеки един отговор ще допринася за определяне на индивида към конкретна фокус група.

Например първа фокус група ще включва служители (военнослужещи) в началото на службата, както и такива, които имат по-голям стаж, но са заемали само една длъжност през целия период и не са участвали в съвместни операции с други институции и не са участвали в мисии и операции зад граница. Тази фокус група ще получи коефициент $K_t = 0,5$. Втора фокус група може да бъде изградена от служители (военнослужещи), които са служили между 5 и 20 години и са заемали повече от една длъжност или са участвали в съвместни дейности с колеги от други институции или в мисии и операции зад граница. Тази група ще получи коефициент $K_t = 0,7$. Трета група ще бъде изградена от военнослужещи (служители), които имат над 5 години служба, заемали са различни длъжности и едновременно с това са участвали в съвместни операции и дейности с други институции от системата за национална сигурност и са участвали в мисии и операции извън територията на страната. Техният коефициент ще бъде $K_t = 0,9$.

Разбира се според показателите в анкетата могат да бъдат определени n на брой фокус групи, но не повече от 7 като всяка от тях следва да влиза с отделен коефициент K_t .

След това се обработват резултатите от въпросника, като за всяка фокус група се попълва таблица, която има следния вид:

	q_1	q_2	q_3	q_4	q_5
Q_1	25%	16%	-	52%	7%
.....					
Q_n	$x\%$	$y\%$	$z\%$	$m\%$	$n\%$

Цифровите стойности за всеки въпрос се умножават по коефициента K_t или:

$$(1) Q_t = q_n \times K_t$$

Така най-големият получен резултат за Q_t се приема за отговор на въпроса на пример: за първата група въпрос 1: $Q_{t1} = 12,5\%$, $Q_{t2} = 8\%$, $Q_{t4} = 26\%$, $Q_{t5} = 3,5\%$. Вижда се, че най-висока стойност има $Q_{t4} = 26\%$, което ще рече че отговора на 1-ви въпрос е 4 - често.

Това се прави за всяка фокус група, след което получените резултати се сравняват, а при различни резултати и в трите групи се събират:

$$(2) q_1 = Q_{t1.1} + Q_{t1.2} + Q_{t1.3}$$

След това се сравняват резултатите: q_1 ; q_2 ; q_3 ; q_4 ; q_5 и най-високият по стойност се приема за отговор на въпроса, т.е. $q_3 > q_1$; q_2 ; q_4 ; $q_5 \Rightarrow Q_1 = q_3$. Тези получени данни се сравняват с резултатите и препоръките от проведените беседи, анализират се и се правят съответните изводи и заключения.

В заключение може да се каже, че този подход на изследване може да се развие в по-голяма система за изследване на взаимодействието между въоръжените сили и другите държавни органи за защита на вътрешната сигурност на страната. Проведеното по този начин изследване на взаимодействието, между въоръжените сили и останалите институции, участващи в операция по защита на вътрешната сигурност, ще осигури достоверна емпирична информация за състоянието на системата за защита на вътрешната сигурност като минимизира субективната оценка на анкетираните военнослужещи и служители от различните ведомства, което ще допринесе за по-качествено изследване на проблема.

Литература:

1. Гоцев, Г. Защита на сигурността и обществения ред, София, ВИ, 2016.
2. Делибеев И, Теория и методи на емпиричното социологическо изследване, София 1987.
3. Закон за управление и функциониране на системата за защита на националната сигурност обн. дв. бр.61 от 11 август 2015.
4. Иванов, В. Охраната на държавните граници и новият световен ред: [Изследване], София: Военно издателство, 2005г., ISBN954-509-324-2.
5. Методология и сценарии за отбранително планиране, София, ВИ.
6. Програма за развитие на отбранителните способности на въоръжените сили на Република България 2020.
7. План за развитие на въоръжените сили до 2020.
8. Радилов Д и колектив, Въведение в статистиката, Варна 1995.
9. Стоянов, Г. Рискове и заплахи за вътрешната сигурност на Република България, София 2000.
10. Фердов, С. Контрол на тълпата. Стратегия и тактика, София, Военно издателство, 2006.

А. Л. Атанасов

АНАЛИЗ НА ПОНЯТИЕТО „ВИСОКОТОЧНО ОРЪЖИЕ”

Атанас Л. Атанасов

*Национален военен университет „Васил Левски”, Факултет “Артилерия,
противовъздушна отбрана и комуникационни и информационни системи”,
телефон: 054 801040, вътрешен 54232, e-mail: lenkov@gbg.bg*

ANALYSIS OF THE CONCEPT “HIGH-PRECISION WEAPONS”

Atanas L. Atanasov

Abstract: *It is shown that different definitions of the concept of “high-precision weapons” (HPW) published in various publications put forward excessive demands on the HPW. The key indicators of the HPW are substantiated. A version for defining of the HPW is proposed.*

Keywords: *High-precision weapons, ordnance, kill zone, zone of targetability, warhead, accuracy of fire, circular probable error, probability of defeat.*

В последно време авторите на много публикации в различни издания разглеждат въпроси относно използването или перспективата за развитие на средствата за поразяване отнасящи се към високоточните оръжия (ВТО). За съжаление в повечето от тези статии не е изведено понятие характеризиращо високоточните оръжия, какви характеристики притежават или трябва да притежават средствата за поразяване и по какви признаци могат да бъдат причислени към ВТО.

В някои публикации авторите предлагат свой подход към разглеждането на ВТО, но те не са единни, което не дава възможност да се улови същността на разисквания въпрос и да се определят основните изисквания, на които трябва да отговарят оръжията от този клас. Отсъствието на примери, от които да се види какви конкретно са средствата за поразяване и по какви цели могат да се използват те, за да могат да се отнесат към ВТО, усложнява възприемането на разглежданите въпроси.

Това създава грешна представа в читателите за понятието „ВТО” и много от тях приемат, че всички управляеми средства за поразяване са ВТО. Вероятно съвременните и най-вече бъдещите въоръжени конфликти и войни ще бъдат водени предимно с оръжия от такъв клас.

Историята, свързана с появата на понятието „високоточно оръжие”, датира от 60-те години на миналия век, когато става ясно, че при стрелба с балистични ракети (БР) с обикновена бойна част (БЧ) грешката в насочването е от 0,3% до 1% в зависимост от разстоянието до целта.

Точността на стрелбата с БР зависи от много фактори, един от които е топогеодезическата подготовка (отчитат се физико-географските, климатичните и атмосферни условия, скорост и посока на вятъра).

Изчисленията са били извършвани с помощта на механически арифмометър³⁹ тип „Феликс“, чрез използване на аналитични зависимости и таблици за стрелба предварително подготвени за пуск на БР на необходимото разстояние. Всички тези данни са се въвеждали в системата за управление на ракетата с достатъчно големи грешки.

Първата крачка към повишаване на точността на стрелбата с БР е използването на електронни изчислителни машини (ЕИМ), което позволило в пъти да се повиши точността на стрелбата, но това не решило изцяло проблема на този етап.

Втората крачка за повишаването на точността на стрелбата е свързана с въвеждането на крайни координати на полета на БР, което позволило в десетки пъти да се намали вероятността за пропуск на целта. При тегло на обикновена БЧ от порядъка на 500-1000 kg и с тази точност на насочването, БР не отговаряла на изискванията за ефективно поразяване на обектите.

Третата крачка към повишаването на точността била създаването на маневрени бойни части, които се използвали в системите за спътниково навигиране и автоматичен прицел. С тяхна помощ отклонението било сведено до разстояние от порядъка на единици метри. Тогава в средите на ракетчиците се появява термина „високоточно оръжие“, което е било напълно основателно и закономерно, защото действително точността на стрелбата се увеличила стотици пъти. Тук трябва да се отбележи, че този термин започва да се използва в САЩ в средата на 70-те години на миналия век. Прилагането му за авиационните средства за поразяване е явен опит да бъде даден физически смисъл на понятието ВТО, което по правило се свежда до ефективността на управляемите средства за поразяване (УСП). Следва да се отбележи, че няма никакво съществено подобрене в характеристиките и точността на УСП за последните 20-30 години. Максимума на вероятното кръгово отклонение от $E_{\text{вко}} = 6-10 \text{ m}$ до $E_{\text{вко}} = 2-4 \text{ m}$ подобрява точността на използване на УСП клас „въздух-земя“ (чрез усъвършенстване на главата за самонасочване на ракетата). Независимо от това, термина ВТО, под който мнозина разбират вероятност за поразяване на целта от УСП 0,5; 0,7; 0,9 до сега широко се използва.

За по-задълбочено изследване същността на въпроса е целесъобразно да се разгледат основополагащи, общоприети определения имащи непосредствено отношение към него.

Зона за поразяване – района около центъра на взрива на заряда, в рамките на който се осигурява зададената степен на поразяване на целта.

Уязвимост на обекта (целта) – степента за възможно поразяване на обекта при въздействие с различни средства за поразяване в зависимост от неговото разположение, размери, функционална схема, здравина, степен на защита, налични средства за противодействие и т.н [4].

Точност на стрелбата – оценката на положението на точките на попадението (разривите) на снаряда (ракетата, куршума) спрямо целта (точката на прицелване), оценявана по вероятното кръгово отклонение ($E_{\text{вко}}$).

Оръжие – устройства и средства предназначени за поразяване на противника във въоръжени сблъсъци. Обичайно се състоят от средства за поразяване и средства за доставянето им до целта, по-сложните оръжия включват също прибори и устройства за управление и насочване [4].

³⁹ Арифмометър – машина за смятане.

Средства за поразяване (СП) – съставна част на оръжието (снаряд, бомба, мина, бойна част на ракети и др.) предназначена за непосредствено въздействие върху обекта (целта).

В речника на оперативно-стратегическите термини (с. 124) е дадено следното определение за понятието ВТО: „*Средство за поразяване с управляема траектория (ракета, бомба, торпедо, боен елемент, снаряд, мина и др.) с неадресно снаряжение, независимо от разстоянието на стрелбата, осигуряващо с вероятност близка до единица, съгласуване на зоната за поразяване на бойните части и зоната на уязвимост на обектите за поразяване функционално обединени в единен процес със системите за информационно осигуряване (в това число разузнаване и целеуказване, бойно управление и свързка)*”.

В изведеното определение може да се отбележат както положителни аспекти, така и някои недостатъци. Към първите може да се отбележи това, че авторите са обвързали точността на стрелбата с ефективността на използване на СП чрез определено съгласуване между зоната за поразяване на бойните части и уязвимостта на обектите за поразяване.

Ако се придържаме към даденото определение следва, че при въздействие по едни цели средството за поразяване ще се отнася към ВТО, а по други цели – няма да се отнася към тях. В случая всичко зависи от това в какво съотношение са зоната за поразяване на бойните части и зоната за уязвимост на разглеждания обект. Следователно, трябва да се уточнява във всеки конкретен случай при въздействие върху какви обекти даденото средство за поразяване може да се счита за ВТО. Към недостатъците на това определение може да се добави, че съгласуването се осигурява с вероятност близка до единица, което с отчитане на отклонението на БЧ от точката на прицелване практически ще е невъзможно да се достигне.

Зоната за възможно поразяване (ЗВП), както и уязвимите зони на целите (УЗЦ), основно зависят от характеристиките на използваните срещу обекта средства за поразяване, степента на устойчивост на обектите срещу действието на тези средства за поразяване и взаимното разположение на обекта и СП.

По този начин горепосоченото твърдение за високоточните оръжия може да бъде използвано в дадения случай само за определен вид средства за поразяване при въздействие по конкретни обекти. Ако УЗЦ превишава съществено ЗВП, то тогава няма значение дали зоната на попадение е в зоната на уязвимост на обекта, той ще се счита за поразен или непоразен с недостатъчна ефективност и за неговото унищожаване ще трябва да се използват повече боеприпаси – тоест такова СП не може да бъде отнесено към класа на високоточните оръжия.

Освен това могат да се направят следните забележки по повод определението за ВТО:

Първо. Какво се разбира под „съгласуване на зоната за поразяване на БЧ и зоната на уязвимост на обекта за поразяване с вероятност близка до единица”? В този случай става дума за покриване на зоната на уязвимост на обекта със зоната на поразяване на СП с гарантирана вероятност от 0,9, както е прието в теорията за ефективността.

Второ. Зоната на възможното поразяване и зоната на уязвимост на целта са взаимно свързани една с друга: ЗВП зависи както от мощността на бойната част на СП, така и от уязвимостта на обекта на действие; УЗЦ на свой ред, зависи от защи-

теността на обекта и мощността на БЧ на средствата за поразяване, действащи върху него.

Трето. Зона за възможно поразяване на БЧ – характеристика на средствата за поразяване описващи мощността на БЧ при въздействие по конкретна цел. Уязвима зона – характеристика на обекта за поразяване при въздействие на конкретно СП.

Четвърто. Какво отношение към ВТО има „информационното осигуряване: разузнаване и целеуказване, бойно управление и свързка“, като средство за поразяване, което в голяма степен се отнася към системата на ВТО - носителя на оръжието и средствата за осигуряване?

Пето. Какво означава „висока точност“, с какво се измерва и може ли изобщо да бъде измерена?

Шесто. Защо към ВТО се отнасят само управляемите средства за поразяване? А неуправляемите, като например оръжията с нови физически свойства (лазерни, радиовълнови)?

Малко по-различно смислово значение влагат авторите в понятието ВТО по отношение на по-рано изведеното определение [5]: „Високоточно оръжие с голям обхват – средство за поразяване с управляема траектория и конвенционално снаряжение, осигуряващо при първия пуск избиращост и висока вероятност за поразяване на целта от определен тип чрез пряко попадане в нейните уязвими елементи или попадане на бойните части в зоната за поразяване“.

В това определение за основа на ВТО се приема не покритието на зоната за поразяване и уязвимата зона на целта, а „поразяване на целта с вероятност близка до единица“. Фактически става дума за високо ефективно оръжие, което се явява важно при решаването на практически задачи.

Съществуват някои неопределености в това определение. Приетата „близка до единица вероятност за поразяване на целта“ и това, че такава „висока ефективност се постига чрез пряко попадане на СП в уязвимия елемент на целта или взривяване на бойната част в зоната за поразяване“.

Не става ясно също как се осъществява „избирателно попадение в цел от определен тип“ по траекторията на полета на средството за поразяване. Освен това от теорията за ефективността е известно, че толкова високи (близки до единица) показатели за ефективност с един пуск на СП е невъзможно да се постигнат, както е и малко вероятно прякото попадение на СП в целта, като се имат предвид точностните характеристики на системите за насочване и индивидуалните характеристики за техническото разсейване на средствата за поразяване.

Към положителните страни на даденото определение можем да отнесем това, че авторите са свързали конкретните средства за поразяване с конкретни цели –, цели от определен тип“.

Нека да разгледаме някои други определения на понятието ВТО [6].

Първо. Високоточно оръжие – това е такъв вид управляемо и самонасочващо се конвенционално оръжие, вероятността за поразяване на което с първия пуск по малоразмерни стационарни и подвижни цели, намиращи се дори на предела по разстояние на носителя на оръжието е близка до единица във всякакви условия на обстановката и при активно противодействие на противника.

Второ. Високоточно оръжие – средство за поразяване с управляема траектория (ракета, бомба, торпедо, боен елемент, снаряд, мина и др.) с неядрено оборудване,

функционално обединено със системите за информационно осигуряване, бойно управление и свързка, избиращо и ефективно (с вероятност не по-малка от 0,9 с първия пуск), унищожавашо, подавящо или дезорганизиращо силите на противника във целия диапазон на разстоянията на стрелба и разчетните условия за неговата бойна употреба.

Трето. Високоточно оръжие (високоточно средство за поразяване) – огнево средство за поразяване с управляема траектория с конвенционално (неядрено) снаряжение, функционално съпроводено със средства за информационно осигуряване, планиране и използване, бойно управление и свързка, осигуряващи при първия пуск избиращо и с висока вероятност (близка до единица) поразяване на целта от даден тип чрез пряко попадение в нейните уязвими елементи или взривяване на БЧ в зоната за поразяване във всичките диапазони и условия за бойно използване.

Следва да се разгледа третото определение, тъй като за първите две се намират много съвпадения с вече разгледаното определение.

Първата част на това определение, където се говори за „функционално съпроводено със средствата за информационно осигуряване, планиране и използване, бойно управление и свързка“, както вече беше отбелязано, в голяма степен се отнася към системата на ВТО, средната част – „при първия пуск избиращо и с висока вероятност (близка до единица) поразяване на целта от даден тип“ – към високата ефективност на оръжието, а не към неговата висока точност, третата част – „чрез пряко попадение в нейните уязвими елементи или взривяване на БЧ в зоната за поразяване“ се отнася непосредствено към ВТО. Всичко това води до известна неопределеност и нееднозначност на даденото определение.

В този доклад е направен опит да се формира обобщен вариант на определение за оръжията от дадения вид, където се опитам да отразя всички положителни аспекти съществуващи в специализираната литература относно понятието ВТО, което предоставям на вашето внимание: „ВТО – това е вид конвенционално (неядрено) оръжие, осигуряващо гарантирано поразяване на малоразмерни и добре защитени цели на всякакво разстояние в пределите на неговата досегаемост с пряко попадение при малък разход на средствата за поразяване в реални условия на бойно използване,,

Това определение също има редица очевидни недостатъци, а именно:

Първо. ВТО трябва да осигури гарантирано унищожение, а не просто поразяване на обекта (целта).

Второ. Защо ВТО трябва да поразява само „малки по размери и силно защитени цели,, а не се използва и срещу цели от типа на пускови установки, РЛС, пунктове за управление, комуникации, складове за боеприпаси, гориво и други второстепенни, но важни обекти?

Трето. Защо гарантирано поразяване на целите се осигурява с „пряко попадение и неголям разход на СП,, а не от първия пуск (изстрел) ?

Четвърто. Не е ясно какво се разбира под „пряко попадение и неголям разход на СП в реални условия на бойно използване,,. Пряко попадение в коя област на целта? И какво означава „неголям разход на СП,,?

Пето. Какво са имали предвид авторите като са написали „поразяване на целите на всякакво разстояние в пределите на неговата досегаемост,,. Всякакво разстояние включва и пределното разстояние до обекта.

Привеждането на повече забележки позволява да се направи извода, че в определението за ВТО трябва да присъстват най-малко три частни показателя, характеризиращи ефективността на всякакви средства за поразяване: точност, сила и приложимост, а също и показател характеризиращ уязвимостта на обекта. При тези показатели мощта се явява зоната за поразяване на обекта (целта), показателя точност - вероятното кръгово отклонение на СП (БЧ) спрямо точката на прицелване, показателя приложимост - разстоянието и условията на използване на СП, показателя уязвимост на обекта – приведената площ на поразяване при въздействие на СП върху целта.

Според тези определения към класа на високоточните средства за поражение, използвани в авиацията, могат да се отнесат СП, имащи вероятно кръгово отклонение (Евко) от точката на прицелване по-малко от 1 m.

Към тези средства могат да се отнесат противотанковите управляеми ракети (ПТУР), поставени на бойните вертолети и штурмови самолети и широко използвани в сухопътните войски. Те осигуряват пряко попадение в малоразмерни наземни цели от типа танк, БМП, БТР с вероятност 0,8. Това още не доказва тяхната висока ефективност, тъй като отчитайки бронепробиваемостта на целите с кумулативни бойни части с динамична защита и малкия среден брой попадения, за тяхното унищожаване са необходими две-три ракети.

Крилите ракети с въздушно базиране, както и повечето управляеми ракети от клас „въздух – земя“, като Х-25, Х-29, Х-31, Х-58, Х-59 с различни глави за самонасочване (ГСН) в повечето случаи не осигуряват необходимата точност на насочване (Евко ≤ 1 m), а също и припокриване на зоната за поразяване с една ракета и уязвимата зона на повечето наземни обекти с вероятност близка до единица, вследствие на което, те не могат да се причислят към класа на ВТО.

Единични малоразмерни слабо уязвими цели от типа на пускова установка, автомобил, РЛС, самолет или вертолет на открита позиция при точност на попадението на средствата за поразяване в целта не повече от Евко = 2-3 m могат да бъдат унищожени, но вече с оръжие от друг клас. В този смисъл, термина „високоточно оръжие“ може да бъде използван за голяма група средства за поразяване при въздействие по единична малоразмерна цел.

Заедно с това икономическата целесъобразност за използване на точно (и още повече на високоточно) оръжие по определена цел, намираща се в състава на групов (площна) цел, е доста ограничена и зависи от оперативната необходимост и значимост на обекта. За решаване на тази задача на въоръжение във ВВС има средства за поразяване на площни цели – авиобомби, контейнери и неуправляеми авиационни ракети с различно предназначение.

В този смисъл, от проведенния анализ се вижда, че термина ВТО съответства на доста ограничен кръг средства за поразяване, които без връзката между обектите и условията на бойните действия въобще нямат приложение. От всичко това следва, че използването на този термин трябва да е доста коректно, тъй като в действителност високоточното оръжие е доста малко (не повече от 3-5%) от оръжието във видовете ВС и родовете войски, а и количеството на обектите (целите), по които е икономически целесъобразно да се използват тези средства за поразяване, също е ограничено.

При въздействие по определени цели (обекти), ВТО е необходимо да осигурява максималната степен на поразяване – тяхното унищожаване. При степените на

поразяване – подавяне, дезорганизация (изваждане от строя) – след известно време целите могат да бъдат възстановени, в резултат на което се губи смисъла на връзката „високоточното средство – високоефективно средство”.

Ако ВТО се разработват за унищожение на определен тип обекти (цели), то мощността на бойните части ще се определя от условието зоната за поразяване на целта при взривяване на БЧ да припокрива с гарантирана вероятност $P \geq 0,9$ уязвимата зона на целта, разсъгласуването между БЧ и точката на прицелване трябва да бъде компенсирано за сметка на увеличаване на масата на БЧ.

При пуск на СП от носител с малка височина на полет (200 – 300 m) и полет на СП на пределно малка височина със следване релефа на местността, което е характерно за крилатите ракети, разсейването на СП по разстояние може да е от порядъка на няколко метра. Ако пуска (стрелбата) на СП се извършва по цел, имаща известно превишаване по височина (многоетажни здания, станции за съпровождане, РЛС разположени на височини, пещери в гори и др.), то при външно целеуказване (с подсветка на целта) е достатъчно висока вероятността за попадение на СП именно в уязвимата зона на целта.

Необходимо е да се отбележи още едно важно обстоятелство. Битува мнение, че наличието на ВТО позволява съществено да се снижи необходимостта от точно определяне на координатите на целите, което е вярно само за боеприпаси, снабдени с ГСН, позволяващи да се компенсират достатъчно добре големите първоначални грешки при извършването на пуск.

Управляеми средства за поразяване, способни ефективно да поразяват голямото разнообразие от наземни цели, различаващи се по размери, живучест, подвижност, структура на функциониране и други параметри, не съществуват. Като правило, такова средство се разработва за въздействие по конкретна група от цели, имащи еднакво целево предназначение или съпоставимост по живучест.

Да се причисляват към класа на ВТО авиационните еднократни касетъчни бомби, снаряжени със самоприцелващи се противотанкови бойни елементи, не е съвсем коректно, тъй като за гарантирано унищожаване на един танк е необходимо в него да попаднат 3 - 4 елемента (в касетата те са 15). В определени условия (при въздействие по танков взвод в район за съсредоточаване) с една такава касетъчна бомба може да се поразят 4 – 5 танка. Възниква въпросът, кое е средството за поразяване – касетата или нейният елемент? Ако е елемента, то той не е ВТО, ако е цялата касета, то тя е ВТО, но с известни условности, тъй като в повечето случаи това СП не отговаря на основните изисквания, предявени към оръжието от този клас.

Авиационните баражиращи суббоеприпаси – боеприпаси от принципно нов тип, са способни да поразят сложни и критически важни наземни обекти (цели) по всяко време на денонощието и годината и при всякакви природни условия без влизане в зоната за ПВО на противника. Тези средства за поразяване могат да извършват продължителен полет в зона за дежурство във въздуха, да изберат цел и да я следят до получаване на команда за нейното унищожаване. Достойнствата на тези боеприпаси като бързата им реакция, малката им забележимост и постоянното присъствие в зоната за бойни действия, позволяват при изпълняване на изискванията предявени към ВТО, те да се определят като особен вид оръжие от този клас.

Възгледите на командванията на армиите на САЩ и НАТО са, че високоточното оръжие се явява основно средство за достигане на огнево превъзходство над

противника в съвременните войни и конфликти. Това се потвърждава от резултатите от военните действия в Персийския залив през 1991 и 2003 г., а също и от конфликтите в Афганистан и Ирак. Развитието и усъвършенстването на системите и комплексите управляемо и самонасочващо се оръжие доведоха до качествени изменения в характера на въоръжената борба и до появата на нови форми и способности за водене на бойните действия.

Успоредно с това трябва да се отбележи, че ВТО не могат напълно да заменят обичайните средства за поразяване. Последните, както преди, така и сега, широко се използват за поразяване на различни обекти, а в това време ВТО се използват за поразяване на критически важни обекти в направлението на главния удар.

Опита от бойните действия в Югославия, Афганистан, Ирак и в Северен Кавказ показва, че ВТО, разработващи се първоначално за водене на борба с тежката бронетанкова техника се оказва ефективна и срещу отделни единични цели. Именно те съставляват основната част от обектите за поразяване. Освен това, бойния опит показва, че оръжията, които притежават висока точност, имат малък радиус на поражение, което осигурява минимални загуби при решаването на огневи задачи и позволява да се избегнат жертви сред населението, които не са въввлечени в конфликта и се изключва причиняването на значителни разрушения на обекти от инфраструктурата и от гражданските съоръжения.

Успоредно с това не считам, че ВТО идеално се вписват в сценариите на контртерористичните операции, характера на военните действия в тези операции изисква разработването на нови такива видове оръжие, предназначени основно за унищожаване на съоръжения от типа на укрепени позиции на огневите средства, командни пунктове, убежища и др. [2]

Мнението ми е, че понятието ВТО не трябва да търпи неконкретни изрази от типа: „с висока вероятност”, „с вероятност близка, до единица”, „степен на поразяване на целта - унищожение”, „подавяне или дезорганизиране”, „при неголям разход на средствата за поразяване”. Понятието ВТО трябва да съдържа еднозначно възприемащи се данни и показатели.

На основата на всичко изложено до тук, предлагам следното определение на това понятие:

Високоточно оръжие - средство за поразяване с управляема траектория с конвенционално снаряжение, осигуряващо с първия пуск (изстрел) унищожаване на цел (обект) от определен тип с гарантирана вероятност $P \geq 0,8$ във всякакви условия на бойно използване.

Нивото на ефективност се достига за сметка на високата точност на доставянето бойната част в обекта на действие – вероятно кръгово отклонение от точката на прицелване по-малко от 1 m – и мощност на БЧ, осигуряваща с вероятност $P \geq 0,9$ покритие на зоната за поражение и уязвимата зона на целта.

Предложеното определение за ВТО предявява някои конкретни изисквания, а именно: унищожението на цели от определен тип трябва да се осъществява от едно СП с първия пуск, точност на попадане на БЧ в целта, не по-малка от Евко ≤ 1 m, припокриването на зоната за поразяване на БЧ с уязвимата зона на целта трябва да се осигурява с вероятност не по-малка от $P \geq 0,9$ – съвкупността от всички тези условия ще доведе до унищожаване на целта с гарантирана вероятност $P \geq 0,8$. Практическата реализация на тези изисквания прави възможно напълно обоснова-

но и обективно в класа на ВТО да се разгледат конкретни средства за поразяване, действащи по определени цели (обекти).

В заключение искам да отбележа, че изпълняване на високите изисквания, предявени към ВТО е невъзможно без всестранното осигуряване, явяващо се съставна част от системата на ВТО, под което се разбира функционално обединение в единен процес на средствата за поразяване, средствата за доставка и средствата за управление със системата за информационно осигуряване (в това число разузнаването и целеуказването, бойното управление и свързките), осигуряващи гарантирано унищожение на целите (обектите) от определен тип.

Литература:

1. Военная мысль, бр. №8, 2013.
2. Военная мысль, бр. №2, 2010.
3. Словарь оперативно-стратегических терминов, МО СССР, Москва, 2006.
4. Военный энциклопедический словарь, МО СССР, Москва, 1984.
5. Наставление по подготовке и ведению военных действий ВС РФ, ч. 3, ГЩ ВВС, 2012.
6. Известия РАРАН, бр. №4, 2012.

Ст. Н. Чанев,

ЗЕНИТНОРАКЕТНА СИСТЕМА ЗА БЛИЗКО ДЕЙСТВИЕ КАТО СИСТЕМА ЗА МАСОВО ОБСЛУЖВАНЕ

Стоян Н. Чанев

Национален военен университет „Васил Левски“, Факултет „Артилерия, противовъздушна
отбрана и комуникационни и информационни системи“,
телефон: 054 801040, вътрешен 54266, e-mail: st.chanев@abv.bg

SHORT-RANGE TACTICAL SURFACE-TO-AIR MISSILE SYSTEM AS A MASS SERVICE SYSTEM

Stoyan N. Chanев

Abstract: The introduction of short-range tactical surface-to-air missile system as a mass service system allows it to assess its performance and to draw conclusions about its effectiveness, taking into account the countermeasures of air strikes

Keywords: Short-range tactical surface-to-air missile system, mass service system, effectiveness

Подходящ вариант за описване действията на СПВО с отчитане противодействието на въздушния противник е използването на теорията за масовото обслужване (ТМО). Всяка система за масово обслужване (СМО) се състои от обслужващи устройства – канали на обслужването. Предмет на ТМО е установяването на количествената зависимост между характера на входящия поток, производителността на отделния канал, броят на каналите и ефективността на обслужването.

За да се разглежда един процес като СМО, то входящият поток от заявки трябва да е прост (Пуасонов), т.е. да притежава следните три свойства:

- да е стационарен – вероятността за постъпване в СМО на заявки в интервала

от време τ не зависи от положението на интервала τ върху оста O_t ;

- да е без последствия – броят на заявките, появяващ се в един от интервалите не зависи от броят на заявките, появяващ се в другите;

- да е ординарен – вероятността за постъпване в даден минимален интервал от време с дължина Δ_t на две и повече заявки е пренебрежимо малка.

Първото условие, което трябва да бъде изпълнено е времето за обслужване на заявките да е случайна величина. В случая такава характеристика се явява времето за обслужване на въздушните цели (ВЦ) в налета, т.е. времето необходимо за обстрелването им. То е случайна величина, чиято продължителност се определя в интервала от момента на получаване на задачата (вземане на решение за обстрелване на целта) до оценка на резултатите от стрелбата включително. Случайният му характер се определя от вероятностния характер на съставлящите го времена, главно

от различното времетраене на ЗУР до точката на срещата с ВЦ в реализируемата зона и от продължителността на стрелбата.

Ако бъдат разгледани принципните особености на входящият поток ВЦ ще се види, че те притежават основните свойства на Поасоновия (прост) поток. Всъщност входящият поток (налета) се състои от детерминирани, обусловени от определени правила бойни редове. В зоната на действие на СПВО и нанасяне на удара обаче тези редове се нарушават и т.к. всичко това има вероятностен характер, то построението на налета се приближава по своите характеристики към Поасоновия поток.

ЗРС за близко действие с далечна граница на зоната за поражение (ЗП) до 10 км се представят като СМО с откази.

Характеристики на обслужването:

- продължителност на обслужването – зависи от параметъра μ – интензивност на обслужването. Определя се от израза:

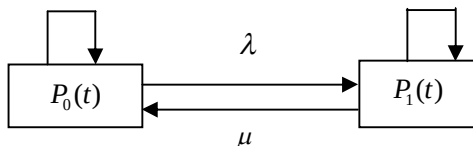
$$\mu = \frac{1}{m_{t_{об}}}, \quad (1)$$

където: $m_{t_{об}} = M(T_{об})$ – МО на времето за обслужване, $T_{об}$ случайна величина;

- пропускателна способност – определя се от максималния брой заявки, които може да се обслужат от СМО за единица време;

- достъпност на каналите – ако всеки канал на СМО след завършване на обслужването на дадена заявка приема за обслужване нова заявка и не излиза от строя, системата се нарича пълнодостъпна.

Нека разгледаме СМО с един канал. Състоянието на системата се дава с граф на състоянието.



Фиг. 1. Граф на състоянието на едноканална СМО

$S_0(t)$ – каналът е свободен – с вероятност $P_0(t)$;

$S_1(t)$ – каналът е зает – с вероятност $P_1(t)$.

Вижда се, че от състояние S_0 с вероятност $P_0(t)$ системата може да премине в състояние S_1 с вероятност $P_1(t)$ под въздействието на входящия поток от заявки с плътност λ , но може и да остане в същото състояние S_0 . От S_1 може да се върне в S_0 под въздействието интензивността на обслужване на заявките. В сила е:

$$P_0(t) = -\lambda P_0(t) + \mu P_1(t), \quad (2)$$

В стационарен режим (след някакъв преходен процес):

$$P_0'(t) = 0; P_0(t) \rightarrow P_0; P_1(t) \rightarrow P_1$$

Получаваме уравнение с две неизвестни:

$$\lambda p_0 - \mu p_1 = 0, \quad (3)$$

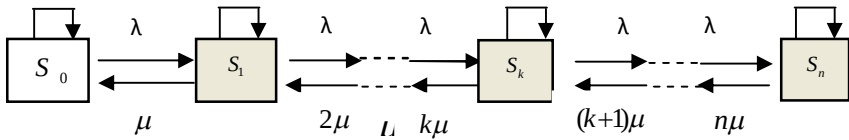
Но $P_0(t)$ и $P_1(t)$ – пълна група несъвместими събития, следователно се достига до система от две уравнения с две неизвестни:

$$\lambda p_0 - \mu p_1 = 0, \quad (4)$$

$$p_0 + p_1 = 1$$

При $\frac{\lambda}{\mu} = \alpha$ – приведена плътност на потока от заявки получаваме:

$$P_0 = \frac{1}{1 + \alpha}, \quad (5)$$



Фиг. 2. Граф на състоянията на многоканална СМО с откази

S_0 – всички канали са свободни – с вероятност P_0 :

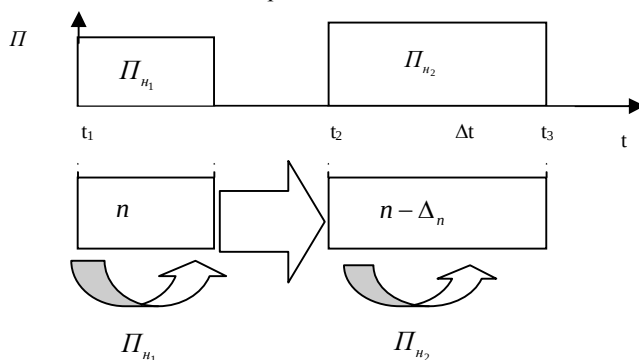
$$P_0 = \frac{1}{1 + \frac{\alpha}{1!} + \frac{\alpha^2}{2!} + \dots + \frac{\alpha^n}{n!}} = \frac{1}{\sum_{k=0}^n \frac{\alpha^k}{k!}}, \quad (6)$$

S_n – всички канали са заети – с вероятност P_n :

$$P_n = \frac{\alpha^n}{n!} P_0 = \frac{\frac{\alpha^n}{n!}}{\sum_{k=0}^n \frac{\alpha^k}{k!}}, \quad (7)$$

Основният проблем тук е, че потокът от заявки (налета) оказва противодействие. В резултат на това броят на целевите канали ще се променя (намалява). Удач-

но е да се разгледа СПВО, изградена от ЗРС за близко действие като многофазна СМО, където изходните данни от първата система се явяват входящи за втората.



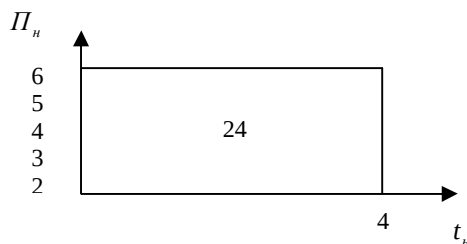
Фиг. 3. Представяне на СПВО като двуфазна СМО с откази

където: Δ – непоразените самолети от групата за подавяне на ПВО;

Δ_n – извадените от строя канали от групата за подавяне на ПВО.

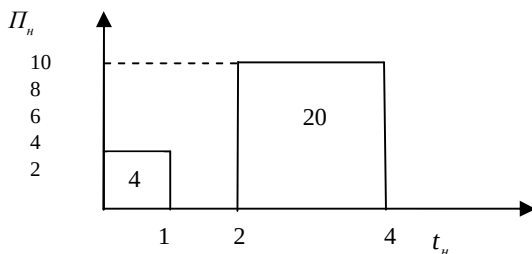
По същество системата с $n - \Delta_n$ канала е същата система с n канала, но след време Δ_t (с отчитане на противодействието). За всяка от двете системи са в сила формулите на Ерланг.

Чрез разделянето на потока и използването на двуфазна система се получава и плътност на налета по-близка до реалната – фигури №4 и №5 онагледяват процеса. Нека $N_y = 24$ за $t_n = 4$ минути. Следователно $\Pi_n = 6$.



Фиг. 4. Средна плътност на налета

Нека 4 от самолетите са за подавяне на ПВО, а на интервал една минута след тях е ударната група. N_y отново е 24, а $t_n = 4$ минути, но се вижда, че за времето на действие на ударната група Π_n достига 10 в продължение на две минути.



Фиг. 5. Реална плътност на налета

При така направеното привеждане на системата за СПВО към двуфазна СМО с откази изведените по-горе зависимости се трансформират както следва:

- интензивност на обслужването μ :

$$\mu = \frac{1}{m_{t_{\text{обсл.}}}} = \frac{1}{M(T_{\text{обсл.}})} = \frac{1}{M(T_{\text{ус}})} = \frac{1}{1} = 1, \quad (8)$$

т.к. за тактически разчети за ЗРС за близко действие $T_{\text{ус}} = 1$ минута;

- интензивност (плътност) на входящия поток λ :

$$\lambda = \Pi_n; \lambda_1 = \Pi_{n_1}; \lambda_2 = \Pi_{n_2}, \quad (9)$$

където: Π_n плътност на сумарния поток (целия налет);

Π_{n_1} плътност на първия поток (групата за подавяне на ПВО);

Π_{n_2} – плътност на втория поток.

- приведена плътност на налета α :

$$\alpha = \frac{\lambda}{\mu} = \frac{\Pi_n}{1} = \Pi_n, \quad (10)$$

- вероятност, че заявката ще бъде отказана (целта ще бъде пропусната), поради факта, че всички канали са заети:

$$P_{\text{отк}} = P_n, \quad (11)$$

- средно число заети целеви канали:

$$\bar{k} = \frac{A}{\mu} = A = \Pi_n (1 - P_n), \quad (12)$$

където: A – абсолютна пропускателна способност на системата. Поради факта, че $\mu = 1$ в случая $k = A$;

- брой на изпълнените заявки (въздействия, стрелби):

за 1 минута $N_{стр} = A$; за времето на налета:

$$N_{стр} = At_n \leq \frac{C}{n}, \quad (13)$$

където: C – 1 БК;

n – разход на боеприпаси (ракети) за една стрелба.

Оценка на качеството на функциониране на системата за противовъздушна отбрана (СПВО)

По същество под ефективност на изградената СПВО се разбира степента на изпълнение на поставената задача. По тази причина ПВО не трябва да бъде ориентирана към неизпълнимата задача да не бъдат допуснати удари на ВП по прикриваните войски и обекти, а да се осигури гарантирана защита на войските и обектите на равнището на приемливите загуби, т.е. изходна точка при оценката на ефективността на ПВО трябва да бъде поставената конкретна задача. В зависимост от възможностите на ВП, прикриваните обекти, влиянието на средата и разполагаемите сили и средства за ПВО поставената задача може да бъде:

- скриване действията на ВП;
- отразяване действията на ВП;
- намаляване потенциала на ВП – при явна асиметричност във възможностите.

Оценката на ефективността се извършва по определени критерии. Те трябва да съответстват на решаваната задача, да бъдат чувствителни към изменение на изходните данни, да имат явен физически (тактически) смисъл. За практически разчети на тактическо ниво при определяне ефективността на СПВО може да бъде използван метода за разчет на надеждността на ПВО (понятието надеждност тук е използвано в смисъла на надеждност на зенитното прикритие, а не вероятност за безотказна работа). Този метод е основан на използването в качеството на критерий на ефективността на ПВО коефициента на надеждност на ПВО - $K_{нпво}$. Този коефициент изразява отношението на броя унищожени самолети на противника или тяхното математическо очакване (МО) към общия брой ВЦ в налета или за определен период от бойните действия:

$$K_{нпво} = \frac{N_{униц}}{N_{ц}}, \quad (14)$$

Според избрания критерий ПВО може да бъде:

- надеждна – $K_{нпво} > 18\%$;
- устойчива – $K_{нпво} = 12 \div 18\%$;
- слаба – $K_{нпво} < 12\%$,

като в качеството на показател за определяне на ефективността се използва МО на количеството поразени цели.

Разчета може да се извърши в следната последователност:

1) Групата за оперативно планиране (ГОП) моделира действията на ВП с отчитане на етапа на боя, важността на обектите, силите и средствата за ПВО, бойните възможности на ВП и влиянието на местността;

2) Задава се праг на ефективността – $K_{\text{нпвостд}}$;

3) На базата на т.1 се определят параметрите на налета – $N_{\text{г}}$, $t_{\text{н}}$, $\Pi_{\text{н}}$, $\Pi_{\text{г}}$ (на групата за подавяне на ПВО), $\Pi_{\text{н2}}$ (плътност на вторият поток);

4) Определя се абсолютната пропускателна способност на системата A_1 по отношение на $\Pi_{\text{г}}$;

5) Пресмята се броят на въздействията за времето на действие на групата за подавяне на ПВО;

6) Определя се МО на броя поразени ВЦ от групата за подавяне на ПВО:

$$M_{n_1} = A_1 t_{n_1} [1 - (1 - P_1)^n] k_{\text{гпр}} k_{\text{бс}} k_{\text{нр}} k_{\text{уч}} , \quad (15)$$

където: n – среден разход на ракети (боеприпаси) за една стрелба от един целеви канал;

P_1 – вероятност за поразяване на единична цел при една стрелба от един целеви канал;

$k_{\text{уч}}$ – коефициент на участие в стрелбата от целевия канал;

$k_{\text{нр}}$ – коефициент отчитащ противодействието на противника срещу целевия канал;

$k_{\text{бс}}$ – коефициент отчитащ боеготовността на целевия канал за изпълнение на поставената задача;

$k_{\text{гпр}}$ – коефициент отчитащ ефективността на управлението.

7) Определя се МО на броя поразени ЦК – Δ_n :

$$\Delta_n = (N_{\text{г1}} - M_{n_1}) P_{\text{нод}} , \quad (16)$$

където: $N_{\text{г1}}$ – броят на ВЦ в групата за подавяне на ПВО;

$P_{\text{нод}}$ – вероятността една цел от групата за подавяне на ПВО да унищожи един ЦК.

$P_{\text{нод}}$ се определя чрез следния израз:

$$P_{\text{нод}} = Q_{\text{нво}} W_{\text{иц}} P_{\text{нор}} k_{\text{н}} , \quad (17)$$

където: $Q_{\text{нво}}$ – вероятност за преодоляване на ПВО. За целите преминавали през зоната на огъня $Q_{\text{нво}} = 1$;

$W_{из}$ – вероятност за излизане в района на целта – зависи от физикогеографските особености на района и мобилността на обектите, определени за удар.
 $W_{из} = 0,7 \div 0,9$;

$P_{пор}$ – вероятност за поразяване с отчитане на противодействието, $P_{пор.} = 0,7$;

k_n – коефициент на надеждна работа на съвкупността платформа–АСП, $k_n = 0,9$

8) Преизчислява се Пн2 (самолетите от групата за подавяне на ПВО преминали през зоната на огъня нарастват усилията на ударните групи);

9) Определя се абсолютната пропускателна способност – A_2 по отношение на преизчисления $P_{н2}$ с отчитане намаления брой ЦК с Δ_n ;

10) Определя се МО на броя поразени цели от втория поток – M_{n_2} в съответствие с (15) с използване на A_2 и $t_{н2}$ и отчитане разхода на ЗУР;

11) Определя се МО на броя поразени цели при огрязване на налета:

$$M_n = M_{n_1} + M_{n_2}, \quad (18)$$

12) Изчислява се $k_{нво}$ и се сравнява с $k_{нво зад}$.

Точки 1÷12 се пресмятат за различен брой канали 1÷п от състава на ЗРС за близко действие и резултатите се записват в табличен вид. Необходимо е да се ограничи п от гледна точка на рационалното използване на силите и средствата за ПВО и осигуряване на зенитно прикритие на всички елементи от бойния ред на войските и обектите за прикритие.

Опитът от последните конфликти сочи, че броят ЦК, необходими за постигане на ефективност не по-ниска от зададената, се ограничава от условието:

$$n - \Delta n \leq n_{уд.группи}, \quad (19)$$

където: $n - \Delta_n$ – целевите канали след противодействието;

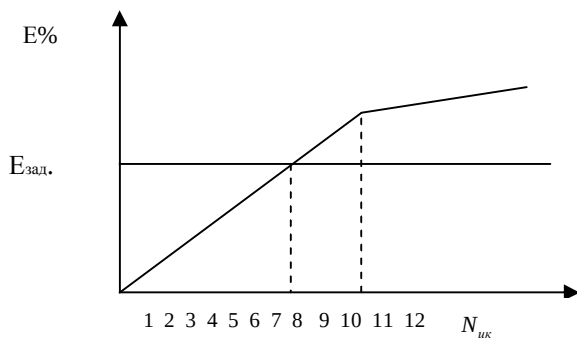
$n_{уд.группи}$ – броят на ударните групи.

При създадена сложна ВО, наличието на ненадеждни средства за радиолокационно разузнаване и бойно управление, когато не е възможно да се оценят целите по важност, то те се приемат за еднакви по важност и израза (19) добива вида:

$$n - \Delta n \leq n_{вл.группи}, \quad (20)$$

където: $n_{вл.группи}$ – броят на влитащите групи.

Броят на ЦК, за които е изпълнено условието $k_{нво} > k_{нво зад}$ е показан на фигура №6 (примерен вариант):



$$n - \Delta_n = n_{\text{вл. групи}}$$

Фиг. 6. Ограничаване на полосата от ЦК

Чрез показателите за ефективност на СМО може да се анализират възможните варианти за постигане на зададената ефективност, като за отправна точка се взема текущото състояние на СПВО. Ако в резултат на предшестващи бойни действия имаме ограничение в броя на изправните сили и средства за ПВО, то ГОП ще се ориентира към $n_{\min}$. При липса на ограничения може да се търси оптималност, т.е. да се анализира отношението на средното число заети канали към общият брой на каналите; минимизиране на загубите; вероятност за пропускане на целта $-P_n$ или максимална ефективност.

Литература:

1. Стойков С.Д., Усъвършенстване на системата за бойно управление на групировка за противовъздушна отбрана, София, 1997
2. Николов Н. В., Преодоляването на противовъздушната отбрана от ударната авиация, учебно пособие, ВА, София, 2004
3. Митрев, Д., Оценка на огневите възможности на ЗРП „Куб” по методите на теорията на масовото обслужване, учебно пособие, ВИ, София, 1987
4. Саати, Т., Элементы теории массового обслуживания и её приложения, Советское радио, Москва, 1971

К. А. Илиев, Р. Б. Чалъков,
**„СЪВМЕСТНА ОГНЕВА ПОДДРЪЖКА” – ФАКТОР
В СЪВРЕМЕННИТЕ ОПЕРАЦИИ**

Калоян А. Илиев, Радослав Б. Чалъков

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen.

**"JOINT SUPPORT MAINTENANCE" - A FACTOR IN CONTEMPORARY
OPERATIONS**

Kaloyan A. Iliev, Radoslav B. Chalakov

Abstract: *Joint fire maintenance in modern operations is aimed at bringing such losses to the enemy, leading to an unacceptable loss of the opponent and a change in the ratio of forces to our advantage and hence to the fulfillment of the assigned task in the operation. It involves different forces and means, with different possibilities and ways of use.*

Keywords: *Joint fire maintenance, lost, operations, contemporary operations*

Съвместната огнева поддръжка е една от основните бойни функции и представява прилагане на огнева мощ, чрез огън от средства от закрити огневи позиции, средства за електронна война (ЕВ), самолети и вертоleti на военновъздушния компонент (ВВК) и военноморския компонент (ВМК), координирана с маневрените формирования с цел унищожаване, неутрализиране и подавяне на противника.

Съвместната огнева поддръжка в операциите е координирано комплексно огнево въздействие върху противостоящия противник с цел нанасяне на максимални загуби на войските и оръжията му и създаване на благоприятни условия за постигане на желания краен резултат на операцията. Съвместната огнева поддръжка е бойна функция, която обединява и съгласува ударите и огъня на оръжията и техния поразяващ ефект за задържане, възпрепятстване, дезорганизиране или сричане на действията на противниковите групировки в хода на изпълнението на оперативните и тактическите задачи.

Чрез нея могат да се измерват резултатите създадени от ефективното използване на огневата мощ и маневъра в тясна връзка със защитата на войските и умението за управление. Тя се провежда от всички оръжия и системи, с които разполага командващия на съвместните сили. Много от тези оръжия и системи, с изключение на определени земно базирани оръжия за стрелба с директно насочване, са в категорията на средствата за съвместна огнева поддръжка, които представляват главния източник на огнева мощ.

Основната цел на съвместната огневата поддръжка е завоюване и удържане на огневото превъзходство над противника на направленията на нанасяните удари с войски, дезорганизиране на системата за командване и управление на войските и

оръжията, нанасяне на решително поразяване на групировките в направление на ударите и непрекъсната поддръжка на настъпващите войски.

На настоящия етап от развитието на средствата на въоръжената борба (широкото внедряване на високоточни боеприпаси) все повече се заговори за дистанционни способности за разгром на противника. Същността на дистанционният разгром на противника се заключава в нанасянето на изпреварващи огневи удари и провеждането на операции от нов тип – огнево сражение, огневи бой и др.

Съвместната огнева поддръжка се прилага на оперативното ниво. Във втория случай това се случва, когато единият от компонентите провежда основната операция, а останалите компоненти провеждат поддържащи операции в негов интерес. Ето защо съвместната огнева поддръжка може да бъде определена като прилагане на споделени ресурси (разположени на земя, въздух и море), което включва средства за разузнаване, наблюдение и определяне местоположението на целите, комуникации, определяне на целите и вземане на решения, командване и управление, оръжия и оценка на бойните загуби за предоставяне на защита на собствените войски.

В основата на съвместната огнева поддръжка в текущите операции е съвместната координация на ударите и огъня, като целта е да се развият на високо ниво определени изисквания, когато дадения компонент провежда основна или поддържаща операция и оръжията са базирани на земята, на море или във въздуха. Всеки командир на компонент може да поиска огнева поддръжка относно новопоявили се и/или определени предварително цели. В такива случаи при планирането на съвместната огнева поддръжка трябва да бъдат определени и приоритизирани целите за поразяване от най-подходящата оръжейна система на разположение на съвместните сили. За тази цел, процесът на планиране и нанасяне на удари, следва да бъде насочен така, че да позволи на органите да вземат най-доброто решение, да определят най-добрите средства за въздействие, да използват установени процедурни процеси, надеждно управление и контрол, разпределение на персонала, желаните ефекти от използване на оръжията и оценка на ефектите от нанесените удари, с цел да се оптимизира съвместната огнева поддръжка.

Първостепенен приоритет на съвместната огнева поддръжка е да се интегрират съвместните действия на сухопътния, военновъздушния, военноморския и компонента сили за специални операции за постигане и непрекъснато удържане на огнево превъзходство над противника.

Основните цели на съвместната огнева поддръжка са:

- ☐ Завоюване и непрекъснато удържане на огнево превъзходство над противника при провеждане на сухопътната операция;
- ☐ Изменение на съотношението на силите и средствата до искано ниво;
- ☐ Дезорганизиране на системата за командване и управление на войските и оръжията на противника;
- ☐ Нанасяне на решително поразяване на групировките на противника на направленията за съсредоточаване на силите и средствата (на нанасяните удари);
- ☐ Непрекъсната поддръжка на бойните действия на маневрените формирования от състава на сухопътния компонент.

Важен елемент за своевременно въздействие върху потенциалните цели е използването на сухопътните, въздушните и морските разузнавателни средства за откриване и оценяване на тези цели. Тази информация трябва да бъде докладвана в органите за таргетиране и за координиране на съвместната огнева поддръжка и ефек-

тите. Координаторът на съвместната огнева поддръжка може да приоритизира исканията за огнева поддръжка срещу специфични цели и след това да назначи средство за поразяване чрез използване на информация за наличните оръжейни системи и ресурси и висококачествено ситуационно разпределение. Целта е да се направи времеви график на поразяването на исканите цели, оптимизиране на ефекта на поразяване на целите и незабавно използване на постигнатия ефект след края на огневото въздействие.

За да са съвместими силите и средствата при провеждане на съвместната огнева поддръжка, трябва да се използват еднакви понятия от всички участващи в нея, такива като: удари, огън и ефекти.

Удари и огън е използване на оръжейни системи за създаване на специфични смъртоносни или несмъртоносни ефекти над целта в борбата за огнево превъзходство.

Ефектът е физически, функционален или психологически резултат (последствие), събитие или значение, който се постига чрез прилагане на специфични военни или невоенни действия за удържане на огневото превъзходство. Обобщено последствие от една или повече дейности в зоната на операцията, водещо до промяна на обстановката в едно или повече направления. Обобщаването на въздействието от един или повече аспекти води до изпълнението на поставените цели.

Борбата за огнево превъзходство при провеждането на съвместната огнева поддръжка, следва да е насочена към използването на ударите и огъня в интерес на маневрените формирания. Това изисква вземане на най-целесъобразното решение за използване на силите и средствата в съвместната огнева поддръжка, отчитайки голямото значение на ефектите за постигане на искания резултат.

Съвместната огнева поддръжка дава съвместен подход, при който индивидуалните системи от различни елементи (разположени на земя, въздух и море) се интегрират като съвместени.

В процеса на оперативно планиране, предварително разузнатите и планирани за поразяване цели се обработват. Вероятно инструментите и възможностите, които следва да се развиват като част на съвместната огнева поддръжка по време ще бъде удобно и полезно за изпълняващия тези задачи персонал. Крайният резултат от това усилие подпомага оперативната обработка на ударите и огъня, т.е. предварително подготвените мисии се превръщат в огневи мисии в системата, като се употреби част (потенциално голяма) от наличните ресурси за изпълнение на мисиите. По този начин, при поразяването на внезапно появили се цели в борбата за огнево превъзходство, една част от поразяващите средства могат да се привличат да поразяват предварително набелязаните цели (като е възможно всяка една да се премести във времевата линия за поразяване или да се назначат различни ресурси да изпълнят предварителната мисия), а другата част от тях да поразяват планови цели. Освен това може да наложи оценките на предварително набелязаните цели да се променят (да претърпят неуспех), което налага една такава цел да се счита за новопоявила се.

На преден план излиза въпроса дали снабдяването е проблемен въпрос на съвместната огнева поддръжка. Като част от съвместната огнева поддръжка, то следва да е насочено към непрекъснато изучаване състоянието на силите и средствата за поразяване и това да бъде основа за извършването на снабдяването с необходимите боеприпаси. По всяко време координаторът на съвместната огнева поддръжка и ефектите трябва да знае коя оръжейна система е на разположение, когато се избира

такава за нанасяне на удар. Тази информация се използва и при снабдяване с необходимите боеприпаси. Специфичните инструменти, заедно със съвместната огнева поддръжка подкрепят, планирането на доставките на боеприпаси, като се отчитат наличните запаси от боеприпаси, отпуснатите боеприпаси и тяхното разпределение по фази на операцията и по дни.

Вземането на решение за провеждане на съвместната огнева поддръжка на стратегическо ниво се извършва в частта ресурсно планиране. Оперативното ниво е основно и най-важно при планирането на борбата за огнево превъзходство в системата на съвместната огнева поддръжка. При него се определят основните приоритети на ударите и огъня, при което се извършва:

- ☐ Съставяне на списък с приоритетните цели;
- ☐ Съставяне на списък с целите с голяма стойност;
- ☐ Подготовка на заповедите за операцията на въздушния компонент;
- ☐ Събиране и анализиране на разузнавателните данни (карти, културни ценности в зоната на операцията, известни местоположения на противника и на приятелските сили, зони забранени за стрелба и т.н.);
- ☐ Непрекъснато събиране и анализиране на данните за времето;
- ☐ Събиране и анализиране на информация за бойна идентификация;
- ☐ Поддържане на база данни за състоянието на оръжията на всички компоненти;
- ☐ Определяне на правилата за употреба на сила и поведение;
- ☐ Непрекъснато изучаване намеренията на командващия за изпълнение на мисията;
- ☐ Събиране на информация за коалицията и състоянието на компонентите.

При провеждането на съвместната огнева поддръжка на оперативно ниво се правят определени допускания, които включват:

- ☐ Действията по нанасянето на ударите и огъня в съвместната огнева поддръжка се извършват най-вече на оперативно ниво;
- ☐ Най-голяма е връзката на процеса на разузнаване и оценка на бойните загуби на противника в резултат на използването на средствата за огнева поддръжка;
- ☐ Приема се, че силите и средствата участващи в борбата за огнево превъзходство от състава на сухопътния, военновъздушния и военноморския компоненти са напълно обучени и тренирани да действат в операции базирани на ефектите и в съвместна, национална среда;
- ☐ Координаторът на съвместната огнева поддръжка има достъп до основна база-данни;
- ☐ В хода на провеждането на съвместната огнева поддръжка може да бъдат предложени нови доктрини, тактики, техники и процедури за усъвършенстване на процесите на планирането и координирането на борбата за огнево превъзходство;
- ☐ Налагане на определени изисквания за оценка на бойните загуби на противника в борбата за огнево превъзходство;
- ☐ Допуска се, че при необходимост от нанасяне на удари и огън има в наличност свободни средства и боеприпаси за тях;
- ☐ Приема се, че наличните средства за разузнаване, наблюдение и определяне местоположението на целите са в състояние да дадат необходимата информация за целите за поразяване с необходимата точност, удовлетворяваща средствата за поразяване;

□ Допуска се, че наличните оръжейни системи са в състояние да поразят с необходимата точност и в точно определеното време определените противникови цели.

Ролята на съвместната огнева поддръжка се определя от степента на интензивност на военния конфликт и нивото на планирането и координирането и т.е. от нейните цели. Ролята на съвместната огнева поддръжка може да се дефинира на три нива: стратегическо, оперативно и тактическо.

На стратегическо ниво се формулират национални или многонационални (съюзни или коалиционни) цели за сигурност и ръководство, развиват се и се използват национални ресурси, за да изпълнят тези цели. Дейностите на това ниво: довеждат национални и многонационални военни цели; последователни инициативи; определят границите и оценката на риска за използване на военни и други инструменти на националната мощ; развиват глобални планове или военни планове за постигането на тези цели.

На оперативно ниво се извършват дейности, при които кампаниите и главните операции се планират, провеждат и продължават за изпълнение на постигане на стратегическите цели на театъра на операциите и в други оперативни зони. Дейностите на това ниво свързват тактики, техники и процедури за определянето на: оперативните цели, необходими за изпълнение на стратегическите цели; прогнозиране на последващи събития за постигане на оперативните цели; инициране на действия и използване на ресурси за довеждане до желан резултат и поддържане на тези събития. Тези действия съдържат граници на пространството и времето, в което действат тактиките.

Те осигуряват логистичната и административната подкрепа на тактическите формирования и създават условия средствата, с които са постигнати тактически успехи, да се използват за достигане на оперативните и стратегическите цели.

На тактическо ниво се извършват дейности, при които бойните действия се планират и изпълняват за постигането на военни цели, поставени на тактически формирования или групировки. Действията на това ниво се фокусират за изпълнение на заповяданите бойни задачи и маньовър от маневрените, бойните и ударните формирования в тясно взаимодействие едни с други и в пряк контакт с противника за постигане на неговия разгром и изпълнение на поставените бойни задачи.

Начална точка за създаване на модела на съвместната огнева поддръжка са разработените концепции за операциите и за съвместната огнева поддръжка. Това е работен документ, който развива процеса за по-нататъшна работа чрез концепцията за развитие и експериментиране. Концепцията за операциите и за съвместна огнева поддръжка е в приоритетите на съвместните сили .

Голямо влияние върху съвместната огнева поддръжка оказва възприетата и разработена оперативна концепция. Изборът на термина „оперативна концепция” от повече основни оперативни концепции е с цел да се избегнат възможни обърквания под двойственото значение на термина „оперативен”, който може да се отнесе специфично само към оперативното ниво на планиране на операциите, но често се отнася основно за всеки вид военни действия. По начина, използван тук, терминът „оперативна концепция” се отнася до произнасянето на термини в широким им смисъл на провеждане на операции, независимо от нивото на планирането им. Някои такива концепции може да имат приложение на повече от едно ниво.

Дейностите по провеждането на съвместната огнева поддръжка трябва непрекъснато да се подлагат на контрол и оптимизация. Оптимизираната концепция за операцията и процесите на провеждане на съвместната огнева поддръжка могат да бъдат развити чрез използването на комбинация от дейности, по-важни, от тях са:

- Възможностите на техническите средства за извършване на определени разчети и за математическо моделиране на процесите на планиране на съвместната огнева поддръжка;
- Конструктивното моделиране и симулациите на операциите и съвместната огнева поддръжка;
- Анализът на човешкия фактор, извършващ планирането на съвместната огнева поддръжка;
- Инструментите за подпомагане на взетите решения;
- Възможностите на използваните оръжия и постигнатите ефекти;
- Моделирането и симулациите – обединено развитие и процес на изпълнение;
- Експериментирането на създадените концепции за операцията и за съвместната огнева поддръжка.

Един от важните инструменти за определяне възможните цели за поразяване е непрекъснатото дефиниране и управление на таргетинг процесите. Тази рамка осигурява указания за това как да се обясни възможността за представяне по последователен начин, който да облекчи оценяването на системните решения. Процесите за планиране и управление на съвместната огнева поддръжка са обхват-спектър, обхват, информация, сътрудничество, подвижност (устойчивост) и запазване. При това рамката служи като указание за развитие от съответната йерархия на мерки за способности при разглеждане на определена заплаха или важност на цел.

За да има определен ефект от провеждането на съвместната огнева поддръжка трябва непрекъснато да се усъвършенства реда за постигане на съвместни ефекти. В процеса на вземане на решение за провеждане на съвместната огнева поддръжка е целесъобразно да се използват 13 стъпки и дейности за избор и поразяване на целите в борбата за огнево превъзходство:

- 1) Оценка на целта според възприетите стандарти за избор на цели;
- 2) Информация за анализ на целта;
- 3) Разпределение (разделяне) на информацията за целта;
- 4) Оценка на оставащото време до исканото начало за поразяване на целта;
- 5) Оценка на крайното състояние на целта;
- 6) Потвърждаване на активността на целта;
- 7) Решение кога да се предприеме действие;
- 8) Решение кога да се въздейства на целта;
- 9) Сравняване на възможностите на оръжието с характеристиките на целта;
- 10) Решение как да се въздейства върху целта;
- 11) Идентифициране на наличните средства за поразяване;
- 12) Следващо изискване на правомощия;
- 13) Крайно решение за предприемане на действие .

Специфичните детайли на индивидуалните стъпки могат да се групират, като съдържание на три фази с пресечни точки за решения, наречени:

Първоначална фаза, където идентичността и съдържанието на целта са оценени чрез първите три стъпки: „Оценка на целта според възприетите стандарти за избор

на цели”, „Информация за анализ на целта” и „Разпределение (разделяне) на информацията за целта”;

Следваща фаза, в която е събрана информацията, за да се осигури вземането на решение, независимо от това дали целта е ефективна или не чрез стъпки „Оценка на оставащото време до исканото начало за поразяване на целта”, „Оценка на крайното състояние на целта”, „Потвърждаване на активността на целта”, „Решение кога да се предприеме действие” и „Решение кога да се въздейства на целта”;

Крайна фаза, когато се предлага решение за въздействие върху целта чрез стъпки „Сравняване на възможностите на оръжието с характеристиките на целта”, „Решение как да се въздейства върху целта”, „Идентифициране на наличните оръжия”, „Следващо изискване на правомощия” и „Крайно решение за предприемане на действие”.

За постигане на исканите ефекти от провеждането на съвместната огнева поддръжка командващият трябва да разполага със специфична информация за координиране на ударите и огъня, която му дава възможност да оптимизира плана и да възприема оптимални варианти за действие.

Тази информация трябва да осигурява специфични данни за:

- Разполагането на средствата за огнева поддръжка, комуникационните системи за управление на оръжията, броя, вида и възможностите на оръжията;

- Синхронизационният статус на средствата за огнева поддръжка (в готовност да получават и изпращат данни);

- Формированията, искащи огнева поддръжка (ефект);

- Местоположението и координатите на целта, разстоянието на стрелбата;

- Характеристиките и предназначението на целта; за огнева поддръжка; за инженерна поддръжка (мост); система за командване и управление (команден пункт); средство за противовъздушна отбрана; маневрена или неподвижна цел; степен на укритост на техниката и личния състав и др.;

- Състояние на формирането искащо огнева поддръжка – формирание под обстрел, в контакт, критична мисия, подкрепа на мисия;

- Искан ефект от огъня и ударите или заявена огнева поддръжка – разрушаване, подтискане, отхвърляне, разстройване, забавяне, неутрализиране, въздействие;

- Искана загуба на целта, определена чрез използване мощта на съвместната огнева поддръжка;

- Определяне на вероятността за постигане на желания ефект;

- Определяне на вероятността за получаване на желани или нежелани вторични загуби.

- Брой на боеприпасите за постигане на ефекта и времето за небоеспособност на целта след края на огневото въздействие;

- Оценка на бойните загуби на целта;

- Ефект от времето на небоеспособност и начин на използване на ефекта от маневрените формирования искащи поддръжка.

За постигане на исканите ефекти координаторът на съвместната огнева поддръжка трябва да предлага на командващия различни варианти на действие и използване на оръжията и боеприпасите.

Различните варианти трябва да осигуряват изпълнението на специфичната заявка на огнева поддръжка, като всички заявки за поддръжка (или ефект) се приори-

тизират съгласно намеренията на командващия, правилата за поведение и употреба на сила, списъка на приоритетните цели, състояние на спешност и др. Командващият трябва своевременно да бъде информиран за начина на изпълнението на решенията за поразяване на целите в окончателния вариант на действие.

Изводи:

1. Ефективността на съвместната огнева поддръжка се основава на спазването на определени принципи и прилагането на единни щабни процедури в работата на органите за планиране и координиране на съвместната огнева поддръжка и за планиране на целите в съответствие с желаните ефекти.

2. Факторите оказващи влияние на съвместната огнева поддръжка могат да бъдат обединени в две групи. Първата група фактори са свързани със съвместимостта на огневите системи и подготовката на личния състав за работа в национална и многонационална среда. Втората група фактори са свързани с дейността на органите за планиране и координиране на съвместната огнева поддръжка и ефектите и за планиране на целите.

3. Познаването и анализът на факторите, които влияят на съвместната огнева поддръжка е в основата на планирането и координирането на операцията на съвместните сили. Съвместната огнева поддръжка е в основата на съвместното планиране и координиране в операцията.

Литература:

1. Доктрина на съвместните операции. ГЩ на БА 2001г.
2. Доктрина на сухопътните войски. Част втора. Тактическа доктрина на Сухопътните войски. София. 2001
3. Доктрина на сухопътните войски – част 1, 2001.
4. Гюргаков, И. „Съотношението на силите в операцията – важен фактор за нейният успех”. Научна конференция на В.А. 2006
5. Гюргаков, И. „Проблеми при планирането на огневата поддръжка при поразяването на първостепенни обекти и цели в операцията”. Учебно пособие, С, ВА, 2006
6. Гюргаков, И. „Огнева поддръжка в съвременните операции”, учебник, В.А. 2007
7. Гюргаков, И. „Огнева поддръжка в съвременните операции”, учебник, В.А. 2007
8. Гюргаков, И. „Огнева поддръжка и ефекти в съвременните сухопътни операции”. Военен журнал 2/2008
9. Гюргаков, И. „Съвместна огнева поддръжка”. Учебник. ВА „Г.С.Раковски” 2009
10. Гюргаков, И. „Планиране на огневата поддръжка на артилерията”, учебник, В.А. 2009
11. Гюргаков, И. „Нов поглед към системата за поразяване на противника в операциите на съвместни оперативни сили”, доклад, военен журнал, книжка 5, 2009

БОРБА ЗА НЕЗАВИСИМОСТ НА ТУАРЕГИТЕ В ОБЛАСТТА АЗАВАД

Ивел Иванов Кешишев

Национален военен университет „Васил Левски, Факултет “Артилерия, противовъздушна отбрана и комуникационни и информационни системи”

INDEPENDENCE STRUGGLE OF TUAREG IN AZAWAD REGION

Ivel Ivanov Keshishev

Abstract: *On northern part is located Azawad region. The size of region is almost 60% of whole territory of Republic of Mali*

Keywords: *independence, struggle, tuaregs, war, Republic of Mali, coalition, allies.*

В северната част на Мали се намира регионът Азавад, който съставлява 60% от площта на Република Мали. Условно той е обширна територия, която заема част от териториите на Алжир, Нигер, Либия и Буркина Фасо. В Малийската част на Азавад се намират областите Тимбукту, Гао и Кидал. Географията на Азавад е доминирана от обширни пустинни терени. Това означава и по-малко ресурси (включително храна и вода), което налага номадския начин на живот на голяма част от населението. Населението е 1.293.449 души. Туарегите са най-многобройната част от населението на региона. Народът на туарегите води полу-номадски начин на живот. През 7 век те приемат Сунитското направление на исляма. Тяхното общество е съставено от племенни кланове, които са йерархично организирани. Системи е изградена от благородници, духовенство, занаятчии и роби. В края на 19. век териториите, на които живеят туарегите, са завзети от френските колониални войски. От тогава до ден днешен техният народ се бори да основе своя собствена държава. За пръв път през 1960 година туарегите се опитват да сформират държава на територията Малийски Азавад чрез водене на въоръжена борба, но армията на Мали потушава бунтовете на независимост. Вторият опит за основане на туарегска държава избухва през май 1990. Боевете са кръвпролитни и се водят на територията на източен Нигер и северно Мали. Под наблюдението на Република Франция и Алжир са подписани мирните споразумения, през януари 1992 с Мали и 1995 с Нигер.

На 16 януари 2012 туарегите започват да водят сражения срещу малийската централна власт. Кампанията е водена от Националното движение за освобождение на Азавад, през април същата година областта е под контрола на туарегските племена. Значителен принос за успеха имат туарегските бойци идващи от Либия. След падането на режима на Муамар Кадафи, голям брой туареги, които са се сражавали на страната Кадафи се изтеглят в Северно Мали, заедно с тях те донасят тежко въоръжение. Бойният опит и техниката, която в миналите кампании за независимост е отсъстала, като част от въоръжението на туарегите, изненадва въоръжените сили на Мали. Първият сблъсък е при малкия град Менака. Бунтовниците овладяват населеното място. На следващия

ден правителствените войски отвоюват града и района около него, но поради липса на боеприпаси, на 1 февруари НДОВА отново поема контрола на Менака. Неефективните мерки на правителството за справяне с кризата пораждат недоволство сред армията. Стига се до военен преврат, който сваля демократично избрания президент на страната Амаду Туре. Военната хунта на следващата сутрин поема властта над страната. НДОВА се възползват от събитията и засилват натиска си. На 30 март Киндал - столица на едноименната област, също преминава под контрола на туарегите. Към борбата за независимост активно се присъединяват и групировките Ансар Дин, Ал Кайда в ислямски Магреб, Движение за единство и джихад в Западна Африка, Ганда Исо, Арабско движение за Азавад. Най-развитият икономически град северно Мали – Гао, е окупиран от туарегските бойци на 31 март. След кратки бойни действия централните власти капитулират. Изпълнителният комитет на НДОВА се обръща към международната общност и декларира независимостта на Азавад. Декларацията е отхвърлена от Африканския и Европейския съюз. Паралелно с военните действия назряват и големи бежански вълни. От северно Мали бягат над 374 000 души.

Туарегските групировки са слабо въоръжени и зле организирани. Бунтовниците предимно използват пикапи с монтирани тежки картечници. За борба с въздушния противник се експлоатират ЗУ-23-2 и ПЗРК Стрела-2. Преносимите зенитно ракетни комплекси са внесени от Либия с тяхна цел е свален вертолет Ми-8 от състава на ВВС на Мали. Най-многочислени са Национално движение за освобождение на Азавад, негов политически лидер е Билал аг Ашериф, военен ръководител е бившият полковник от либийската армия Мохамед аг Наджем. Числеността на организацията е приблизително 10 000 души. По-голямата част от личния състав са военни с туарегски и берберски произход, служили във въоръжените сили на полк. Муамар Кадафи. Към тях се присъединяват и дезертъори от малийската армия. НДОВА са въоръжени с оръжие, изнесено от либийските военни складове след разгрома на Джамахирията през 2011. Близки по идеология с Националното движение за освобождение на Азавад са Арабско движение за Азавад и Ганда Исо. Тях ги свързва идеята за независима светска държава на туарегите. Ансар Дин е сунитска ислямистка организация формирана от Ияд аг Гали. Той е туарегски благородник и бивш дипломат от малийска мисия в Саудитска Арабия в Периода 2005-2008. Около 2000 члена и множество пикапи, модифицирани чрез монтирани на каросериите тежки картечници, и зенитни установки. Модифицираните автомобили изиграват важна роля в конфликта през 2013 година. Голяма част от арсенала на групировката е придобит посредством набези върху конвои от армията на Мали. Един от братовчедите на аг Гали е Хамда аг Хама е един от лидерите на Ал Кайда в ислямски Магреб. Поради тази връзка и общата идеология двете групировки са тясно свързани. Абделмалик Друкдел е лидер на организацията. Редиците и са попълнени от бойци произхождащи от държавите в района на Магреб. Членовете наброяват няколко хиляди и са разпръснати под формата на клетки и оперативни групи. За 2015 АКОВ са спечелили на 1 млрд. долара от контрабанда на оръжия, наркотици, антики и хора. По-късно през годината възникват противоречия между отделните бунтовнически фракции. Част от противниците на правителството са организирани в по-скоро светски настроеното Национално движение за освобождението на Азавад. След оттеглянето на правителствените войски Ал Кайда в Ислямски Магреб, Ансар Дин и Движение за единство и джихад в Западна Африка сформират коалиция стремяща се към налагане на радикални форми на исляма. Конфликтът между отделните групировки прераства във въоръжен сблъсък,

като представителите на Националното движение са победени от ислямистите и принудени да отстъпят от всички по-важни градове в северната част на Мали. В периода 26.06.2012 до 19.11.2012 се водят боеве между туарегите националисти и радикалните ислямисти, като през този период неколккратно се променят регионите под контрол между двете враждуващи страни. В края на октомври НДОО си възвръща Тимбукту и Киндал. На 16.11 град Гао е окупиран от ислямистките групировки. В едно от стълкновенията е ранен генерал Билал аг Ашериг военния ръководител на НДОО. Междувременно се формира международна военна коалиция, която получава разрешение от Съвета за сигурност на ООН да се заеме със стабилизирането на положението в страната. Коалицията се състои от други африкански страни (Чад, Нигер, Нигерия и др.) и от държави членки на ЕС. Водеща роля има Франция. На 11.01.2013 започва операция „Сервал“, ръководена от френските въоръжени сили. В нея си сътрудничат френските, малийските войски и 3330 военнослужещи от страни от западна Африка. Интервенцията е предприета с цел възпиране напредването на радикалните групировки към столицата на Република Мали-Бамако, защитата на няколкото хиляди френски граждани в страната, опазване на териториялната цялост на страната и освобождаването на северната част на страната от ислямистките бунтовнически организации. Френските войски участват с 3500 военнослужещи предимно от състава на Френския легион, подразделения от специалните части, многоцелеви вертолети SA-342 „Газела“, многоцелеви изстребители „Рафал“ и стратегически бомбардировачи Mirage-2000 D. В конфликта френската армия губи 5 военнослужещи и 1 вертолет. Най-интензивни са боевете през периода 11-13.02.2013 в боевете при бастията на ислямистите град Гао. В операцията за овладяване на Гао участват подразделения на армията на Мали подкрепени от френски войски и от НДОО. Боевете се водят в околностите на града, нанесени са и множество удари от френската авиация. Радикалните ислямисти губят над 250 бойци и около 30 бойни пикапа. На 16.02 започва настъпление срещу всички позиции на ислямистките групировки. В него участват и войски от състава на въоръжените сили на Нигерия, Нигер, Чад, Габон и Канада. До юни месец всички градове са отвоювани от ислямистите. На 18.06 туарегските бунтовници и правителството на Мали подписват мирно споразумение. В боевете са убити и лидерите на АКИМ Абделхамид абу Зеид, Моктар Белмоткар. ООН основава мисия, целяща да стабилизира мира в региона - MINUSMA. 20.02.2015 е дата, в която окончателно се прекратява огънят между Националното движение за освобождение на Азавад и Република Мали.

При конфликта в Азавад загиват 210 военнослужещи от коалицията срещу радикалните ислямисти и над около 750 бойци от радикалните организации. Над 370 000 бежанци и множество унищожени културни паметници. В наши дни продължават да се водят боеве срещу малки групи бунтовници. Районът остава все още дестабилизиран.

Литература:

1. <https://remilitari.wordpress.com/whoiswho/insahel/>
2. <http://www.wreview.eu/s/konfliktyt-v-mali.html>
3. https://en.wikipedia.org/wiki/Northern_Mali_conflict
4. https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F_%C2%AB%D0%A1%D0%B5%D1%80%D0%B2%D0%B0%D0%BB%C2%BB

Х. А. Десев,

ПОДХОДИ ЗА ПОВИШАВАНЕ НА ЕФЕКТИВНОСТТА ПРИ ПРОТИВОДЕЙСТВИЕ НА ИЗПОЛЗВАНЕТО НА ПАРИТЕ, ПРИДОБИТИ ОТ ПРЕСТЪПНА ДЕЙНОСТ

Христо А. Десев

*Национален Военен Университет "В. Левски" гр. Велико Търново
Факултет "Артилерия ПВО и КИС" гр. Шумен*

APPROACHES TO ENHANCE EFFICIENCY IN THE FIGHT AGAINST THE USE OF MONEY, ACQUIRED FROM CRIMINAL ACTIVITY

Hristo A. Desev

Abstract: *The goals of the exhibition, fully related to the needs of bank management, dictate the setting up and solving of a complex research problem - limiting the access of illegal capital to the banking sector by improving the banking control and risk management system by means of an integrated preventive approach towards some more, risk sensitive to money laundering banking activities, operations and products.*

Keywords: *banking sector, bank management, criminal origin.*

Използването на средства, придобити от престъпна дейност, е получило широка гласност и общоприетото название: "изпиране на пари". Терминът *изпиране на пари*, макар и условен, следва да се счита за определен от правната теория и се използва в международното право, правото на Европейската общност. Условността му може да бъде ориентирана най-вече в две насоки.

От една страна, предмет на придобиване чрез или по повод на престъпление, респективно – предмет на посочените икономически операции са не само пари, но и всякакви други блага. Поради факта, че парите са универсално средство за разплащане, то обикновено на определена фаза от развитието на дейността по изпиране на облагите от престъпление те се обръщат в паричен еквивалент. Сложните операции с тях затрудняват в значителна степен разкриването на първоначалния им произход. Затова върху парите се поставя акцент още в наименованието на посочената престъпна дейност.

От друга страна, с условно значение се използва и думата изпиране. Целта е да се подчертае, че предмет на съответното поведение са блага с неясен "мръсен", престъпен произход, а самото поведение по своето съдържание е предназначено да ги "пречисти", да им даде вид, че са продукт от законна дейност.

Предпочитани видове бизнес за прикриване или пране на пари са:

➤ заведения, ресторанти и нощни клубове - фирмите, които обикновено се използват, за да стоят пред операциите за пране на пари (които осигуряват лицето

на операциите), включват барове, ресторанти и нощни клубове. Стоките и услугите на тези фирми имат сравнително високи цени и клиентите им са много различни в своите покупки. Продажбите обикновено са в брой и е всеизвестна трудността да се съпоставят разходите по приготвянето на храна, спиртни напитки и оборудване с приходите, които последните осигуряват;

➤ автомати за продажби на дребни стоки - операциите с автомати за продажби на дребни стоки имат изключително променлив и трудно измерим обем на касовите бележки и при големи операции разполагат със задоволителна гъвкавост относно различния транспорт, инсталиране и разходи по промоцията, осигуряващи прикритие за изтеглянето на изпраните средства;

➤ продажби на недвижими имоти - при продажбите на недвижими имоти често декларираната стойност е много по-ниска от действителната и за доплащане на разликата могат да се изперат и “мръсни пари”;

➤ Използване на куриери и професионални консултанти - кримерите отговарят за транспортирането на парите до обект, където те се превръщат в друга форма на валута. Тъй като куриерът няма очевидна връзка с истинския собственик на средствата, перачът на пари запазва своята анонимност. [2]

Професионалните консултанти като адвокати, счетоводители и брокери също може да послужат за пране на незаконни средства. Посредством схеми с инвестиции, кредити, парични трансфери и избягване на данъци тези професионалисти могат да манипулират финансовата, търговската и правната система, за да прикрият източника на и собствеността върху активите.

Терминологично изпирането на пари по смисъла на Закона за мерките срещу изпирането на пари е:

- преобразуването или прехвърлянето на имущество, придобито от престъпна дейност или от акт на участие в такава дейност, за да бъде укрит или прикрит незаконният произход на имуществото или за да се подпомогне лице, което участва в извършването на такова действие, с цел да избегне правните последици от своето деяние;

- укриването или прикриването на естеството, източника, местонахождението, разположението, движението или правата по отношение на имущество, придобито от престъпна дейност или от акт на участие в такава дейност;

- придобиването, владението, държането или използването на имущество със знание към момента на получаването, че е придобито от престъпна дейност или от акт на участие в такава дейност;

Изпирането на пари по своята същност е „последваща престъпна дейност“ за легализиране на придобитите по престъпен начин средства. Това е дейност, при която се прикрива съществуването на незаконния произход на доходи, получени при финансово престъпление. [1]

Основният негативен ефект върху националната икономика и върху финансовата система се състои в това, че прането на пари спомага за формирането и стимулира развитието на престъпните дейности – „сивата икономика“, корупцията, наркотрафика и контрабандата, тероризма и много други, тъй като престъпниците стават все по-богати и по-силни, използвайки като инвестиции изглеждащите вече чисти пари.

От друга страна, икономическото и политическо влияние на престъпните организации намалява ефективността на усилията на страните в преход към изграждане на демократични общества. Практически, прането на пари се явява престъпление, съпътстващо всяко друго, чрез което се генерират незаконни постъпления или имотни облаги.

Като потенциални негативни макроикономически последици от безпрепятственото пране на пари Международният валутен фонд цитира

- непредсказуемите промени в паричното търсене;
- значителните рискове за банковата надеждност;
- заразните ефекти върху законните финансови операции;
- увеличаващата се колебливост на международните капиталови потоци;
- валутни курсове, в следствие на непредсказуемите транснационални трансфери на активи.

Възможната последователност в изпирането на пари могат да се обобщат до следните няколко етапа:

1. Първоначална трансформация на придобитото чрез престъпна дейност имущество, с цел да се затрудни идентифицирането му. Това става чрез депозирание в банки

2. Извършването на икономически и финансови операции с вече въведените във финансовата система, за да се заличи престъпния им произход.

3. Инвестиране на средства в легална икономика. От този момент изпраните средства се представят като законно придобити и техният собственик свободно може да оперира с тях

Контрола върху изпирането на пари предполага предотвратяване и разкриване на действия от физически и юридически лица. Обект представляват сделките и операциите, свързани с преобразуване, укриване, придобиване на имущества и парични средства от незаконна дейност. В обхвата на контрола се включва събиране и разкриване на информация, идентифициране и проверка на клиенти, действителни собственици, финансови и търговски отношения по съмнителни сделки и операции. Съмнителните операции, сделки и клиенти, се класифицират по определени критерии:

- изпиране на пари чрез операции в брой;
- изпиране на пари чрез разплащателни сметки;
- изпиране на пари чрез сделки с ценни книжа;
- изпиране на пари чрез офшорни банки;
- изпиране на пари чрез обезпечени и необезпечени кредити;
- съмнителни клиенти.

Незаконното или противозаконното придобиване на пари и тероризмът са стари спътници на човешката цивилизация. Такива мащаби обаче, каквито те придобиха в края на 20-тия и особено в началото на 21-вия век, едва ли някога са имали; чрез своите глобални измерения те се превърнаха в централна тема на международната общност.[4]

На пръв поглед прането на „мръсни“ пари и тероризмът са два различни проблема, но фактически не е трудно да се открие солидна връзка между тях. Именно

поради това и борбата срещу тях в организационен, институционален и нормативен план е необходимо да е обща и единна.

До около 80-те години на 20-ти век придобиването на „мръсни“ пари и „прането“ им се свързваше с нелегалната търговия с оръжие и преди всичко на наркотици или главно – с мафията. Фактически обаче се оказа, че става дума за нелегален бизнес с огромни мащаби – 2-5% от световния БВП, който е над 30 трилиона долара.

Успоредно с прането на „мръсни“ пари с изключителни темпове и мащаби се разви и международният тероризъм, като датата 11.09.2001г. се превърна в отправна точка на противодействието му. От тази дата понятието международен тероризъм широко и трайно навлезе в международната и националната лексика, но в същото време се организира и предприе широко мащабна „война“ срещу него.

Понятието пране на „мръсни“ пари (Money Laundering) възниква в началото на 80-те години в САЩ, като израз на стремежа към легализиране на придобитите по незаконен, противозаконен начин пари, наричани „мръсни“ пари. Под пране на пари обикновено се разбира трансформирането в легалния бизнес на придобитите чрез престъпни сделки пари с цел да се прикрие техния нелегално-криминален произход.

„Мръсните“ пари и тероризмът са провокирани от „сътресения, сблъсъци и конфликти в социалния живот на човечеството“. Те са продукт на идеологически, политически, етически, религиозни, икономически и културни диференциации, а така също на морално-културна недостатъчност и нетърпимост към другия, различния от нас и нашата общност.

Общоприето е, че „мръсните“ пари и тероризмът са едни от най-уродливите явления на съвременната цивилизация, което определя и организираната борба срещу тях. В исторически аспект международно организираната и институционализирана борба срещу „мръсните“ пари предхожда тази срещу международния тероризъм и неговото финансиране, като след 11.09.2001г. те започнаха да се третират като обща тема.

Благоприятно прикритие за прането на „мръсните“ пари и за финансирането на тероризма, а следователно и основна пречка за ефективната борба срещу тях е търговската и банкова тайна – Underground Banking. Ето защо и главните насоки на борбата срещу тези явления се основава на ограничаване на търговската и банковата тайна и осъществяването на необходимата прозрачност по отношение на търговските сделки и на банковите операции и трансфери върху основата на принципа “Know Your Customer” - идентифицирай своя клиент или контрагент, независимо дали е физическо или юридическо лице. За физическите лица това ще рече легитимация – актуален адрес, а при съмнения да се потърси и допълнителна информация. Относно юридическите лица идентификацията им означава актуализирана регистрация, данъчен номер, Булстат и други идентификационни характеристики. Става дума по същество за ограничаване на анонимността и за разширяването на прозрачността в търговско-банковите сделки, операции и трансфери до степен, която не би благоприятствала прането на „мръсните“ пари и финансирането на тероризма.

Принципът “Know Your Customer” беше лансиран като основен принцип и стратегия в борбата срещу прането на пари и беше допълнен с принципа за ограни-

чаване на Underground Banking, благоприятстващ финансирането на нелегалния бизнес и на тероризма в частност.

На налагане и прилагане на посочените принципи бяха създадени и специални структури. На първо място създадената въз основа на Г-7+1 в Париж през 1989г. специална международна организация – Financial Action Task Force Money (FATF).

Във FATF членуват над 33 държави. Активна роля играят и Международния Валутен Фонд (МВФ) и Световната банка (СБ). Те изготвят съвместни проекти. Целта и задачата е държавите да се кооперират и под егидата на FATF да работят за ограничаване прането на „мръсни“ пари и финансирането на тероризма. На страните, които не се приобщават към борбата срещу тези злини бе изготвен „черен списък“, който ги заклеява като несътруднически в борбата. За практическото прилагане на основните принципи през 1990г. FATF разработи и публикува 40 препоръки, които впоследствие бяха допълнени и актуализирани. Именно тези 40 препоръки са основа, насоки, стандарти, и указания, които следва да се прилагат от държавите.[4]

След включването на FATF борбата срещу финансирането на международния тероризъм, при активното съдействие на МВФ и СБ, FATF допълнително разработи и публикува още 8 специални препоръки за борба срещу финансирането на международния тероризъм. Предмет на тези специални препоръки са преди всичко финансовите трансфери, които следва да се извършват само от официално регистрирани или концесионирани стопански и нестопански структури.

Активно участие в борбата срещу прането на „мръсни“ пари и финансирането на тероризма осъществява и Европейския съюз. В изпълнение на конвенциите и резолюциите на ООН и на Съвета за сигурност, ЕС издава свои директиви до страните-членки, в които се препоръчват указания за конкретното им прилагане и изпълнение. Освен това ЕС е колективен член на FATF и усърден проводник сред страните-членки на неговата стратегия и политика. В организираната борба, освен МВФ, СБ, ЕС, могат да се посочат и Създаденият през 2001г. в Базел нов международен банков стандарт относно „Задължението на банките при установяване идентичността на клиентите“.

Създаването на т.нар. Волфбургска банкова група между 12 банки с цел изработването и прилагането на общи стандарти срещу “Underground Banking” и за прилагането на принципа “Know Your Customer” а така също и за препоръките на FATF.

Най-ефективната мярка за недопускане прането на пари и финансирането на тероризъм е тяхната превенция. От своя страна световната банковата общност предприема поредица от инициативи, свързани с превенцията и ограничаване достъпа на незаконни капитали до финансовата системата, които намират приложение и в българската банкова практика.

Заплахата от използването на банковите институции за осъществяване на финансови престъпления може да се управлява чрез разпознаването, разбирането и свързването на риска от настъпването на тези събития с вида на клиентите и извършваните трансакции. Това се постига чрез строгото спазване на принципа “Познавай своя клиент” и прилагането на рисков базирани подход за управление на риска, съобразен със спецификата на дейността на банковите организации и типологията на обслужваните клиенти.

Предотвратяването на прането на пари в банковата система чрез интегрирано и комплексно приложение на целенасочени превантивни дейности, паралелно с основния банков бизнес, изразява най – общо същността на банковата политика срещу изпирането на пари, включваща разработване и внедряване на ефективна програма за противодействие, обезпечаваша следните основни дейности в банковите структури:

- прането на пари и тероризмът са две явления, които са свързани помежду си противозаконни действия, срещу които държавите по света обединяват своите усилия.

- решение на проблема се открива с конструктивен диалог и преговори, ако двете страни в конфликта – държавата и субекта на тероризма – съумеят да намерят общо взаимноизгодно решение;

- прилагане на съвременно международно и национално законодателство в областта на противодействието на прането на пари;

- въвеждане на стандарти, правила и процедури за контрол и управление на прането на пари;

- методично изготвяне на стандартизиран финансов профил спрямо всички подозрителни лица и организации, който да позволи разграничение на легитимните от нелегитимните им доходи и съпричастност към пране на пари;

- създаване, поддържане и развиване на бази данни за лица, организации, факти и обстоятелства, потенциално или реално свързани с прикрито финансиране на тероризъм или пране на пари;

- подбор и привличане на високо квалифициран кадрови ресурс и осигуряване на адекватна материално – техническа база;

- периодично организиране на обучения за банковите служители и обмен на практически опит по конкретни въпроси, с цел функционална специализация или при необходимост – преквалификация;

- осъществяване на адекватно сътрудничество за борба с прането на пари, тъй като ефективно противодействие е възможно само в условията на тясно взаимодействие с останалите участници в борбата с това престъпно явление.

Разширяването и засилването на борбата срещу прането на „мръсни“ пари и финансирането на тероризма обуславят значителна част от държавите в света да отделят все повече материални, човешки и финансови ресурси. Ако могат да се обхванат и изчислят разходите, които се отделят за борба срещу прането на „мръсни“ пари и финансирането на международния тероризъм, те сигурно ще се окажат впечатляващи.

Литература:

1. Закон за мерките срещу изпирането на пари (ЗМИП)
2. Madinger John, Money Laundering: a Guide for Criminal Investigators – 2nd ed., 2006 by Taylor&Francis Croup, LLC
3. Правилник за прилагане на ЗМИП
4. Стратегия за противодействие на изпирането на пари в Република България 2011-2015 година

K. Slavyanov,

CONTEMPORARY SYNTHETIC APERTURE RADAR SYSTEMS. MARKET SITUATION

Krasimir Slavyanov

Shumen, Bulgaria, 1 “Karel Shkorpil” str., “Artillery, Air Defense and Communication and Information Systems” Faculty

Abstract: *This report discusses the operation of the Synthetic Aperture Radar (SAR) systems. A brief analysis of the current market situation of these systems is made.*

Keywords: *imagine phased array, unmanned aerial vehicle, industry development.*

1. Introduction

The airspace monitoring system is part of the air defense system, which is developed to provide early detection and warning, defense and guarantees the sovereignty of the airspace of each independent state. The radar stations are mainly designed for radar coverage over the territory of the country and radar information is provided by the Operational Center for Air Sovereignty to carry out the NATO Air Policing task. These centers form a well-informed picture of the airborne situation that is transmitted to NATO Headquarters to form a Common Operational Picture in the NATO Integrated Air Defense System.

With the admission to NATO, radar positions from the State Air Force team are included in the NATO integrated Air Defense (NATINADS) [1]. This article discusses the principle of operation of SAR systems and major corporations that develop them.

Developed modern SAR technologies have found their specific application in radar systems based on existing space stations and special intelligence aircraft of the Air Force and solve a number of civil and military tasks related to the production of topographic maps on the Earth's surface and high resolution still images in real-time [2, 3].

The main problem with these automated systems is to achieve an optimal balance between the required computing resources and image quality. Due to the diversity of potentially observed ground objects of interest to air intelligence, the process of recognizing the depicted objects is carried out by photo-card readers. The development of systems for automatic recognition of SAR images is in the process of research [4, 5, 6].

2. Synthetic Aperture Radar principles.

A Synthetic Aperture Radar (SAR), or SAR, is a coherent mostly airborne or spaceborne sidelooking radar system (Side Looking Airborne Radar (SLAR)) which utilizes the flight path of the platform to simulate an extremely large antenna or aperture electronically, and that generates high-resolution remote sensing imagery. Over time, individual transmit/receive cycles or pulse repetition times (PRT's) are completed with the data from each cycle being stored electronically (fig. 1). The signal processing uses magnitude and phase of the received signals over successive pulses from elements of a

synthetic aperture. After a given number of cycles, the stored data is recombined (taking into account the Doppler effects inherent in the different transmitter to target geometry in each succeeding cycle) to create a high resolution image of the terrain being over flown (fig. 2).

Clutter spreads in the Doppler domain due to platform motion. As the radar moves past two point targets from B to A, the Doppler shift will vary approximately linearly with time, passing the zero frequency at boresight for zero squint. This Doppler shift approximates to a linear chirp, as the platform moves past the targets. Azimuth compression can be thought of as the compression of the Doppler signal produced during the integration length. The Doppler bandwidth consists of the frequencies produced, as a result of scatterers falling in the beamwidth of the radar, as the platform moves past the targets.

The SAR works similar of a phased array (phased array antenna), but contrary of a large number of the parallel antenna elements of a phased array, SAR uses one antenna in time-multiplex. The different geometric positions of the antenna elements are result of the moving platform.

The SAR-processor stores all the radar returned signals, as amplitudes and phases, for the time period T from position A to D. Now it is possible to reconstruct the signal which would have been obtained by an antenna of length $v \cdot T$, where v is the platform speed. As the line of sight direction changes along the radar platform trajectory, a synthetic aperture is produced by signal processing that has the effect of lengthening the antenna. Making T large makes the „synthetic aperture” large and hence a higher resolution can be achieved.

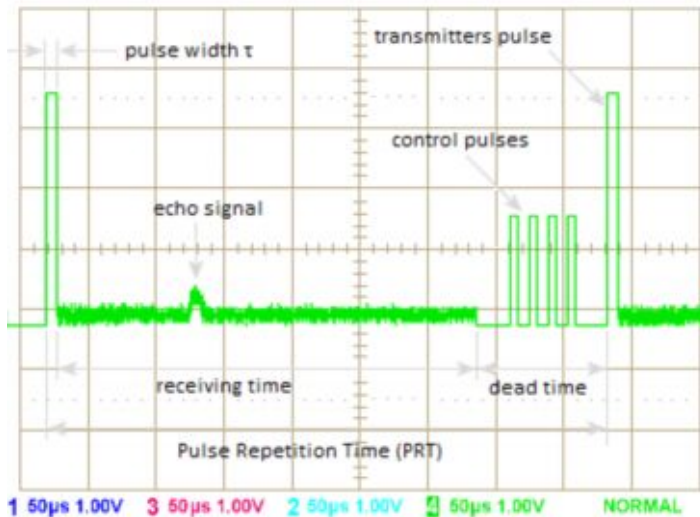


Figure 1. Radar pulse relationships



Figure 2. Radar silhouette of a ship, produced with the ISAR-Processor of the radar set of type Ocean Master

As a target (like a ship) first enters the radar beam, the backscattered echoes from each transmitted pulse begin to be recorded. As the platform continues to move forward, all echoes from the target for each pulse are recorded during the entire time that the target is within the beam. The point at which the target leaves the view of the radar beam some time later, determines the length of the simulated or synthesized antenna. The synthesized expanding beamwidth, combined with the increased time a target is within the beam as ground range increases, balance each other, such that the resolution remains constant across the entire swath (fig. 3).

The achievable azimuth resolution of a SAR is approximately equal to one-half the length of the actual (real) antenna and does not depend on platform altitude (distance).

The requirements are: stable, full-coherent transmitter; an efficient and powerful SAR-processor; exactly knowledge of the flight path and the velocity of the platform.

Using such a technique, radar designers are able to achieve resolutions which would require real aperture antennas so large as to be impractical with arrays ranging in size up to 10 m.

A Synthetic Aperture Radar was used on board of a Space Shuttle during the Shuttle Radar Topography Mission (SRTM).

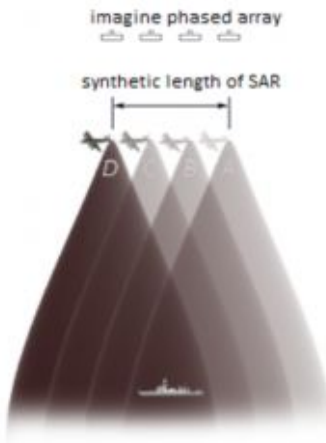


Figure 3. The synthesized expanding beamwidth

SAR radar is partnered by what is termed Inverse SAR (abbreviated to ISAR) technology which in the broadest terms, utilizes the movement of the target rather than the emitter to create the synthetic aperture. ISAR radars have a significant role aboard maritime patrol aircraft to provide them with radar image of sufficient quality to allow it to be used for target recognition purposes (fig. 4) [7].

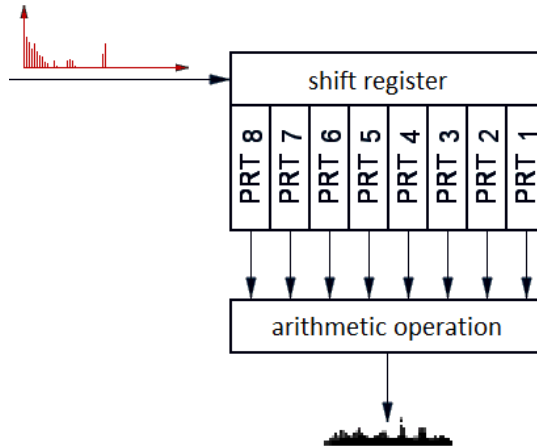


Figure 4. Principle of SAR- operation

Slant-range distortion.

The slant-range distortion occurs because the radar is measuring the distance to features in slant-range rather than the true horizontal distance along the ground. This results in a varying image scale, moving from near to far range.

Foreshortening occurs when the radar beam reaches the base of a tall feature tilted towards the radar (e.g. a mountain) before it reaches the top. Because the radar measures distance in slant-range, the slope (from point a to point b) will appear compressed and the length of the slope will be represented incorrectly (a' to b') at the image plane (fig. 5).



Figure 5. Foreshortening

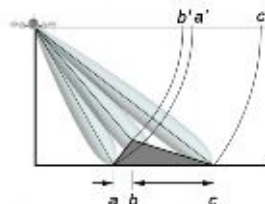


Figure 6. Layover



Figure 7. Shadowing

Layover occurs when the radar beam reaches the top of a tall feature (b) before it reaches the base (a). The return signal from the top of the feature will be received before the signal from the bottom. As a result, the top of the feature is displaced towards the

radar from its true position on the ground, and „lays over” the base of the feature (b' to a') (fig. 6) [7].

The shadowing effect increases with greater incident angle θ , just as our shadows lengthen as the sun sets (fig. 7).

3. Overview of the global SAR market.

Market research analysts [8] predict that the global synthetic aperture radar (SAR) market will grow steadily during the next four years at a CAGR of over 5% by 2021. This market research analysis identifies the increasing investments in surveillance and attack unmanned aerial vehicle (UAVs) as one of the primary growth factors for this market. Owing to technological advancements and the significance of UAVs in security countermeasure operations, there is an increasing integration of UAVs with electronics such as the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4IRS) systems that support military operations. Additionally, with advancements in tactical control system software, the ground station controllers can also seamlessly receive or control information from UAVs. Furthermore, the software also provides the operator with necessary tools for planning, tasking, and executing missions, computer-related communications, data processing, and data dissemination.

One of the latest trends that will gain traction in the SAR market in the coming years is the rising preference for the integrated C4ISR ecosystem. To address issues such as the requirement of separate systems and displays for collecting and analyzing information, defense agencies are inclined towards the adoption of the enterprise integration approach which advocates the integration of secure and interoperable C4ISR networks and systems. Moreover, to cater to the monolithic operational requirements of the combat forces, the military organizations will also shift from the vast acquisition approach to agile and incremental procurement strategies.

Competitive landscape and key vendors.

Owing to the presence of several players, the SAR market appears to be fragmented. The growth of the players depends on factors such as market conditions, government support, and industry development. To survive and succeed in such an intensely competitive market, it is imperative for players to distinguish their product and service offerings through clear and unique value propositions.

The leading vendors in the market are: Airbus Defense and Space, Israel Aerospace Industries (IAI), Lockheed Martin, Northrop Grumman, Thales.

The other prominent vendors in the market include MDA Information Systems, SSTL, Sandia National Laboratories, and Raytheon.

Segmentation by product type and analysis of the SAR market can be: Space-based SAR and Airborne SAR.

During 2016, the space-based SAR segment accounted for the major shares of the SAR market. These radars employ microwave illuminators or operating frequencies and this keeps the radar imaging unaffected even in adverse weather conditions. These satellite-based SARs can acquire and broadcast images of various strategic areas during extreme weather conditions or complete darkness and are the only available resource to several defense agencies [8].

Geographical segmentation and analysis of the SAR market: Americas; Asia-Pacific; Europe, the Middle East and Africa.

By the market studies Americas will be the major revenue contributor to the market by 2021. The collaboration of the National Aeronautics and Space Administration (NASA) with the US Department of Defense (DoD) that results in an increase in R&D-related activities in space-based SAR satellites will be a major factor fueling the growth of the SAR market in this region.

5. Conclusion.

In SAR technology, the process of synthesizing the aperture is determined by the a priori known trajectory parameters of the carrier object of the radar system. Automated data processing systems receive the necessary output data directly from the current flight data control systems, and the task is to determine the start and end time of the registration of the echo signals and to perform the procedures related to the restoration of the final photo-image.

Growing development of satellites by various countries may influence the demand for synthetic aperture radar. The upcoming industry research reports for the global synthetic aperture radar market categorizes the key drivers, major trends, as well as the restraints that the defense sector currently experiences. It is important the key insights into the quickly changing competitive scenario to give clients an accurate picture of the approaching events within the aerospace and defense industry. The deep-dive market assessments into the sectors such as aerospace components and aerospace manufacturing are vital for any future state investments in air defense radar systems.

References

1. NATO Joint Air & Space Operations Doctrine AJP 3.3, 2002.
2. Jakowats,Jr., Wahl,DE., Eichel,P.H., Ghiglia,D.C., Thompson,P.A. Spotlight-mode synthetic aperture radar: a signal processing approach.. Kluwer Academic Publishers, Norwell, MA, 1996.
3. Čučej Ž., Gleich D., 17th International Conference on Systems, Signals and Image Processing IWSSIP, 2010.
4. Kaplan L.M., Improved SAR target detection via extended fractal features, IEEE Transactions on Aerospace and Electronic Systems (Volume: 37, Issue: 2, Apr 2001), 436 – 451.
5. Xiong W., Cao L., Automatic Target Recognition Based on Rough Set-Support Vector Machine in SAR Images, Computational Sciences and Optimization, International Conference CSO 2009, April 2009.
6. Han Z., Su Z., Han P., Wu R., Efficient subspace-based recognition method for SAR targets with similar structure, Radar Conference, IET International April 2009
7. <http://www.radartutorial.eu>, 23.05.2017.
8. D- TechNavio (Infiniti Research Ltd.), Global Synthetic Aperture Radar (SAR) Market 2017-2021, June 7, 2017.

Д. К. Марков.

ПОРАЗЯВАНЕ НА ЦЕЛИ ОТ АРТИЛЕРИЙСКИ ФОРМИРОВАНИЯ, ВЪОРЪЖЕНИ СЪС 122-ММ СГ 2С-1 „ГВОЗДИКА“ В БЛИЗОСТ ДО ЗОНАТА ЗА КООРДИНИРАНЕ НА ВЪЗДУШНОТО ПРОСТРАНСТВО

Дилян К. Марков

THE ATTACK OF TARGETS FROM ARTILLERY FORMATIONS, ARMED WITH 122 MM SELF-PROPELLED HOWITZER 2С-1 "GVOZDIKA" IN THE PROXIMITY TO THE ZONE OF THE AIRSPACE COORDINATION AREA

Dilyan K. Markov

Abstract: The article focuses on the problems of the attack of targets from 122 mm Self-Propelled Howitzer 2С-1 "Gvozdika" in the proximity to the zone of the airspace coordination area. The cases where the projectile trajectory is lower than the minimum altitude and when it is above the maximum altitude of the airplanes.

Keywords: Joint Fire Support, Fire Support Coordinating Measures, Airspace Coordination Areas.

I. Въведение

Огневата поддръжка е една от основните бойни функции и представлява прилагане на огнева мощ, чрез огън на средствата от закрити огневи позиции на артилерийските формирования, средствата за електронна война, средствата за огнева поддръжка на военноморския и военновъздушния компонент, координирани с маневрените формирования, с цел унищожаване, неутрализиране или подавяне на противника.

Целта на огневата поддръжка е да се нанесат загуби на противника и се подкрепят неговите възможности да води бойни действия, да се подпомогне удържането от маневрените формирования на райони, както и да се даде свобода на командира при изпълнение на неговия замисъл за провеждане на операцията.

Артилерията е предназначена да действа съвместно и непрекъснато с маневрените формирования, да бъде в основата на огневата система на всяко формирование, бързо да се развърща и внезапно да поразява противника в тясно взаимодействие с авиацията и другите родове войски и огневи средства.[1]

За да изпълни в пълен обем своите задачи и едновременно с това да осигури безопасност на нашите войски от въздействието на собствения огън от артилерията се изисква да координира своите действия с другите средства за огнева поддръжка. За тази цел участието на средствата за огнева поддръжка е необходимо да интегрират огъня си във времето и пространството в зони за подпомагане на дейностите по огневата поддръжка с цел да се осигури оптимално използване на собствения огневи потенциал и да се гарантира свобода на действието на силите.[7]

Това е непрекъснат процес на взаимодействие на действията на формированията от сухопътния, военновъздушния и военноморския компонент на всички нива на

командване и управление, което се извършва от координаторите по огнева поддръжка и офицерите за свръзка.

От практическа гледна точка съвместните действия на средствата за огнева поддръжка и в частност артилерията и авиацията са много важни за изхода на всяка една операция. Ето защо, когато се планират бойни действия трябва да се координират дейностите по прехвърляне на войски, поразяващите огневи налети от авиацията, коридорите за прелитане на летателните апарати, огъня на планираните от по-високите нива бойни хеликоптери, защитните мерки за ПВО, огъня на всички огневи средства и др., за да се гарантира безопасността на собствените войски.[2]

Това се постига чрез мерките за координиране на огневата поддръжка. Тяхната роля е да улеснят задачите на средствата за огнева поддръжка, при нанасяне на удари от различни средства за поразяване, както и сигурност на собствените сили.

Една от най-трудните за планиране и координиране мярка е зоната за координиране на въздушното пространство (ЗКВП - Airspace Coordination Areas (ACA)).[6] Необходимостта от избягване на взаимно поразяване от собствени средства и въвеждането на въоръжение на все по-скорострелни огневи системи изисква внимателен подход при използване на въздушното пространство. Опитът от бойните действия и ученията показва, че тази зона ограничава огъня на артилерията в близост до тези зони.

Ето защо в настоящия доклад се разглежда проблема при поразяване на цели от артилерийски формирования, въоръжени със 122 mm СГ 2С-1 „Гвоздика“ в близост до зоната за координиране на въздушното пространство

II. Поразяване на цели в близост до зоната за координиране на въздушното пространство

Зоната за координиране на въздушното пространство е една от основните ограничителни мерки. Тя е триизмерна зона от въздушно пространство, която се установява с цел да се предпазят собствените летателни апарати от огъня на огневите средства на сухопътния и военоморския компонент.[7]

Анализирайки внимателно границите на тази триизмерна зона се забелязват два варианта за използване на нарезната артилерия при поразяване на цели в близост до нея:

- височината на траекторията на снарядите да е по-малка от минималната височина на полета на летателния апарат;
- височината на траекторията на снарядите да е по-голяма от максималната височина на полета на летателния апарат.

1. Стрелба по цели с височина на траекторията на снарядите по-малка от минималната височина на полета на летателния апарат

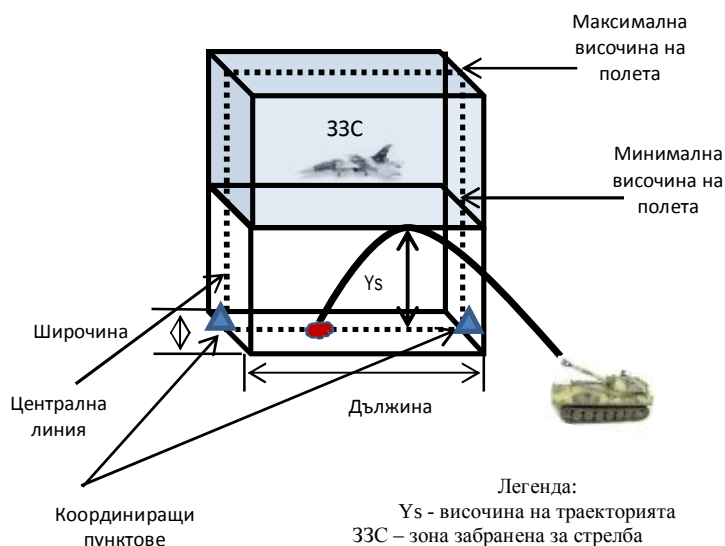
В този случай единствената мярка за контрол ще бъде височината на траекторията (Ys), според която ще се ограничи използването на артилерийската система (фиг.1). Нейната стойност се взема от таблиците за стрелба за системата и зависи от съответния заряд и взривател.

Като се използва височината на траекторията за система 122 mm СГ 2С-1 „Гвоздика“, която е посочена в таблиците за стрелба № 0141[4] и се въведат данни за

снаряда, взривателя и минималната височина на полета на летателните апарати в ЗКВП, както следва:

- снаряд ОФ - 462;
- взривател - РГМ – 2;
- минималната височина на полета (минимална височина на траекторията на снаряда) - 500 m,

ще се получат резултати в таблица № 1, които могат да се използват за анализ на възможностите на артилерийската система за стрелба по цели с височина на траекторията на снарядите по-малка от минималната височина на полета на летателния апарат.



Фиг. 1. Височината на траекторията на снарядите е по-малка от минималната височина на полета на летателния апарат

Таблица № 1

Максимална далекобойност на 122 мм СГ 2С-1 „Гвоздика“ при стрелба с височина на траекторията по-малка от минималната височина на полета на летателни апарати за ЗКВП

Заряд	Минимална височина на траекторията, m	Далекобойност, m	% от макс. далекобойност	Максимална далекобойност
Пълен	500	7900	52%	15260
	750	9100	60%	
Намален	500	6900	53%	12874
	750	8000	62%	
Първи	500	6400	56%	11521
	750	7500	65%	
Втори	500	5800	57%	10043
	750	6950	69%	
Трети	500	5400	64%	8355
	750	6400	76%	
Четвърти	500	4700	74%	6356
	750	5420	85%	

Вследствие на получените резултати от таблица № 1 могат да се направят следните изводи за стрелба със 122 мм СГ 2С-1 „Гвоздика“ по цели с височина на траекторията на снарядите по-малка от минималната височина на полета на летателния апарат и действаща по размери и време ЗКВП:

- при 500 m минимална височина на полета на летателни апарати максималната далекобойност на системата се намалява приблизително с 1/2 (от 15260 до 7900);
- при 750 m минимална височина на полета на летателни апарати максималната далекобойност на системата се намалява приблизително с 2/3 (от 15260 до 9100).

2. Стрелба по цели с височина на траекторията на снарядите по-голяма от максималната височина на полета на летателния апарат

В този случай отчитането на височината на траекторията няма да става по максималната височина на полета на летателния апарат, защото част от траекторията на снаряда ще премине през ЗКВП и ще се получат зони с възможност за поразяване на собствената авиация (фиг. 2).

За безопасност на летателните апарати стрелбата на нарезната артилерия изцяло трябва да прехвърля ЗКВП (фиг. 3).

За да се определи дали траекторията на снарядите преминава над ЗКВП, трябва да се използват графиците на траекториите с кривите за времелетенето на снаряда за съответната система, взривател и заряд.[5]

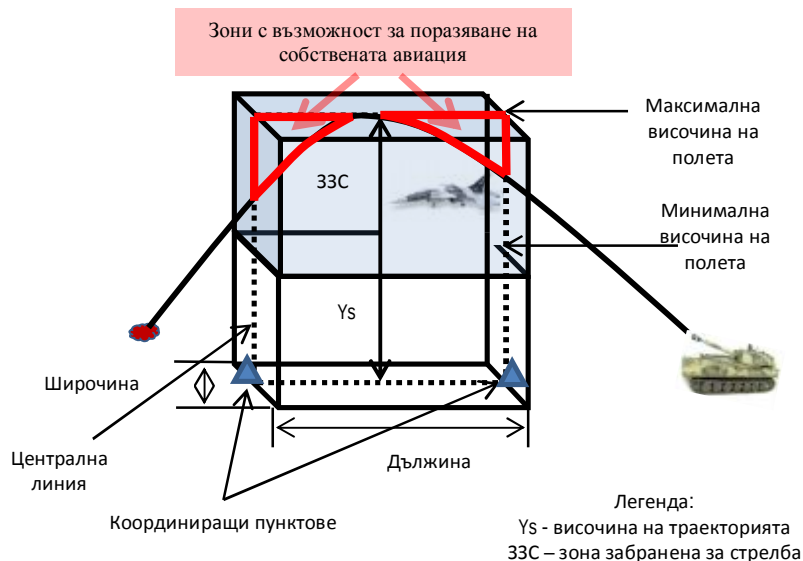
Поради наличие на графиците на траекториите с кривите за времелетенето на снарядите за артилерийските системи на въоръжение в Българската армия само за планинска местност, то анализа ще бъде в тази насока.

Графичните таблици за стрелба са разделени от ъгъла на възвишение:

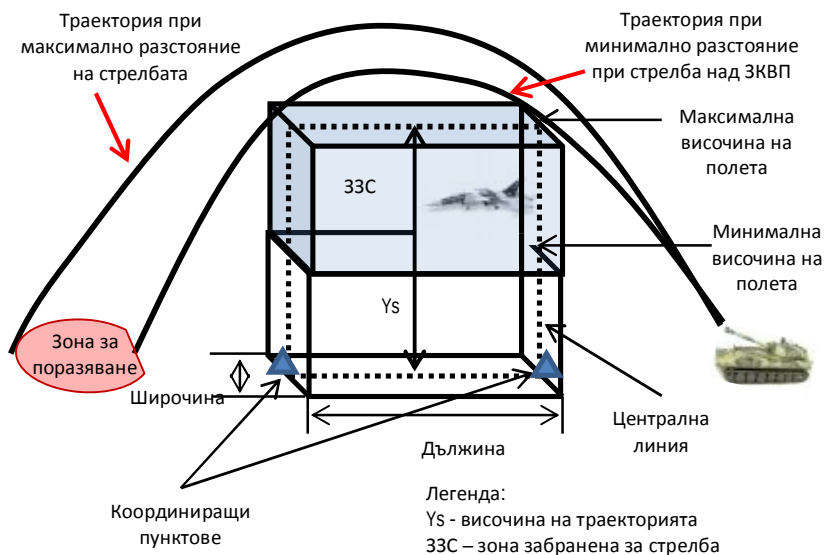
- с ъгли на възвишение до 45°;

- с ъгли на възвишение над 45° .

За това примери за възможност за поразяване на цели от нарезната артилерия, когато траекторията на стрелбата прехвърля ЗКВП ще бъдат изложени за двата случая. Важно е да се отбележи, че височината на траекторията ще зависи и от отдалечението на ЗКВП от оръдието (огневата позиция на формиранието).



Фиг. 2. Височината на траекторията на снарядите е по-голяма от максималната височина на полета на летателния апарат, но в непосредствена близост до нея



Фиг. 3. Височината на траекторията на снарядите е по-голяма от максималната височина на полета на летателния апарат и преминава над ЗКВП

За да се определи каква е възможността за стрелба по цели с височина на траекторията на снарядите по-голяма от максималната височина на полета на летателния апарат при ъгли на възвишение до 45° , ще се използват следните данни:

- система 122-мм СГ 2С-1 „Гвоздика“;
- таблица за стрелба - ТС ПМ № 141Г;
- снаряд ОФ - 462;
- взривател - РГМ – 2;
- разстояния от оръдието до ЗКВП – 1000, 3000, 5000 m;
- максимални височини на полета – 500, 7500, 1000 m.

Получените резултати в таблици № 2, 3 и 4, могат да се използват за анализ за възможностите на артилерийската система.

Таблица № 2

Възможности на 122-мм СГ 2С-1 „Гвоздика“ за стрелба над ЗКВП при 500 m максимална височина на полета на летателни апарати
(ъгли на възвишение до 45°)

Разстояние от оръдието до ЗКВП	Заряд	Мерник мин.	Далеко-Бойност, m	Макс. далеко-бойност, m	Зона за поразяване фиг.3
1000	Пълен	444	14100	16600	2500
	Намален	451	11600	13800	2200
	Първи	466	10400	12200	1800
	Втори	493	9200	10500	1300
	Трети	500	7650	8800	1150
	Четвърти	534	6000	6500	500
3000	Пълен	195	9150	16600	7450
	Намален	211	7200	13800	6600
	Първи	226	6600 ЗКВП до 1 km	12200	5600
	Втори	258	6000 ЗКВП до 800 m	10500	4500
	Трети	Траекторията на снаряда или част от нея преминава през ЗКВП			
	Четвърти				
5000	Пълен	168	8150	16600	8450
	Намален	211	7200	13800	6600
	Първи - Четвърти	Траекторията на снаряда или част от нея преминава през ЗКВП			

От анализът на данните от таблица № 2 могат да се направят следните изводи за стрелба със 122-мм СГ 2С-1 „Гвоздика“ по цели и действаща по размери и време ЗКВП при 500 m максимална височина на полета:

- разположението на огневите позиции на близки разстояния до ЗКВП е неефективно за стрелба при ъгли на възвишение до 45°, поради малката зона за поразяване на целите;
- разположението на огневите позиции в район около 5 км от ЗКВП ще изисква използване само на заряди „пълен“ или „намален“, което ще ограничи използването на системите по режима на огъня;
- за най-ефективно поразяване на цели е необходимо използване на заряди от „пълен“ до „втори“ и разположение на огневите позиции в район около 3 км от ЗКВП.

Таблица № 3

Възможности на 122 мм СГ 2С-1 „Гвоздика“ за стрелба над ЗКВП при 750 m максимална височина на полета на летателни апарати
(ъгли на възвишение до 45°)

Разстояние от оръдието до ЗКВП	Заряд	Мерник мин.	Далекобойност, m	Макс. далекобойност, m	Зона за поразяване фиг.3
1000	Пълен	580	15650	16600	950
	Намален	590	13100	13750	650
	Първи	600	11700	12100	400
	Втори	610	10100	10500	400
	Трети	628	8400	8600	200
	Четвърти	650	6400	6500	100
3000	Пълен	249	10400	16600	6200
	Намален	269	8600	13750	5150
	Първи	270	7400 ЗКВП до 2 km	12100	4700
	Втори	333	7200 ЗКВП до 1,5 km	10500	3300
	Трети	373	6400 ЗКВП до 1 km	8600	2200
	Четвърти	Траекторията на снаряда или част от нея преминава през ЗКВП			
5000	Пълен	191	8950 ЗКВП до 1 km	16600	7650
	Намален - Четвърти	Траекторията на снаряда или част от нея преминава през ЗКВП			

От анализът на данните от таблица № 3 могат да се направят следните изводи за стрелба със 122 мм СГ 2С-1 „Гвоздика“ по цели и действаща по размери и време ЗКВП при 750 m максимална височина на полета:

- разположението на огневите позиции на близки разстояния до ЗКВП е неефективно за стрелба при ъгли на възвишение до 45°, поради малката зона за поразяване на целите;
- разположението на огневите позиции в район около 5 км от ЗКВП ще ограничи използването на системите по режима на огъня, поради използването само на заряд „пълен“;
- за най-ефективно поразяване на цели е необходимо използване на заряди от „пълен“ до „втори“ и разположение на огневите позиции в район около 3 км от ЗКВП.

Таблица № 4

Възможности на 122 мм СГ 2С-1 „Гвоздика“ за стрелба над ЗКВП при 1000 m
максимална височина на полета на летателни апарати
(ъгли на възвишение до 45°)

Разстояние от оръдието до ЗКВП	Заряд	Мерник мин.	Далекобойност, m	Макс. далекобойност, m	Зона за поразяване фиг.3
1000	Пълен - Четвърти	Траекторията на снаряда или част от нея преминава през ЗКВП			
3000	Пълен	348	12400	16600	4200
	Намален	357	10200	13750	3550
	Първи	390	9300	12100	2800
	Втори	421	8200	10500	2300
	Трети	459	7300 ЗКВП до 1,2 km	8600	1300
	Четвърти	Траекторията на снаряда или част от нея преминава през ЗКВП			
5000	Пълен - Четвърти	Траекторията на снаряда или част от нея преминава през ЗКВП			

Данните от таблица № 4 показват, че при стрелба със 122-мм СГ 2С-1 „Гвоздика“ и действаща по размери и време ЗКВП при 1000 m максимална височина на полета могат да се направят следните изводи:

- разположението на огневите позиции на близки разстояния и такива по-големи от 3 км от ЗКВП е невъзможно поради това че траекториите на снарядите или част от тях ще преминава през ЗКВП;

- за най-ефективно поразяване на цели е необходимо използване на заряди от „пълен“ до „втори“ и разположение на огневите позиции в район около 3 км от ЗКВП.

За да се определи каква е възможността за стрелба по цели с височина на траекторията на снарядите по-голяма от максималната височина на полета на летателния апарат при ъгли на възвишение над 45°, е необходимо да се използват графичите на траекториите с кривите за времетраенето на снарядите от таблица за стрелба - ТС ПМ № 141Г. За тази цел ще се използват и следните данни:

- снаряд ОФ - 462;
- взривател - РГМ - 2;
- разстояния от оръдието до ЗКВП - 1000, 3000, 5000 m;
- максимални височини на полета - 500, 7500, 1000 m.

Получените резултати в таблица № 5, могат да се използват за анализ за възможностите на артилерийската система при мортирна стрелба.

Таблица № 5

Възможности на 122 мм СГ 2С-1 „Гвоздика“ за стрелба над ЗКВП
(ъгли на възвишение над 45°)

Макс. височина на полета на летателни апарати, m	Заряд	Мин. разстояние от оръдието до ЗКВП, m	Макс. далекост, m	Мин. далекост, m
500	Пълен	500	16600	10950
	Намален	500	13750	8950
	Първи	500	12100	7900
	Втори	500	10500	6800
	Трети	600	8600	5450
750	Четвърти	600	6500	4100
	Пълен	750	16600	10950
	Намален	750	13750	8950
	Първи	750	12100	7900
	Втори	750	10500	6800
1000	Трети	800	8600	5450
	Четвърти	900	6500	4100
	Пълен	1000	16600	10950
	Намален	1050	13750	8950
	Първи	1050	12100	7900
	Втори	1100	10500	6800
	Трети	1200	8600	5450
	Четвърти	1300	6500	4100

Данните от таблица № 5 показват, че при стрелба със 122-мм СГ 2С-1 „Гвоздика“ и действаща по размери и време ЗКВП могат да се направят следните изводи:

- разположението на огневите позиции в непосредствена близост (до 1300 m) до ЗКВП е невъзможно поради това че траекторията на снарядите или част от тях ще преминават през ЗКВП;

- за най-ефективно поразяване на цели е необходимо използване на мортирна стрелба на всички заряди и разположение на огневите позиции в район на разстояние около 1,5 km и по - голямо от ЗКВП.

- при мортирна стрелба максималната далекост на системата ще зависи от разположението на ОП от ЗКВП, но не и от височината на полета на летателните апарати.

III. Заключение

От разгледания проблем за възможността за използване на артилерийски формирования, въоръжени със 122-мм СГ 2С-1 „Гвоздика“ за поразяване на цели в близост до зоната за координиране на въздушното пространство трябва да се отчитат следните особености:

- при стрелба по цели с височина на траекторията на снарядите по-малка от минималната височина на полета на летателния апарат и действаща по размери и

време ЗКВП максималната далекобойност на системата се намалява приблизително с 1/2 (2/3) при 500 (750) m минимална височина на полета на летателни апарати;

- при стрелба по цели с височина на траекторията на снарядите по-голяма от максималната височина на полета на летателния апарат за най-ефективно поразяване на цели при ъгли на възвишение до 45° е необходимо използване на заряди от „пълен“ до „втори“ и разположение на огневите позиции в район около 3 км от ЗКВП;

- при стрелба по цели с височина на траекторията на снарядите по-голяма от максималната височина на полета на летателния апарат за най-ефективно поразяване на цели при ъгли на възвишение над 45° е необходимо разположение на огневите позиции в район на разстояние около 1,5 km и по - голямо от ЗКВП.

Литература:

1. Атанасов, А. Бойно използване на полевата артилерия в операцията и боя. София. 2016 г.
2. Марков Д., А.Атанасов. Условия за единно управление, чрез интегриране на системите за огнева поддръжка при участие в многонационални операции. Годишник на ВА „Г.С.Раковски“, 2016 г. Издателство: ВА „Г.С.Раковски“, 2016 г.
3. Речник на термините и дефинициите, използвани в НАТО (ААР 6), (на английски и български език). 2014г.
4. Таблици за стрелба със 122 мм самоходна гаубица 2С-1 (ТС № 0141). Военно издателство. София 1986г.
5. Таблици за стрелба за планинска местност със 122 мм самоходна гаубица 2С-1 (ТС № 141Г). Военно издателство. София 1991г.
6. Тактическа доктрина на полевата артилерия. Военно издателство 2005г.
7. Joint Publication 3-09. Joint Fire Support. 12 December 2014
http://www.dtic.mil/doctrine/new_pubs/jp3_09.pdf

Д. К. Марков,

ПОРАЗЯВАНЕ НА ЦЕЛИ ПРИ СЪВМЕСТНА ОГНЕВА ПОДДРЪЖКА В ЗОНАТА ЗА КООРДИНИРАНЕ НА ВЪЗДУШНОТО ПРОСТРАНСТВО

Дилиан К. Марков

THE ATTACK OF TARGETS FROM JOINT FIRE SUPPORT IN THE AIRSPACE COORDINATION AREA

Dilyan K. Markov

Abstract: The article focuses on establishing the airspace coordination area, types of ACA and use it a restrictive measure of Joint Fire Support.

Keywords: Joint Fire Support, Fire Support Coordinating Measures, Airspace Coordination Areas.

I. Въведение

Успехът в съвременните операции се постига чрез съвместните усилия на компонентите от трите вида въоръжени сили и родовете войски, обхванати в единна командна структура. Необходимите способности за операцията се изграждат в процеса на генериране на силите в зависимост от националните способности на държавите членки на НАТО и междусъюзническите споразумения за изграждане на специфични способности.

Ефективността на артилерийския огън се определя основно от неговата координация и интегрираност с огъня на другите средства за поразяване за постигане на необходимия резултат. По този начин един от основните проблеми на развитие на модерна артилерия е да осигури на маневрените формирования широки възможности в района на бойните действия. Поради това подготовката и участието на артилерийските формирования от Българската армия както в национални, така и в многонационални операции изведе на дневен ред необходимостта от изпълнение на задачи в системата на съвместна огнева поддръжка.

Съвместната огнева поддръжка изисква синхронизирано и координирано взаимодействие на всички елементи, задълбочено и непрекъснато планиране, агресивна координация и енергично изпълнение. Тя включва целеопределяне и целеразпределение, командване и контрол (C2) и системи за поразяване, които трябва да функционират колективно, за да се осигури ефективна огнева поддръжка, където и когато командирът изисква.

II. Мерки за координиране на огневата поддръжка

В рамките на своите зони за отговорност командирите на сухопътния и военноморския компонент е необходимо да назначат разрешителни и ограничителни мерки за координиране на огневата поддръжка (МКОП), за да улеснят бързата процедура по поразяването на целите и същевременно да осигурят безопасността

на собствените сили. МКОП улесняват огневата поддръжка и включват: линии за координиране на огъня (Coordinated Fire Lines - CFLs), линии за координиране на бойното поле (Battlefield Coordination Lines - BCLs), линии за координиране на огневата поддръжка (Fire Support Coordinated Lines – FSCLs), зони свободни за стрелба (Free-Fire Areas - FFAs) и “kill boxes”. Ограничителните мерки гарантират безопасността на собствените сили и включват зони за координиране на въздушното пространство (Airspace Coordination Areas - ACAs), линии за ограничаване на огъня (Restrictive Fire Lines - RFLs), зони за ограничаване на огъня (Restrictive Fire Areas - RFAs) и зони забранени за стрелба (No Fire Areas - NFAs).[5]

Използването на мерките за координиране на огневата поддръжка (Fire Support Coordinating Measures - FSCM) зависи от тактическата ситуация. Те се предлагат от координатора на огневата поддръжка и се утвърждават от командира. МКОП се изобразяват графично с черни линии. Всички мерки се обозначават с напис с цялото наименование или със съкращения, показващ кой щаб ги е установил и до кога са валидни. Мерките за координиране на огневата поддръжка могат да влезнат в сила незабавно, в планирано време или при необходимост от извикване.[2]

III. Използване на зоната за координиране на въздушното пространство в съвместни операции

Една от основните ограничителни мерки е зоната за координиране на въздушното пространство (ЗКВП). Тя е триизмерна зона от въздушно пространство, която се установява с цел да се предпазят собствените летателни апарати от огъня на огневите средства на сухопътния и военноморския компонент.

Съществуват два вида: формални и неформални.[3]

Първият вид области изискват детайлно планиране. Вертикалните и хоризонталните граници на тези зони позволяват свобода на действие за средствата за огнева поддръжка на сухопътния, военноморския и военновъздушния компонент за поразяване на най-голям брой цели. Органът за контрол на въздушното пространство установява ЗКВП по искане на съответния командир на сухопътния компонент (на ниво бригада и по-високо). Те се могат да бъдат определени за действие след определено време или незабавно. При планиране на ЗКВП се посочва времето, за което те трябва да бъдат ефективни (Пример: 191830Z - 191835Z). (фиг. 1.)

По искане на подчинените формирования, командирът на сухопътния компонент може да поиска да се определят неформални ЗКВП. Те могат да се назначат на батальонно или по-високо ниво. Средствата за огнева поддръжка на сухопътния, военноморския и военновъздушния компонент могат да бъдат разделени по време или по разстояние (по хоризонтала, по вертикала, или чрез комбинация от двете). Разделянето по разстояние изисква по-подробна координация между военновъздушния компонент и другите средства за огнева поддръжка, но може да бъде с много ограничения за маршрутите на самолетите.

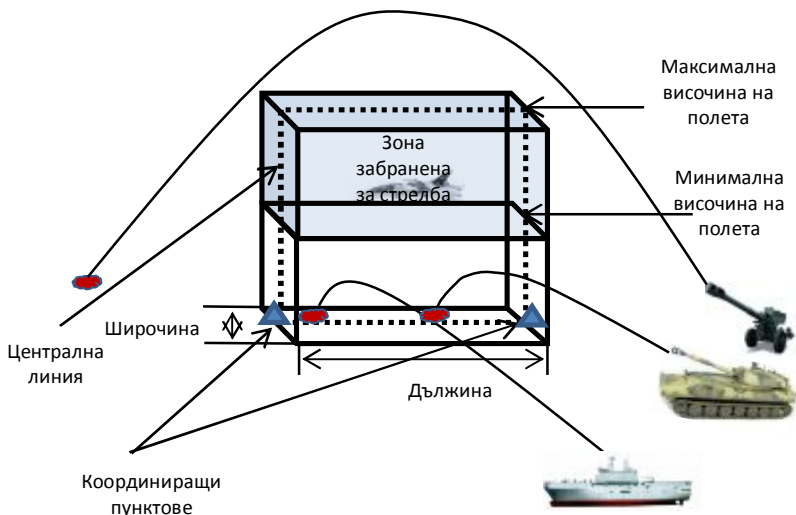
В центъра за координиране на огневата поддръжка трябва да се избере техниката на разделяне, която изисква координацията да се извършва без да има неблагоприятно въздействие върху способността на самолетните екипажи безопасно да изпълнят мисията.

ЗКВП може да се обозначават по различен начин:

- с кодово име - ZUMA;
- съгласно номера и датата - AC39MR (ACA 3, 9th Mar);

- по номера на целите - LB 4512;
- по координатната мрежа.

Кодовото име е най-лесният начин за използване, особено за предварително планирани ЗКВП, но незабавно определените ЗКВП могат да бъдат и без кодово име. ЗКВП по номер на целта или по координатната мрежа, улесняват незабавното разпространение на зоните до формированията.



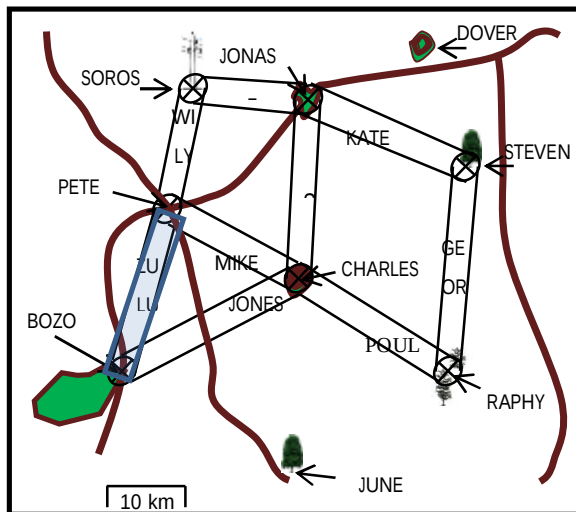
Фиг. 1. Зона за координиране на въздушното пространство

За определяне на ЗКВП се назначават координиращи пунктове (coordinating points) [1], които са лесно разпознаваеми обекти на земната повърхност, на които се дава име или номер и се използва като помощно средство за навигация или контрол на кораби, лодки или самолети.[4] По време на планирането, те се избират и назовават в цялата област. Когато е необходимо, тези координиращи пунктове се определят като изходни точки, точки за контрол при влитане и др. За координиращи пунктове могат да се използват и обекти с кодови имена. Когато се извършва това, имената на координиращите пунктове се заместват с координатите на мрежата. Например:

ACA ZUMA, altitude 500 to 1000 meters, Rose to Jones, width 300 meters, effective 191830Z to 191835Z.

Координиращите пунктове се използват, за да се улесни създаването на ЗКВП за въздухоплавателни средства, опериращи в тилните зони, където техните маршрути могат да се пресекат с траекториите на артилерийските снаряди. Често използваните зони могат да останат в сила за постоянно. Маршрутите, които се използ-

ват понякога (по време на извикване), могат да получат кодови имена и да се активират, при нужда. Например: “Activate ACA ZULU 181600Z to 181610Z.” (Фиг.2)



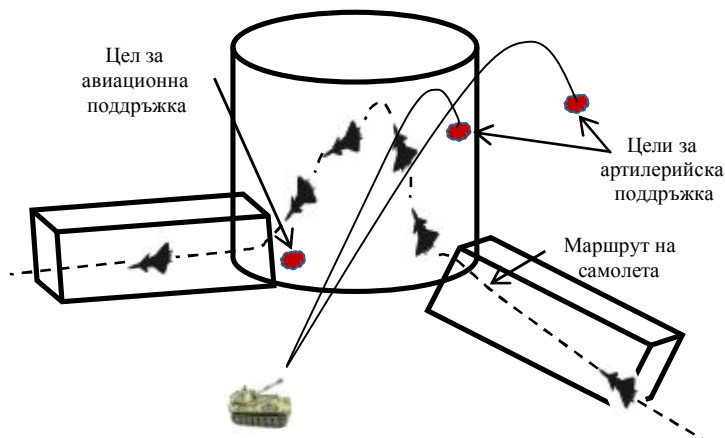
Фиг. 2. Зона за координиране на въздушното пространство по координиращи пунктове

Когато въздухоплавателните средства трябва да следват непредвидени маршрути, те могат да бъдат насочени да преминат от серия координиращи пунктове. Тези координиращи пунктове могат да бъдат назначени като незабавни ЗКВП.

Подходите за хеликоптери също могат да бъдат определени като ЗКВП за периода, в който те всъщност се използват. По същия начин, задържащите области и атакуващите позиции за средствата за въздушна огнева поддръжка могат да бъдат определени като ЗКВП.

ЗКВП за въздухоплавателни средства, действащи в рамките на зоната за поразяване на противниковите средства за ПВО е необходимо да се планират детайлно. Докато въздухоплавателните средства летят извън тези зони, те могат да следват прави, предвидими пространства. Въпреки това, когато въздухоплавателните средства са в зоната за действие на средствата за ПВО на противника, въздухоплавателното средство обикновено се нуждае от свобода за маневриране. По този начин ЗКВП за въздухоплавателни средства, действащи в близост до противникови ПВО, обикновено съдържат дълги тесни зони от въздушно пространство, които избягват зоните на противниковите ПВО или големи обемни въздушни пространства в тези зони.

ЗКВП в зона с висока заплаха е представена на фиг. 3. В този случай зоната близо до целта е във вид на голям цилиндър. В него атакуващият самолет разполага с необходимото пространство за избягване на противниковите оръжия за ПВО.[3]



Фиг. 3. Зона за координаране на въздушното пространство
в зона с висока заплаха

Формата и размерът на ЗКВП се променят със заплахата и тактиката за използване на самолетите. Също така зависят от вида на самолета, възможностите му за маневриране и използваните тактики за противодействие на заплахата. Офицерът за управление на авиацията (air officer) в центъра за координаране на огневата поддръжка (ЦКОП) трябва да бъде наясно с развиващите се авиационни тактики, така че при определяне на размера и формата на ЗКВП да се предвиждат като важно условие.

ЗКВП може да се намира над зоната за поразяване на целите. Може да бъде във формата на правоъгълна кутия или цилиндър по протежение на пътя на самолета или комбинираная от двете форми (фиг.3). Формата на ЗКВП се определя от пътя на самолета и от необходимостта да се осигури защита от „приятелски огън“.

Размерите на ЗКВП могат да бъдат изпращани до подчинените формирования под каквато и да е форма, която предоставя достатъчно информация, за планиране на огневата поддръжка около полетния път на самолета.

За ЗКВП с правоъгълни размери описанието може да включва името, минималната и максималната височина над земната повърхност, дължината (по координирани пунктове), ширината (общо, разделена от централната линия) и времето за прелитане (Military Date Time Group - DTG)[6].

Размерите на ЗКВП могат също така да бъдат определени в стандартните оперативни процедури или според конкретна заплаха, така че да се публикува само името, точките за местоположението им и ефективното време.

Размерът и формата на ЗКВП зависят от:

- Типа на въздухоплавателно средство. Обикновено, колкото по-висока е скоростта на самолета, толкова повече място е необходимо за маневриране.

- Вида на въоръжението. Зависи както от маршрута към целта, така и от радиуса на завоя на атакувания самолет.

- Заплахата от оръжията за ПВО на противника. Заплахата често определя вида на ЗКВП, използван в дадена операция. В рамките на обсега на оръжията за ПВО въздухоплавателните средства се нуждаят от пространство за маневриране.

- Ниво на ограничаване. ЗКВП могат да варират в зависимост от нуждата за маневриране на въздухоплавателни средства или при използване на средства за артилерийска поддръжка. Създаването на ЗКВП, които позволяват на самолетите максимална свобода на движение имат много големи размери и значително ограничават възможността за използване на артилерията. Те трябва да се поддържат в сила за възможно най-кратък период от време.

Предварително планираните ЗКВП и тези по извикване се разпространяват от командните пунктове (Ground Combat Element (GCE) и / или Marine Air-Ground Task Force Force Fires Coordination Center (MAGTF FFCC), с писмен документ.

Пример за съобщение за ЗКВП:

*ACA ZUMA, 41st MBr
Min Alt: 500 meters (MSL)
Max Alt: 1,000 meters (MSL)
Effective: 131000-131005 OCT16*

Непосредствено определени ЗКВП обикновено се разпространяват от центъра за координиране на огневата поддръжка на формирането, поискало въздушната огнева поддръжка. Планираните заявки и тези по извикване обикновено се изпращат от 18 до 24 часа преди мисията. През този период ЗКВП, свързани с тези мисии, се събират от GCE или MAGTF FFCC, преглеждат се, коригират се и се разпространяват към формиранятията.

IV. Заключение

Постигането на високо качество на управлението на войските е един от най-важните, сложни и комплексни съвременни проблеми на военното дело. Решаващ фактор за оценка на качеството на управлението си остава крайният резултат – степента на изпълнението на задачите от формиранятията.

Съвместната огнева поддръжка изисква пълно синхронизирано и координирано взаимодействие в всички елементи в нея, както и задълбочено и непрекъснато планиране.

Времето за действие на ЗКВП зависи от разпределението на целите за поразяване между сухопътния, военноморския и военновъздушния компонент. При съставянето на матрицата на огъня, времето за авиационните огневи налети ще бъде и времето на действие на ЗКВП, този случай се използва за широки зони, като средствата за огнева поддръжка на останалите видове въоръжени сили не изпълняват огневи задачи.

Изпълнението на съвместна огнева поддръжка при действаща по време ЗКВП е възможна при условие, че траекториите на снарядите на сухопътния и военноморския компонент минават под минималната височина или над максималната височина на полета на средствата за авиационна огнева поддръжка.

Използвани съкращения

МКОП - мерки за координиране на огневата поддръжка

ПВО - противовъздушна отбрана

ЦКОП - център за координиране на огневата поддръжка

ACA - Airspace Coordination Area

CFL - Coordinated Fire Line

BCL - Battlefield Coordination Line

DTG - Military Date Time Group

GCE - Ground Combat Element

FFA - Free-Fire Area

FSCL - Fire Support Coordinated Line

FSCM - Fire Support Coordinating Measures

MAGTF FFCC - Marine Air-Ground Task Force Force Fires Coordination Center

RFA - Restrictive Fire Area

RFL - Restrictive Fire Line

Литература

1. Речник на термините и дефинициите, използвани в НАТО (AAP 6), (на английски и български език). 2014г.
2. Тактическа доктрина на полевата артилерия. Военно издателство 2005г.
3. Appendix B. Fire Support Coordinating Measures
<http://www.globalsecurity.org/military/library/policy/usmc/mcwp/3-16/appb.pdf>
4. DOD Dictionary of Military and Associated Terms, July 2017
5. Joint Publication 3-09. Joint Fire Support. 12 December 2014
http://www.dtic.mil/doctrine/new_pubs/jp3_09.pdf
6. http://armawiki.zumorc.de/index.php/Date-time_group

Д. К. Марков,

ТРАНСФОРМИРАНЕ НА КООРДИНАТИТЕ НА ТОЧКИ МЕЖДУ КООРДИНАТНИ СИСТЕМИ СК-42 И WGS – 84 ЗА НУЖДИТЕ НА АРТИЛЕРИЙСКИТЕ ФОРМИРОВАНИЯ

Дилян К. Марков

TRANSFORMATION OF POINT COORDINATES BETWEEN CK-42 AND WGS-84 COORDINATE SYSTEMS FOR ARTILLERY UNITS

Dilyan K. Markov

Abstract: *The purpose of this publication is to briefly present the coordinate systems used in artillery of the Bulgarian Army. It specifies how to convert the coordinates of the points in the different coordinate systems and the possible assumed conversion errors.*

Keywords: *coordinate systems, geodetic transformations, datum transformations, converting, CK - 42, WGS 84*

Въведение

Едно от най-важните условия за ефективното изпълнение на задачите от артилерийските формирования е да са налични точните координати на целите. Местоположението на целите може да се определи по полярни или правоъгълни координати посредством различни средства за разузнаване.

Когато средствата за разузнаване и поразяване на целите работят в една координатна система, не съществува проблем, но използването на различни системи ще доведе до трудности в дейността им.

В артилерията на Българската армия се използват Координатна система 1942 (СК-42) и Световна геодезическа система 84 (World Geodetic System 84 - WGS84).

Наличието на двете системи изисква преобразуване на координатите от едната в другата и обратно. За тази цел е необходимо използване на определен математически апарат. Преди за се разгледа същността на конвертирането е необходимо да се разяснят видовете координати и същността на координатните системи.

Фигурата на земята

Фигурата на Земята има формата и размерите на реалната или физическа земна повърхност, т.е. повърхността, която разделя твърдите и течни маси (земната кора, моретата и океаните) от атмосферните. Спокойната повърхност на Световния океан, която обхваща 71% от повърхността на Земята, представлява идеална повърхнина, която навсякъде е перпендикулярна на силата на тежестта на отвесната линия. Повърхността на земната кора (материците) е най-разнообразна и сложна, като най-големите възвишения достигат до 8825 m. Спрямо средния радиус на Земята (6371 km) те са много малки (1/600). Ако се вземе глобус за модел на Земята с радиус 600 mm, представляващ повърхността на Световния океан, то най-високата точка на матерациите ще се издига на 1 mm. За това за фигура на Земята се взема

нивоповърхнината, която съвпада със средното положение на водната повърхност на океаните и откритите морета. Тя навсякъде е перпендикулярна на отвесната линия. Тялото, което се ограничава от тази повърхност се нарича геоид. Повърхността му има сложна и неправилна форма. При обработка на резултатите от геодезически измервания, вместо сложната повърхност на геоида се приема математически правилна повърхност на елипсоид.[4]

Повърхността на елипсоида е тази математична референтна повърхност (координатна повърхност), на която се проектират измерените елементи (дължини и ъгли), след което се обработват за определяне на взаимното положение на проекциите на геодезическите пунктове.

Земният елипсоид е ротационен, чиито размери са определени от размерите на Земята. Размерите се определят от градусни измервания и съвместно използване на гравиметрични наблюдения и геодезически измервания.

Видове координати в артилерията

Координатите са линейни и ъглови величини, които определят положението на точките на някаква повърхнина или в пространството. Линиите и равнините, от които се определя положението на точките са координатните оси и координатните равнини.

Положението на точките на земната повърхност и на повърхността на елипсоида се определя от техните координати, като за целта се използват географски, правоъгълни и полярни координати.

Географски координати

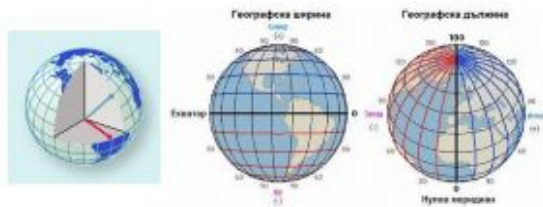
Координатните равнини в системата на географските координати са екваторната и меридианната равнина. В тази система положението на която и да е точка се определя чрез географската ширина и географската дължина (фиг. 1).

Ширината се отчита от двете страни на екватора и може да бъде северна и южна, като има стойности от 0° до 90° .

Дължините се отчитат от Гринвичкия меридиан на изток и на запад. Имат стойности от 0° до 180° .

Геодезическата ширина и дължина (В и L) определят положението на дадена точка върху повърхността на елипсоида. За определяне на съответстващата точка от физическата земна повърхност е необходима надморската височина – h, като трета координата, т.е. разстоянието от геоида до терена.

Геодезическата координатна система е обща за цялата повърхност на елипсоида. Тя е основа за преминаване към системата от линейни повърхностни координати към равнинни повърхностни координати (например проекцията на Гаус).

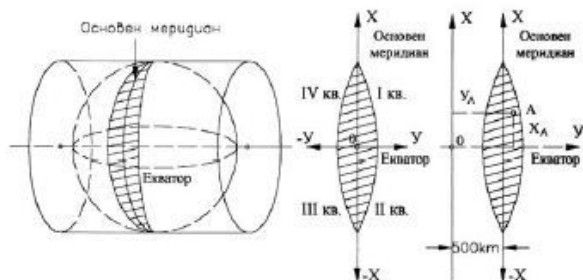


Фиг. 1. Географски координати

Равнинни правоъгълни координати

Най голямо приложение в артилерията намират равнинните правоъгълни координатни системи. Те се използват при изобразяване на ограничени части от повърхността на елипсоида върху върху равнина в една или друга проекция.

Равнинната правоъгълна координатна система се дефинира от взаимно перпендикулярните оси OX – абциса и OY – ордината. За абцисна ос се приема даден меридиан (основен меридиан), а за ординатна ос – екватора. Пресичането на двете оси е началото на координатната система (фиг. 2).



Фиг. 2. Равнинната правоъгълна координатна система

За да се използват равнинните правоъгълни координати вместо геодезическите, е необходимо да се премине от повърхността на земния елипсоид върху равнина. Повърхността на елипсоида е неразвиваема в равнина и нейното изображение е възможно само с използване на дадена проекция. Всяка проекция на елипсоида върху равнина се съпровожда неизбежно от деформации на изобразяваните фигури, намиращи се върху повърхността на елипсоида. Величината и характерът на деформациите се определят от вида на дадена проекция.

Координатна система 1942 (СК-42)

Геодезическата ситема 1942 г. е въведена през 60-те години. Това е Съветската геодезическа система, със следните изходни данни и параметри[2]:

Геометрични параметри:

Елипсоидът на Красовски с размери:

- $a = 6378245 \text{ m}$. - екваториален радиус;
- $1/f = 298.3$ - геометрична сплеснатост.

Изходни геодезически данни:

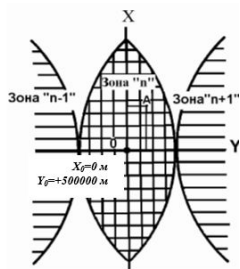
Геодезическите географски координати на основната точка в астрономо-геодезическата обсерватория „Пулково“:

- $\varphi_0 = 59^\circ 46' 15''.359$,
- $\lambda_0 = 30^\circ 19' 28''.318$,
- $\alpha_0 = 120^\circ 06' 42''.305$ към специално стабилизиран сигнал.

Елипсоидът на Красовски се използва и в геодезическа и картографска работа на всички страни от бившия Съветски съюз, Източна Европа, Китай, Индия, Северна Корея, Южна Корея, Монголия и други страни. В бившия СССР, Русия и някои други страни за мащабни карти, се използва подобна проекция на Гаус-Крюгер. Тази проекция е конформна и запазва ъглите и посоките.

Основните проекционни координати са Гаусовите координати, със съответствашата на тях проекция. В нея се обработват и поддържат държавните геодезически мрежи от всички класове и се изработват военните топографски карти.

Начало на координатната система е пресечната точка на екватора с някой от меридианите, наречен осев. Този меридиан се изобразява върху съставящата на цилиндъра в мащаб, т.е. в реалната си дължина и това е абсцисата X (север) на системата. Ординатата Y започва от оста X – на изток положителна (растяща), на запад отрицателна (намаляваща).



Фиг. 3. Разделяне на 6° зони

За да не надминат деформациите графическата точност на топографските карти, граничните меридиани на координатните зони се вземат през 6°. Граничните меридиани за две съседни зони са общи и започват от Гринвичкия меридиан. Така например първа зона се ограничава от меридианите с дължина 0 и 6, втора – 6 и 12 и т.н.

СК- 42 е разпространена в България в началото на 60-те години на XX век чрез Държавната триангулация, след[1]:

- допълване на първокласната мрежа с Лапласови азимути, свързането ѝ с тази на Румъния и ново изравнение върху елипсоида на Красовски, с изходни точки от тогавашната руска първокласна мрежа;
- усъвършенстване и ново изравнение на второкласната мрежа;
- усъвършенстване, реструктуриране и изравнение на мрежите III и IV клас.

На територията на България, в СК - 42 са дефинирани следните видове координати:

- географски координати върху елипсоида на Красовски;
- проекционни Гаусови координати в две шестградусови зони – с осев меридиани 21° и 27°, мащаб по меридиана – единица и начало на абсцисите от екватора.

Всяка от тези зони има свой номер и той се определя по формулата:

$$№ = (L_0 + 3) / 6 \quad (1)$$

За територията на България: № 21 = (21+3)/6 = 4;

$$№ 27 = (27+3) / 6 = 5.$$

Положението на дадена точка по картата се определя в пълни или съкратени правоъгълни координати.

Пълните правоъгълни координати определят положението на точката в границите на една координатна зона, при това абсцисата X се отчита от екватора, а ординатата Y от условно начало, изнесено на 500 km на запад от осевия меридиан на зоната (по Баумгард).

Към значението на ординатата отпред се записва цифра, която означава номера на зоната, например 5 459458, където цифрата 5 е номера на зоната.

Световна геодезическа система 84 (World Geodetic System 84 – WGS 84)

Световната геодезическа система WGS 84 е въведена (дефинирана и реализирана) от Националната агенция за геопространствено разузнаване - National Geospatial Intelligence Agency (NGIA), бившата Национална агенция за изображение и картография – National Imaginery and Mapping Agency (NIMA), и Министерството на отбраната (Department of Defense DoD) на Съединените щати.

Тя, се използва у нас от началото на 90-те години на миналия век. При това без да се подменят действащите към момента национални системи. С навлизането на тези технологии с особена острота възникват проблемите за преобразуване на националните геодезически референтни системи към WGS 84. По отношение на българското картно производство, реализирано в нея, Военно географската служба на БА издава военнотопографски карти на страната в UTM / WGS84, по единна разграфка и мащабен ред, съгласно стандартите на NATO. [3]

Световна геодезическа система 84 използва универсалната напречна проекция на Меркатор (UTM - Universal Transverse Mercator). Това по своята същност е наименование на гаусовата проекция, но се налага по терминология, приета от Военно географската служба на САЩ и е разпространено в страните на NATO като един от стандартите на тази организация. Тя се използва за създаване на военнотопографски карти в дребни мащаби – от 1:50 000 и по-дребни. Реализира се по 6^о -ови зони с мащаб по основния меридиан - Mo = 0,9996.

На нея се базира работата на GPS (Global Position Sistem) и се препоръчва като международен стандарт е със следните компоненти:

- координатна система с начало в масовия център на земята и ориентация на осите идентично с това на Конвенционалната земна референтна система (CTRS) приета през 1991г.
- общоземен референтен елипсоид WGS 1984 с параметри:
 - голяма полуос $a = 6378137$ м.
 - сплеснатост на елипсоида $f = 1/298,2572223563$.
- нормалната сила на тежестта се изчислява по формулата на Пицети - Сомилана;
- трансформационни параметри за установяване връзка със 83 местни координатни системи.

Картографска проекция при WGS 84

За картографиране на територии е възприета Универсалната напречна проекция на Меркатор (UTM), която се използва за областта ограничена от 80 ю.ш. и 84 с.ш., а за полярните области на север от 84 с.ш. и на юг от 80 ю.ш. се използва Универсалната полярна стереографична проекция.

Основните характеристики на Универсалната напречна проекция на Меркатор са:

- проекцията е равногълна;
- деформациите са малки и лесно се отчитат;
- формулите за преход са прости и удобни за табулиране и изчисления.

Универсалната напречна проекция на Меркатор е проекция върху цилиндър, допирателен на Екватора (меридианите се изправят по цилиндъра). Оста на цилиндъра е перпендикулярна на Земната ос и сече, земната повърхност в две секущи спрямо осевия меридиан на зоната.

UTM проекцията се получава като цилиндърът е условно неподвижен и Земята се завърта и на всеки 6° и се снима ивица за проекцията.

Номерацията на зоните се извършва с начало, вместо на 3° от Гриничкия меридиан (0°+3°), с 3° от меридиана $L = 180^\circ$ ($180^\circ+3^\circ$), т.е. на обратната страна на същата меридианна елипса. Номерата на шестградусови зони, в които попада територията на нашата страна, се определят по формулата:

$$N_z = (180 + L_0 + 3) / 6, \quad (2)$$

където - L_0 е географската дължина на осевия меридиан.[3]



Фиг. 4. Номера на зоните за територията на България при UTM проекцията

За територията на България (фиг. 4):

$$N_z 21 = (180 + 21 + 3) / 6 = 34;$$

$$N_z 27 = (180 + 27 + 3) / 6 = 35.$$

Получените по този начин номера на зоните не се изписват към стойностите на ординатата Y , както това се прави при СК 42. Тук към ординатата остава само добавената константа 500 000 м. При това положение еднозначното определяне на местоположението на дадена точка по нейните X , Y – координати, изисква указването и на съответната зона, в която попада точката.

В реализацията на UTM са разменени местата на координатите, като на първа позиция е поставена ординатата Y , с обозначение E (Easting), а на втора позиция – абсцисата X с обозначение N (Northing). Това е чисто формално подреждане, но облекчава контактуването с различните системи.[3]

Трансформиране на координати на точки между референтните координатни системи

Когато работим с електронни карти или използваме устройства за дистанционно отчитане на данни, почти винаги имаме необходимост от трансформиране на координатите в други координатни системи. Въпреки, че по себе си този процес не е сложен, съществуват уловки в тази дейност.

Както беше посочено, ако се работи в една координатна система, това е просто, но преходът към данните от друг мащаб, промяна на проекцията, която съчетава в едно данни от различни източници, прехода от местна координатна система към глобална се проявява с това, че изображението на обект в една система е различно в друга. Причините за това могат да бъдат обективни обстоятелства или потребителски грешки.

Точни формули за трансформиране на координати между различни координатни системи се прилагат само в сферата на „перфектната геометрия“, а не в реалния свят. Координатите на точка в една координатна система се получават от голям брой наблюдения, които се осредняват заедно, като се използва цял набор от предположения. Както наблюденията, така и предположенията са само приблизително правилни и могат да бъдат със съмнително качество, особено ако данните за точка-

та са били определени преди много време. Тя ще е сменила своето местоположение, поради множество явления настъпили със земната кора.

Реалните координати на точка на земната повърхност се променят, поради непрекъснатите деформиращи движения на Земята. Относно центъра на Земята, точка на земята може да се движи всеки ден на един метър нагоре и надолу, само заради приливните влияния на слънцето и луната. Относителното движение на два континента може да бъде 10 сантиметра годишно, което е важно за картографирането, тъй като е постоянно година след година и след 50 години един регион на Земята може да се е преместил с 5 метра спрямо съседен континент. Много други малки ефекти могат да се наблюдават - потъването на Великобритания, когато приливът попада над континенталния шелф (няколко сантиметра), потъването на вътрешните територии при високи климатични условия (около 5 милиметра) и покачването на нивото на Земята в следствие от топенето на ледовете (около 2 милиметра годишно в Шотландия, до 1 сантиметър годишно в Скандинавия). Като цяло, колкото повече размерът на Земята, над който искаме да използваме една координатна система, се променя, толкова повече тези динамични ефекти на са значителни.[9]

Съвременната тенденция е да се използват глобални координатни системи дори за локални приложения. Ето защо е важно да осъзнаем, че в една глобална координатна система, нашата позиция постоянно се движи. Това води до тънкостите в дефинирането и използването на координатните системи.

Поради това, връзката между две координатни системи в настоящия момент също трябва да се наблюдава на място, а това наблюдение също е подложено на грешка. В следствие на това могат да съществуват само приблизителни модели, за да се трансформират (преобразуват) координатите от една координатна система в друга.

Важен въпрос, върху който реалистично трябва да се помисли е „Каква точност наистина се изисква?“ Като цяло, ако изискванията за точност са ниски (от 5 до 10 m), тогава трансформирането на координати от една координатна система в друга е лесно. Ако изискванията за точност са по-високи (от 1 cm до 0,5 m), ще бъде необходим по-подробен процес на трансформация. И в двата случая процедурата за преобразуване трябва да има посочено ниво на точност.

За нуждите на артилерийските формирования точността (от 5 до 10 m) е напълно достатъчна за изпълнение на поставените задачи.

Геодезическата трансформация е математическа операция, която приема координатите на точка в една координатна система и връща координатите на една и съща точка във втора координатна система. За постигането на тази задача се използват много видове математически операции.

Степента на грешка при геодезическата трансформация ще зависи от видовете грешки, които често са характерни за методите, използвани за тази дейност, както и от това колко внимателно е извършена трансформацията. Например, данните за точките от една мрежа, установени чрез триангулация, обикновено съдържат значителни грешки в общия размер на мрежата и често тези грешки варират в различните части на мрежата. Следователно реалната трансформация е вероятно да представлява не само разликата между геодезическите данни, но и разликата между точките, които реализират тези данни поради грешки в първичните наблюдения.

Причините, по които могат да се различават данните от два елипсоида, са:

- производ на координатите;

- ориентация на координатните оси;
- размер и форма на еталонния елипсоид.

Важен параметър е и коефициента на мащаба, който позволява мащабът на осите да варира между двете координатни системи. Това може да бъде объркващо, защото мащабният фактор няма нищо общо с конвенционалната дефиниция на данните, изразена от други параметри за преобразуване.

Може да съществува перфектна трансформация само между перфектните тематически референтни системи. На практика се определят и използват трансформации между множества от реални земни точки, т.е. между такива, които са предмет на грешките на реалния свят. Колкото повече изкривявания, понижения и т.н. присъстват при определяне на техните координати, с толкова повече отклонения ще бъде трансформацията. Това означава, че както входните данни на трансформацията, така и изходните координати ще съдържат грешки.

Когато характеристиките на извитата повърхност на Земята са представени на равнинна повърхност, изкривяванията при разстоянията и ъглите са неизбежни. Първоначално „равнината на повърхността“ е била карта. Сега тя често е равнина координатна система на GIS софтуер. Една проекция на картата е всяка функция, която преобразува елипсоидните в равнинни координати. Картографските карти използват различен тип проекция за съответната система

За преобразуването на координатите на точките, от една координатна система в друга могат да се използват вече съществуващи методики [1, 5, 6, 7, 8, 9], които извършват:

- преобразуване на правоъгълни пространствени координати в геодезически;
- преобразуване на правоъгълни пространствени координати от една система в друга;
- преобразуване на геодезически координати в правоъгълни пространствени координати.

Заклучение

Преобразуването на координатите от една система в друга и обратно е трудоемък процес, изискващ определено програмно осигуряване или използване на електронни таблици, с необходимата точност за артилерията, които да отчитат посочените различия в системите.

За да се избегнат дори и минималните натрупани грешки при работата в двете системи е необходимо преминаване за работа само със Световната геодезическа система 84 (World Geodetic System 84 - WGS84), съгласно стандартизационните споразумения на НАТО и поради факта, че използваните в нашата армия GPS приемници функционират с тази система.

Литература:

1. Инструкция № РД-02-20-12 от 03 август 2012 г. за преобразуване на съществуващите геодезически и картографски материали и данни в „Българска геодезическа система 2005“. 2012 г.
2. Йовев И. Държавните геодезически мрежи на България и свързаните с тях референтни, координатни и височинни системи. БАН, Висша геодезия, бр.16, 2003.
3. Йовев И. GPS – технологиите и създаване на условия за тяхното ефективно приложение в България. сп. „География 21“, изд. МОН, бр. 4, 2007.
4. Топогеодезическа подготовка в земната артилерия. МО. София. 1978г.

5. ГОСТ Р 51794-2001 Аппаратура радионавигационная глобальной навигационной спутниковой системы и глобальной системы позиционирования. Системы координат. Методы преобразований координат определяемых точек https://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_51794-2001

6. A guide to coordinate systems in Great Britain. An introduction to mapping coordinate systems and the use of GPS datasets with Ordnance Survey mapping. D00659. May 2002

7. Datum Transformations of GPS Positions.

<https://microem.ru/files/2012/08/GPS.G1-X-00006.pdf>

8. Handbook for Transformation of Datums, Projections, Grids and Common Coordinate Systems. U.S. Army Corps of Engineers Topographic Engineering Center. January 1996.

9. User's Handbook On Datum Transformations Involving WGS 84. International Hydrographic Bureau MONACO, July 2003

<https://badc.nerc.ac.uk/help/coordinates/OSGB.pdf>

Н. Г. Борисова,
**ОПАЗВАНЕТО НА ОБЩЕСТВЕНИЯ РЕД ОСНОВНА ДЕЙНОСТ
НА ОРГАНИТЕ НА МВР**

Нели Г. Борисова

*Шуменски университет „Епископ Константин Преславски”, Шумен
Факултет по технически науки
e-mail: neli_borisova@abv.bg*

**PRESERVATION OF THE PUBLIC ORDER MAIN ACTIVITY
OF THE BODIES OF THE MIA**

Neli G. Borisova

*Konstantin Preslavsky University of Shumen, Shumen 9712,
115, Universitetska str.*

Abstract: *The ministry of the interior is the institution, which has a main place in the functioning of the public life in the country, in the activities of the other state bodies, taking care of the protection of the public order and the counteracting crime in the territory of the whole country. Its tasks and activities derive from the law on the ministry of interior, which defines the principles for the implementation of the activities, the functions, the management, the organization of the employees.*

Keywords: *public order, Ministry of Interior*

Въведение

Министерството на вътрешните работи е институцията, която заема основно място във функционирането на обществения живот в страната, в дейността на другите държавни органи, като се грижи за опазването на обществения ред и противодействието на престъпността на територията на цялата страна. Задачите и дейностите ѝ произтичат от ЗМВР, който определя принципите за осъществяване на дейността, функциите, управлението, устройството и статута на служителите.

Опазването на обществения ред и противодействието на престъпността винаги са били в основата на развитието и дейността на органите в системата на МВР. Дейността на МВР основно е насочена към защита на правата и свободите на гражданите, защита на националната сигурност, опазване на обществения ред и пожарна безопасност и защита на населението, а част от основните дейности са оперативно-издирвателна, охранителна и превантивна.

Съставките на различните проявления на дейността по опазване на обществения ред са:

- Защита на националната сигурност
- Противодействие на престъпността

- Защита на права и свободите на гражданите и имуществото им
- Осигуряване на държавна и аварийна безопасност
- Охрана и контрол на държавната граница
- Защита от тероризъм
- Оказване на съдействие и на други държавни органи и др.

Изложение

Понятието „опазване на обществения ред“ от органите на МВР се определя като регламентирана с норми на публичното право система от обществени отношения, осигуряваща общественото спокойствие и безопасност, охраната на които е възложена на полицията със закон.

МВР гарантира опазването на обществения ред и сигурността на гражданите чрез охранителната дейност на своите органи.

Като цел на опазването на обществения ред може да се посочи овладяването и ограничаването на престъпността, повишаване на личната сигурност, опазване на личното, частното и държавното имущество, защита на законните права и интереси на гражданите, предприемане на превантивни мерки спрямо уязвимите за обществения ред места и спрямо рисовите социални групи от обществото.

При осъществяване на дейността си по опазване на обществения ред служителите на МВР имат следните правомощия:

- възможност за издаване на административни актове, разпореждания, разрешения, удостоверения;
- право на призовавания;
- право на проверка за установяване на самоличността;
- право на задържане на лица;
- право на използване на технически средства за явно наблюдаване;
- право на личен обиск;
- право на проверка в жилищни и други помещения;
- право да се използва физическа сила и помощни средства – само като крайно средство;
- извършване на други действия;
- реализиране на принудителни административни мерки;
- реализиране на административно-наказателна отговорност – реализира се чрез налагане на глоба до 2000 лв.;
- използване на оръжие.

Издаване на „Разпореждания“ като основанията за това са регламентирани в чл. 64, ал. 1 от ЗМВР *„Полицейските органи могат да издават разпореждания ... когато това е необходимо за изпълнение на възложените им функции.“* Законът регламентира и формите за отправяне на разпореждането - устно или писмено. Важно е да отбележим, че разпорежданията на полицейския орган са задължителни за изпълнение.

Издаване на „Предупреждения“ - чл. 65, ал. 1 от ЗМВР *„Полицейските органи предупреждават устно или писмено лицата, за които има достатъчно данни и се предполага, че ще извършат престъпление или нарушение на обществения ред“.* От текста на тази правна норма се вижда, че на полицейските органи е предоставена възможност да отправят предупреждения както при наличието на данни за престъпление, така и за нарушение на обществения ред. Предупреждението може да

бъде отправено устно или писмено, с което законодателят е очертал възможност за алтернативно решение, предоставено на избора на полицейския орган.

Съгласно чл. 65, ал. 2 от ЗМВР *„за писменото предупреждение се съставя протокол, с който лицето се предупреждава за отговорността, която се предвижда при извършване на съответното престъпление или нарушение на общественения ред“*.

По своята същност предупреждението е само едно авторитетно напомняне за отговорността, която е предвидена в материално - правните норми и която въпросното лице ще понесе в случай на извършване на правонарушението, независимо от това дали е предупреждено или не. С протокола лицето се предупреждава за отговорността, която е предвидена при извършване на съответното престъпление или нарушение на обществения ред. С това ясно и категорично е очертана целта на предупреждението - да се въздейства върху психиката, върху целия мисловен, емоционален и волеви комплекс на конкретното лице с оглед мотивирането му към правомерно поведение.[1] Реализирането на целта с полицейското предупреждение и постигането на ефективни резултати при решаването на всеки един случай зависи най-вече от правилната организация на работа. Като изхождаме от това положение, на това място от работата си позволяваме да посочим някои подробности, съпътстващи осъществяването на полицейското предупреждение.

„Призоваване на граждани“ - Правото на полицейските органи да призовават лица е визирано в чл. 69 от ЗМВР. Съгласно тази норма *„Полицейските органи могат да призовават в служебните помещения граждани за осъществяване на действия по определените им с този закон правомощия.“* Призоваването на граждани се осъществява писмено. В неотложни случаи призоваването може да се извършва по телефон или факс. Призоваването по телефон или факс се удостоверява писмено от длъжностното лице, което го е извършило. В Закона за Министерството на вътрешните работи е предвидена административнонаказателна санкция за лице, което без уважителни причини не се яви след като е редовно призовано. От това следва, че неизпълнението на задължението за явяване е обявено като самостоятелен неправомерен фактически състав.

„Установяване на самоличността“ - съгласно чл. 70, ал. 1 от ЗМВР органите на полицията могат да извършват проверки за установяване самоличността на лице:

- за което има данни, че е извършило престъпление или друго нарушение на обществения ред;
- когато това е необходимо за разкриване или разследване на престъпления и при образувано административно-наказателно производство;
- при осъществяване на контрол по редовността на документите за самоличност и пребиваване в страната;
- на контролен пункт, организиран от полицията;
- по искане на друг държавен орган за оказване на съдействие при условия и по ред, предвидени в закон.

В този текст правната норма съдържа две подхипотези. Едната се отнася до наличието на данни за извършването на престъпление, а другата - на данни за извършено нарушение на обществения ред. Съгласно чл. 70, ал. 2 от ЗМВР основният способ за установяването на самоличност е посредством представяне на документ. Законът допуска установяването на самоличността и чрез сведения на граждани с

установена самоличност, които познават лицето, както и други начини за събиране на достоверни данни.

„Задържане на лица“ - ограничаване правото на свободно придвижване може да бъде както превантивна мярка, така и административно наказание. В чл. 72, ал. 1 от ЗМВР законодателя е посочил хипотезите, при които полицейските органи могат да задържат лице, а именно:

- за което има данни, че е извършило престъпление;
- което след надлежно предупреждение съзнателно пречи на полицейски орган да изпълни задължението си по служба;
- което показва тежки психични отклонения и с поведението си нарушава обществения ред или излага живота си или живота на други лица на явна опасност;
- при невъзможност да се установи самоличността му в случаите и по начините, посочени в от ЗМВР;
- което се е отклонило от изтърпяване на наказанието лишаване от свобода или от местата, където е било задържано като обвиняем в изпълнение на разпореждане на орган на съдебната власт;
- обявено за издирване с цел задържане, както и по искане на друга държава във връзка с неговата екстрадиция или в изпълнение на Европейска заповед за арест, както и в други случаи, определени със закон.

„Използване на физическа сила и помощни средства от полицейските органи“

А. Използване на физическа сила и помощни средства от полицейските органи при противодействие или отказ да се изпълни законно разпореждане – чл. 85, ал. 1, т. 1 от ЗМВР - с цел защита правата и свободите на гражданите, противодействие на престъпността, защита на националната сигурност и опазване на обществения ред, полицейските служители от Министерство на вътрешните работи извършват следните дейности:

- оперативно-издирвателна;
- охранителна;
- разследване на престъпления;
- осигуряване на пожарна безопасност и защита при пожари, бедствия и извънредни ситуации;
- осигуряване на достъп на гражданите до службите за спешно реагиране чрез Националната система за спешни повиквания с единен европейски номер 112;
- информационна;
- контролна;
- превантивна;
- административнонаказателна и предоставяне на административни услуги.

Предвид гореизложеното на полицейските органи са предоставени определен кръг от правомощия, едно от които е издаването на разпореждания.

По своята същност разпореждането е изискване за предприемане на определени действия или въздържане от такива. В този смисъл с оглед изсяняване същността на хипотезата на чл. 85, ал. 1, т. 1 от ЗМВР, важно е да се отбележи, че с незаконното си противодействие конкретно лице възпрепятства полицейския служител да изпълни възложените му функции. Незаконното противодействие по своята същност е юридически факт, с възникването на който правната норма предвижда прекратяване на незаконното противодействие чрез използване на физическа сила и помощни средства и реализиране на съответната отговорност на виновното лице.

Отговорността за извършеното правонарушение от лицето може да е наказателна или административно-наказателна. При незаконния отказ да се изпълни законно разпореждане се цели въздействие върху адресата, мотивирайки същия към изпълнение на даденото полицейско разпореждане.

Независимо от формата, с която са отдадени, разпорежданията на полицейски орган са задължителни за изпълнение, като изрично е регламентирано, че същите могат да бъдат оспорвани по реда на Административно-процесуалния кодекс.

От посоченото до тук следва изводът, че с основание е регламентирано правото за използване на физическа сила и помощни средства от полицейските органи при противодействие или отказ да се изпълни законно разпореждане.

Б. Задържане на правонарушител, който не се подчинява или оказва съпротива на полицейски орган – чл. 85, ал. 1, т. 2 от ЗМВР.

Нарушаването неприкосновеността на личността е възможно, но само в изрично посочени от закона случаи. Изрично е регламентирано, че не се допуска ограничаване на свободата, въвежда се задължение за уведомяване на съответните компетентни органи и ограничение - задържането на лица не може да превишава срок, по-голям от 24 часа.

Съгласно чл. 72, ал. 1 от ЗМВР полицейските органи могат да задържат лице:

1. за което има данни, че е извършило престъпление;
2. което след надлежно предупреждение съзнателно пречи на полицейски орган да изпълни задължението си по служба;
3. което показва тежки психични отклонения и с поведението си нарушава обществения ред или излага живота си или живота на други лица на явна опасност;
4. при невъзможност да се установи самоличността му в случаите и по начините, посочени в чл. 70 от ЗМВР;
5. което се е отклонило от изтърпяване на наказанието лишаване от свобода или от местата, където е било задържано като обвиняем в изпълнение на разпореждане на орган на съдебната власт;
6. обявено за издирване с цел задържане, както по искане на друга държава във връзка с неговата екстрадиция или в изпълнение на Европейската заповед за арест;
7. в други случаи, определени със закон.

Видно от гореизложеното, законодателят е регламентиран конкретни хипотези, при които полицейските служители имат право да задържат физическо лице. В тази връзка с използването на физическа сила и помощни средства спрямо лице, което не се подчинява на полицейския служител се цели преустановяване на неподчинението и задържане на лицето.

В. Използване на физическа сила и помощни средства от полицейските органи при конвоиране на лице или при опит да избяга, да посегне на своя живот или на живота на други лица – чл. 85, ал. 1, т. 3 от ЗМВР.

Във всяка правова държава целта на правораздавателните органи, е налагането на справедливо наказание на всеки правонарушител. Своевременното отвеждане на извършителите на престъпления до съдебните органи и изпълнение на наложените им наказания имат пряко отношение към ефективното разкриване и превенция на престъпленията. Ето защо конвоирането на лица е една от основните дейности на органите на МВР. По своята същност конвоирането представлява принудително отвеждане от едно място на друго на едно или повече лица.

Обект на конвоиране са лица:

- по отношение на които е постановен акт за принудително довеждане от разследващ полицей по реда на НПК;
- задържани по чл. 72, ал. 1, т. 1-4, т. 6 и 7 от ЗМВР;
- с наложено от съда наказание “задържане в териториалната структура на МВР” при условията и по реда на Закона за опазване на обществения ред при провеждане на масови мероприятия и задържане до 15 денонощия в структурно звено на МВР” по реда на Указ № 904 от 28.12.1963г. за борба с дребното хулиганство;
- полицейските органи могат да конвоират и други лица, когато това е предвидено в закон.

Г. Използване на физическа сила и помощни средства от полицейските органи при оказване съдействие на други държавни органи или длъжностни лица, включително на контролорите на Европейската комисия, на които противозаконно се пречи да изпълняват задълженията си – чл. 85, ал. 1, т. 4 от ЗМВР.

Д. Използване на физическа сила и помощни средства от полицейските органи при нападения срещу граждани и полицейски органи – чл. 85, ал. 1, т. 5 от ЗМВР.

Съгласно ЗМВР полицейските органи защитават правата и свободите на гражданите и съдействат за упражняването на същите. Личната неприкосновеност е сред основните права на гражданите и, както вече е отбелязано е обект на правна регламентация не само в националното ни законодателство, но и в нормите на международното право. В този смисъл това е една от основните функции на полицейските органи.

От значение е наличието на нападение, при което на полицейските органи е предоставено правото да прилагат това полицейско правомощие. Независимо дали нападението е насочено срещу полицейски орган или трето лице, наличието му само по себе си обуславя адекватна защита и противодействие. Това е оправдано както с оглед опазване на обществения ред в страната, така и от гледна точка на обществен интерес - опазване живота и здравето на гражданите. Това правило в най - голяма степен се отнася до дейността на полицейските органи, призвани да противодействат на всяко правонарушение.

Е. Използване на физическа сила и помощни средства от полицейските органи при освобождаване на заложници – чл. 85, ал. 1, т. 6 от ЗМВР. Хипотезата на чл. 85, ал. 1, т. 6 от ЗМВР допуска използването на физическа сила и помощни средства при освобождаване на заложници. В конкретния случай е налице противозаконно лишаване от свобода или с други думи извършено е престъпление по смисъла на чл. 142а от Наказателния кодекс. Непосредствен обект на противозаконното лишаване от свобода са обществените отношения, чрез които се осигурява обективната възможност всеки човек да се придвижва свободно в пространството, като законосъобразно ограничаване може да се извършва единствено въз основа на закона, и то само от специално оправомощени за това държавни органи. Във връзка с гореизложеното с основание следва да бъде отбелязано, че разглежданата хипотеза, касае високорискова ситуация, която предполага участието на повече от един полицейски служител.

Ж. Използване на физическа сила и помощни средства от полицейските органи при групови нарушения на обществения ред – чл. 85, ал. 1, т. 7 от ЗМВР.

Използването на физическа сила и помощни средства в разглежданата хипотеза е свързано с нарушения на обществения ред, като субект на същите са две или повече лица (група). В тази връзка предвид високата степен на обществена опас-

ност на груповите нарушения на обществения ред законодателят е регламентирал възможност за преустановяването им чрез използване на физическа сила и помощни средства.

3. Използване на физическа сила и помощни средства от полицейските органи при нападения на сгради, помещения, съоръжения и транспортни средства – чл. 85, ал. 1, т. 8 от ЗМВР - използването на физическа сила и помощни средства има правно основание, когато е налице непосредствено противоправно нападение, което създава опасност от увреждане на обществени отношения, свързани с неприкосновеността на сгради, помещения, съоръжения и транспортни средства.

И. Освобождаване на незаконно заети обекти, ако им е разпоредено от компетентен орган – чл. 85, ал. 1, т. 9 от ЗМВР - с оглед изясняване на приложимостта на хипотезата следва да се отбележи, че съгласно чл. 323, ал. 1 от НК обектът е незаконно зает, ако извършителят не по установения от закона ред, осъществява едно оспорвано от друго свое или чуждо действително или предполагаемо право. В ал. 2 от същия член е регламентирано самоволното заемане на недвижим имот, от чието владение деецът е отстранен по надлежния ред.

Й. Вземане на мерки за осигуряване на личната безопасност по чл. 75, ал. 2 – чл. 85, ал. 1, т. 10 от ЗМВР - в тази хипотеза, законодателят е предвидил съществуването на висока степен на риск за нанасяне на телесни повреди и дори причиняване на смърт на полицейския служител. Извършването на проверка на задържано лице за наличие на опасни предмети и вещи е рискова ситуация, при която полицейският орган следва да има законова възможност да използва физическа сила и помощни средства с цел лична защита.

При осъществяване на дейността си по опазване на обществения ред полицейските органи са оправомощени да използват физическа сила и помощни средства. Видовете помощни средства съгласно разпоредбата на чл. 85, ал. 2 от ЗМВР :

- белезници;
- усмирителни ризи;
- каучукови, пластмасови, шурмови и електрошокови палки и прибори;
- химически вещества, утвърдени от министъра на здравеопазването;
- служебни животни - кучета и коне;
- халосни патрони;
- патрони с гумени, пластмасови и шокови куршуми;
- устройства за принудително спиране на превозни средства;
- устройства за отваряне на помещения;
- светлинни и звукови устройства с отвличащо въздействие;
- водометни и въздухоструйни машини;
- бронирани машини.

За осъществяване на своята дейност по опазване на обществения ред в МВР има утвърдена Стратегия „В близост до обществото“. Промяната в динамиката и структурата на отношенията между полиция и общество се налагат на първо място от причини, свързани със самата полиция:

- прекалена бюрокрация на полицейската система;
- откъсване на полицията от нуждите на гражданите;
- лоша координация и дублиране на функциите на службите;
- приоритетите на полицейската работа се определят от висшестоящите звена, без да се отчитат местните потребности от сигурност;

- полицията се стреми да постигне собствени критерии за качество, обикновено в сферата на организираната и тежката престъпност и др.

Философията на "Полицията в близост до обществото" се крепи върху две основни отправни точки: проактивност и решаване на проблеми. Проактивността се изразява в концентриране върху премахване на източниците на престъпността като не по-малко значима дейност от разкриването на извършените престъпления.

Решаването на проблеми в духа на "Полицията в близост до обществото" се свързва с намирането на креативни подходи за преодоляването на възникнали проблемни ситуации. Особено място в този процес играе местната общност и обществото като цяло.

Заклучение:

Настоящото проучване е продиктувано от необходимостта от осъществяване на анализ на огромния брой функции изпълнявани от служителите в Районното управление на МВР, съобразно дадените им правомощия и свързани с опазване на общественения ред, което е сложна и многоаспектна дейност.

Литература:

1. Христов, Х. Доклад на тема: „ Подходи за идентифициране на източниците на заплаха на организацията ”. Трета международна научна конференция –„Наука, образование, иновации”, посветена на 145 годишнината на БАН и 35 годишнината от космическия полет на Георги Иванов, 21-23.05.2014 г., Шумен. [1]

2. Закон за МВР, изм. ДВ. бр.58 от 18 Юли 2017г.

3. Указ № 904 от 28.12.1963г. за борба с дребното хулиганство.

4. Стратегия „В близост до обществото“.

М. М. Галиб, Х. Й. Косева.

ПРИЛОЖЕНИЕ НА КРИПТОВАЛУТАТА BITCOIN В ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА СИГУРНОСТ

Мерал М. Галиб, Христина Й. Косева

*Шуменски университет „Епископ Константин Преславски”,
Факултет по технически науки, e-mail: meralmhmd@abv.bg, hristinaii_@abv.bg*

IMPLEMENTATION OF CRYPTOCURRENCY BITCOIN IN THE INFORMATION SECURITY SYSTEMS

Meral. M. Galib, Hristina I. Koseva

Abstract: *In this paper implementation of cryptocurrency bitcoin in the information security systems. The bitcoin presents a special accounting communication system for supporting of online accounts. It works on Peer-to-peer security computer network with fully decentralized open source software or paid special software.*

Keywords: *Bitcoin, Cryptocurrency, Security, Computer networks.*

1. Увод

Човечеството се развива с изключителни темпове и именно навлизането и развитието на технологиите свидетелстват за тези процеси. Компютърните системи и устройства са до толкова навлезли в ежедневието на човека, че това налага извода, че бъдещето му ще зависи изцяло от тях. Колите вече имат автопилот, има GPS вместо географска карта в ръка. След това скоростно „заместване“ на така необходимите за човека неща, скоро е напълно възможно парите (т.е материалната им форма) да изчезнат и да бъдат превърнати в електронни кредити. Точно това се разработва и се създава нов проект в ерата на финансовия свят или с други думи това е т.н. Bitcoin. Това е валутата, която съществува само и единствено в електронен вариант, именно затова се нарича още и криптовалути, която става все по-популярна, превземайки отрасли с нейния лесен начин за използване, прашане и съхранение [1, 2, 3, 6].

2. Изложение

Биткойн е експериментална валута и парична система от нов вид, която няма аналог и до днес. Зад Биткойн не стои никой, т.е. няма държавен орган, централна банка или физическо, или юридическо лице, които да могат да му въздействат пряко или косвено. Освен това никой не притежава изключителни права да издава, разпространява, пуска или спира тези парични единици от обръщение. Има определена компютърна мрежа, която осъществява управлението. Тук няма географско местоположение за отговорното съхранение и пазене на Биткойн, както е например при златото и среброто, когато се използват за пари. Наред с това тук няма центра-

лен сървър, който се използва обикновено за индексване на съдържанието, както е при торент мрежите, използвани за споделяне на електронни книги, видео или аудио файлове. Накратко казано Биткойн се определя, като първата разпределена криптовалута [1, 2, 3, 6].

За да бъде платежната система защитена и наред с това да функционира без проблем се използват криптографски методи, а автентичността на транзакциите се гарантира и защитава чрез цифрови подписи. Един от основните елементи от мрежата е т. нар. публична счетоводна книга, съдържаща в себе си достъпен списък на всички извършени транзакции, наречен блокова верига. По този начин всеки потребител има възможността да проверява валидността на всяка извършена транзакция [1, 2, 3, 6].

Платежните единици биткойн играят ролята на възнаграждение за извършена изчислителна работа по криптиране, т.е. потребителите проверяват (валидират) съществуващите блокове от блоковата верига и създават нови, използвайки изчислителната мощ на компютрите си. Колкото е по-голяма е изчислителната мощ, включена в добиването, толкова по-сложна става математическата задача, което прави скоростта на добиване ограничена и предсказуема [1,2,3,6].

Биткойните могат да бъдат изпращани и получавани от потребителите по електронен път срещу определена такса, чрез употребата на електронно портмоне на своя компютър, мобилно устройство или уеб приложение. Освен чрез „добиване“ те могат да се получават срещу други валути, продукти или услуги. Същността на генерирането им предопределя „паричната им маса“. Към 2014 година има над 12 милиона биткойни в обръщение, като наред с това на всеки 10 минути се създават приблизително 25 биткойна. Въпреки това има установена горна граница на тяхното количество, която е от 21 милиона, на всеки четири години, а скоростта на тяхното добиване се намалява на половина, което показва, че нови биткойни ще продължат да се създават в бъдещите сто години [1,2,3,6].

Биткойните могат да бъдат изпращани и получавани от потребителите по електронен път срещу определена такса, чрез употребата на електронно портмоне на своя компютър, мобилно устройство или уеб приложение. Освен чрез „добиване“ те могат да се получават срещу други валути продукти или услуги. Същността на генерирането им предопределя „паричната им маса“. Към 2014 година има над 12 милиона биткойни в обръщение, като наред с това на всеки 10 минути се създават приблизително 25 биткойна. Въпреки това има установена горна граница на тяхното количество, която е от 21 милиона, на всеки четири години скоростта на тяхното добиване се намалява на половина, което показва, че нови биткойни ще продължат да се създават в бъдещите сто години [1, 2, 3, 6].

Начините за сдобиване с биткойн са седем на брой:

- Директно закупуване като това е възможно директно от банкомат или от т.нар. „Битомати“. Такъв има и в България, намира се в Интерпред-София. Чрез него може да се получават биткойни срещу левове.
- Размяна на продукти или услуги за биткойни.
- Expidia приема биткойн за хотелски резервации- Expidia е фирма за онлайн резервации, която позволява на клиентите си да използват дигитални пари.
- TESLA Motors приема плащания биткойн- виртуалната валута е използвана за покупка на TESLA електромобил. Продажбата става в

шоурум на Lamborghini в Калифорния. Стойността му - 103 000 долара се равнява на 91.4 биткойна.

- Възможно е да се купи къща с биткойн- за първи път това става от анонимен купувач, който се сдобил с луксозна вила на острови Бали.
- Университетът в Кипър приема биткойни като разплащателно средство, и не само той.
- Копане на биткойн, т.е. предоставяне на индивидуална изчислителна мощ за обработка и поддържане на данни. Всеки, който го направи се възнаграждава с новосъздадени биткойни [1, 2, 3, 4, 5, 6].

Всеки собственик трябва да има т. нар. Биткойн портфейл. Това е мястото, където се съхраняват електронните пари и чрез който могат да се плащат и получават биткойни. Тук се използват т. нар. криптографски ключове: един публичен, чрез който се идентифицира портфейлът и един личен, чрез който може да се пращат биткойни и който удостоверява собствеността на портфейла [1, 2, 3].

- Лесен трансфер на средства- лесно и бързо до всяка точка на света.
- Не подлежи на конфискация- за това са необходими двата ключа.
- Анонимност - тъй като електронният портфейл е напълно анонимен, трансферът на средства от и към него не изисква лични данни, а само идентификационния ключ, който показва адреса, където трябва да се пратят парите [1, 2, 3, 6].

Недостатъци на биткойна:

- Скъпоструващата техника- специализираната техника за копане на биткойни възлиза на 10 000 долара.
- Разход на електроенергия- използването на такива машини води до огромни разходи на ток.
- Биткойните са апетитни за хакерите- те могат да ги откраднат с ключовете и да ги продадат без да се разбере за това.
- Висока ликвидност- цената се мени изключително бързо и в двете посоки [1,2,3,6].

Възможностите, които предлага биткойнът са избягване на инфлацията, защото те са ограничен брой- 21 милиона и не могат да се генерират за разлика от парите, които просто биват напечатани нива. Другата възможност е безконтактното плащане, което дава все по- широки спектри на употребата на биткойни. Възможно е биткойнът да сложи край на финансовата система, т.е всеки сам ще си е банка и ще разполага със средствата си както желае без комисионни, с други думи той може да донесе свобода, непонятна на човечеството до този етап на развитие [1, 2, 3].

Биткойнът, както всяко нещо, си има положителни и отрицателни страни според възгледите на хората. Според привържениците на виртуалната валута той дава възможност за добро бъдеще, стига тази иновация да е по- бърза, сигурна и ефективна. Според други биткойнът може да направи всичко по-добре дори и от златото [1, 2, 3].

Противниците на виртуалната валута пък смятат, че ако всички започнат да го използват, то той ще остане в историята като разрушителя на долара. Това ще донесе и загуби на бизнеса. Има мнения, че цената му е неустойчиво висока. Бан-

кери пък смятат, че той е просто един балон и затова валутата трябва да има истинска стойност [1, 2, 3].

Първият ATM автомат за биткойни е изграден в Dubai Mall, OAE. На фиг.1 е показан първият имплементиран Bitcoin ATM автомат [5].



Фиг. 1. Първият Bitcoin ATM автомат в Dubai Mall, OAE

Най-известните софтуерни инструменти, с които могат да се „копаят“ биткойни, са:

- Bitcoin Miner;
- BTCMiner;
- CGMiner;
- BFGMiner;
- EasyMiner;
- RPC Miner и много други.

Трябва да се обърне и сериозно внимание на сигурността при получаване и продаването на биткойни. За тази трябва да се използва специален хардуерен криптовалутен портфейл, с който да се гарантира съхранението и трансфера на биткойни. На фиг. 2 е показано хардуерно криптовалутно устройство на компанията “Ledger” [4].



Фиг. 2. Хардуерен криптовалутен портфейл

3. Изводи

С развитието на технологиите, криптовалутите стават все по-популярни. Цената на биткойна зависи от търсенето и докато има разменна стойност той ще съществува. Тя ще нараства с оглед на все по-честата му употреба от все повече хора. За да бъде заличен е необходима глобална забрана, но тъй като той е децентрализирана валута няма кой да го забрани. Докато има хора, които да го ползват, ще го има и Биткойн.

Литература

1. <https://bitcoin.org/bg/you-need-to-know>.
2. <https://www.google.bg/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwi8tuiBsLnWAhWmQJoKHQ2FAUIQFghZMAQ&url=http%3A%2F%2Fhash.bg%2F%25D0%25BA%25D0%25B0%25D0%25BA%25D0%25B2%25D0%25BE-%25D0%25B5-%25D0%25B1%25D0%25B8%25D1%2582%25D0%25BA%25D0%25BE%25D0%25B9%25D0%25BD%2F&usg=AFQjCNE6iVGJCuD-k1nry0VIXBQdgwAOUg>.
3. <https://www.google.bg/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=0ahUKEwi8tuiBsLnWAhWmQJoKHQ2FAUIQFgh4MAk&url=https%3A%2F%2Fdariknews.bg%2Fnovini%2Fbylgariia%2Fkakvo-e-kriptovaluta-bitkojn-i-kakvo-mozhem-da-si-kupim-s-tiah-2049377&usg=AFQjCNErtJ-NBpZeGxPnnTk1TZWUH0QDbQ>.
4. <https://www.ledgerwallet.com/images/products/lens/ledger-nano-s-plug-medium.png>.
5. <https://twitter.com/bitcoinmena/status/445966642594336768>.
6. Hristov H., A modern survey on problems of business organization's security, Journal Scientific and Applied Research, vol. 7, 2015, pp. 72-80.

НЕТОРИЗИРАНО ПРИДОБИВАНЕ НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ ЧРЕЗ КИБЕРАТАКАТА PHISHING

Мерал М. Галиб, Христина Й. Косева

Шуменски университет „Епископ Константин Преславски”,
Факултет по технически науки, e-mail: meralmhmd@abv.bg, hristinai_@abv.bg

UNAUTHORIZED ACQUISITION OF CONFIDENTIAL INFORMATION THROUGH THE CYBER ATTACK PHISHING

Meral. M. Galib, Hristina I. Koseva

Abstract: In this paper unauthorized acquisition of confidential information through the cyber attack phishing is made. This paper also presents the modern way of information obtaining via special cyber attack with creation of fraud web sites.

Keywords: Computer networks, Cybercrime, Information security, Information technologies.

1. Увод

В днешни дни киберпрестъпленията се срещат все по- често. Това е причината да се полагат неимоверни усилия и огромни количества ресурси за гарантиране на киберсигурността, като се започне от огромни организации и корпорации и се стигне до обикновения потребител. Всяко едно киберпрестъпление струва милиарди долари в световен мащаб след щетите, които нанася. За да има защита и ограничаване на щетите от киберпрестъпленията се използват определени методи и технологии. Към днешна дата най- актуалните и мащабни киберпрестъпления са няколко на брой [1,2,3,4,5,6].

Компютърно престъпление е престъпление, което е свързано с компютъра или компютърната мрежа (най-често Интернет). В тези случаи компютърът е средство за извършване на злодеяние или целта на хакерите. Такива престъпления могат да застрашат както сигурността на нацията, така и финансовото здраве. Въпросите към тях са високо профилирани особено тези към хакерството, нарушените авторски права, детската порнография и прочие. Когато поверителна информация бъде разкрита, може да се стигне до проблеми, които вече са свързани с личната неприкосновеност на потребителя [1, 2, 3, 4, 5, 6].

2. Изложение

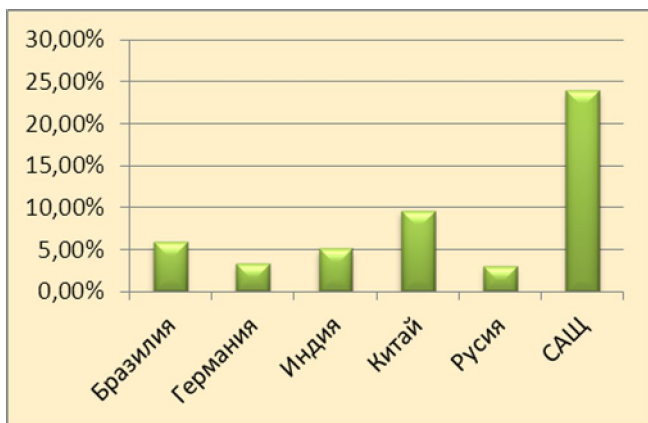
За интернет измамите се използва интернет услуга или софтуер с Интернет достъп за измама на потенциална жертва или придобиване на нещо определено за сметка на жертвата. Например, ако се открадне лична информация, това може да доведе до кражба на самоличност. Най- често се срещат измами чрез фалшив софтуер за сигурност. Потенциалните жертви се локализируют и чрез Интернет услуги-

те, които използват. Интернет измамите може да се появят в чат, уеб сайт, имейл, като една от най- разпространените измами е тази при покупката на даден предмет или услуга. Това става, когато сделката е свързана с транзакция на средства. Тогава злонамереният субект използва фалшиви средства, за да заплати, което най- често е с откраднати или фалшиви кредитни карти. По този начин продавачът не получава плащане по сделката и в резултат на това губи пари. Начините за осъществяване на този вид измами са много. Според целите, които са си поставили престъпниците има широк спектър от комбинации между тях. Две от най- разпространените и актуални техники са фишинг атаките и злонамереният софтуер- компютърен вирус [1, 2, 3, 4, 5, 6].

Фишинг атаката представлява възможността да се придобие чувствителна информация, която представлява потребителски имена, пароли и информация за кредитни карти. Най- често за целта се използва източник, който е маскиран като надежден в електронната комуникация. Името „фишинг“, на английски език „phishing“ - „зарибяване“, произлиза от английската дума „fishing“, означаваща риболов, защото изпращаните електронни съобщения са като „въдици“. Измамниците целят получателите да се „хванат“, като им върнат отговор, тъй като са неопитни и не добре информирани. За целта хакерите използват връзки, копиращи реални, популярни уеб сайтове, банки, онлайн терминали за плащане и най- вече в последно време се спекулира с имена на обществени институции с цел жертвите да бъдат привлечени. Най- често срещаната практика е фишинг имейлът да съдържа връзки в сайтове, заразени със злонамерен софтуер, което се извършва чрез фишинг имейл или обикновени съобщения. Тези съобщения насочват потребителя към фалшив уебсайт, който е почти идентичен с истинския [1, 2, 3, 4, 5, 6].

Според проучване на Symantec шестте страни с най- големи източници на киберпрестъпления са [1,2,3,4,5,6]:

- САЩ - 23.96% - според класацията на Symantec през 2015 г. САЩ са на второ място с 18.89% произлезли заплахи. През 2016 г. бележат 5% ръст. Те са на първо място заради зловредния софтуер Mirai, който е нов вид и плъзна по цял свят.
- Китай - 9.63% - това е вторият по големина източник на заплахи според Symantec.
- Бразилия – 5.84% - по данни на Symantec през последните 10 години киберпрестъпността значително расте.
- Индия – 5.11% - за разлика от други държави тя пада от трето през 2015г. до четвърто място през 2016 г.
- Германия – 3.35% - от осмо място през 2015 г. тя се изкачва до пето място през 2016г., когато хакери заразяват германската атомна електроцентра.
- Русия – 3.07% - според данните на Symantec през 2016 г. тя бележи значителен скок, той като през 2015 г. е била на единадесето място. Това е показано на фиг. 1.



Фиг. 1. Брой на проведените фишинг атаки в цял свят

Едни от най-често срещаните измами са свързани с имейлите. Този вид имейли служат за кражба на лични данни в интернет пространството- имена за достъп, пароли, сметки, адреси и т.н. В повечето случаи това се прави с цел потребителят да въведе лични данни, след което хакерът пренасочва потребителя към определена страница/телефон, където да го направи.

Фишинг имейлите имат най- различни форми [1, 2, 3, 4, 5, 6]:

- най- често те изглеждат, като електронни писма на институции или от сайтове на социални мрежи;
- могат да бъдат маскирани, като писма от някой, който потребителят познава. Такива фишинг атаки се наричат „spear phishing“;
- „телефонният фишинг“ – той представлява директно препращане към отдела за поддръжка, на който потребителят звъни, след като от него е изискано да проведе телефонно обаждане. Същевременно от другата страна чака хакерът, който взема ценна лична информация. Най- често хакерите правят това под предлог, че регистрацията на потребителя ще бъде прекратена или ще има проблеми с нея в бъдеще;
- не е изключено фишинг писмата да съдържат официално лого или отличителни знаци, взети от законни интернет сайтове. Често пъти те съдържат и убедителна информация за потребителя, която хакерът е намерил в социалните мрежи [1, 2, 3, 4, 5, 6].

Фишинг атаките стават все по- чести, което непрекъснато увеличава броя им. Въпреки мерките за безопасност, които се предприемат при електронното банкиране и онлайн търговията, работна група за борба с фишинга подготвя списък с полезни съвети, за да не стане потребителят жертва на този вид измами. Някои от тях са [1, 2, 3, 4, 5, 6]:

- Обръщане на особено внимание към всяко съобщение, изискващо лични данни:
 - няма гаранция, че дадено съобщение не е фалшиво освен ако не носи електронен сертификат за индентичност;

- хакерите често си служат с лъжливи твърдения, провокирайки незабавни отговори, за да получат необходимите лични данни;
- обикновено фишинг имейлите не са предвидени за конкретен човек, но и това може да се случи;
- при подозрение, че съобщението е фалшиво не се препоръчва да се използват линкове към други страници в имейли;
- информацията, която съдържа в себе си данни за кредитни карти и сметки се предава само на уеб сайтове със сигурна връзка;
- препоръчително е потребителят да има инсталирана лента с инструменти за браузъра си, която спомага борбата с фишинг сайтовете;
- наложително е редовното онлайн проверяване на сметки;
- редовно обновяване на уеб браузъра, с цел инсталиране на обновлението за сигурност;
- при наличие на фишинг измама е необходимо да се докладва до съответните органи [1, 2, 3, 4, 5, 6].

3. Изводи

Въпреки неимоверните усилия за борба с фишинг атаките, както и мерките, които правителства, компании и обикновеният потребител предприемат, броят на кибератаките непрестанно расте. Достигането на абсолютна сигурност практически е невъзможно, но все пак се полагат огромни усилия за изграждането на защитни механизми, които да бъдат в полза, както на големи организации, така и на обикновения потребител. Чрез създадените механизми и най-вече с повече бдителност рискът към посегателства върху личното киберпространство може да се намали, което от своя страна ще доведе до ограничаване на щетите от извършваните киберпрестъпления.

Литература

1. <https://www.expert.bg/bizbuzz/6-te-dyrzhavi-v-sveta-ot-koito-trygvat-naj-mnogo-kiberataki--611528.html>.
2. http://computerworld.bg/41911_s_evolyuciyata_na_tehnologiite_evolyuirat_i_instrumentite_i_metodite_zakiberataka.
3. https://www.google.bg/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj-uoC_qrvWAhVFCpoKHSaPCGcQFggmMAA&url=http%3A%2F%2Fwww.investor.bg%2Fnovini%2F261%2Fa%2Fbumyt-na-fishing-i-farming-atakite-i-kak-da-se-predpazim-218957%2F&usg=AFQjCNF5ogZyVwiqfdUh8yCM5vzTh4OH_Q.
4. https://www.google.bg/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwIU25PT47vWAhUoQpoKHZTeAcgQFggmMAA&url=http%3A%2F%2Febox.nbu.bg%2Fsec16%2Fpdf%2F51.pdf&usg=AFQjCNENfCPwkdOHry5D3sfxID0QFb_yFw.
5. <http://www.cybercrime.bg/bg/internet/e19df9/>.
6. Hristov H., A modern survey on problems of business organization's security, Journal Scientific and Applied Research, vol. 7, 2015, pp. 72-80.

В. Д. Делев
**ЕНЕРГИЙНАТА СИСТЕМА КАТО КОМПОНЕНТ
НА НАЦИОНАЛНАТА СИГУРНОСТ**

Видьо Д. Делев

*Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” – гр. Шумен*

ENERGY SECURITY AS A PART OF THE NATIONAL SECURITY

Vidyo D. Delev

E-mail: vidyo.delev@abv.bg

Abstract: *In recent years the people are debating a lot about the energy security, energy resources and their use for the future. This report considers the energy problems in our society and the way to prevent them in our days.*

Keywords: *energetic, security, energy, threat, problems.*

Увод:

Националната сигурност изгражда за обществото, състояние при което са защитени основните права на гражданите – гарантирано е резултатно благосъстояние и устройване на държавата. В частност енергетиката като важен социално-икономически отрасъл и пряко свързана със сигурността на държавата, възпира фатални кризисни ситуации. Всяка една съвременна енергийна система – национална, регионална или континентална – е базирана на концепцията за разнообразието - от енергийни източници, както и от видове енергия. Енергията е била винаги стратегически ресурс и разнообразяване на енергийното портфолио винаги е означавало търсене на благоприятен стратегически баланс. След изпадането на Западна Европа в още по - дълбока зависимост от енергийните ресурси на Близкия изток, отрицателни демографски и политически ефекти, след 1973 г. се наложи търсене на диверсификация. Друг източник за диверсификация на енергията се осигурява от новооткритите маршрути за доставка на петрол и газ от Каспийския и Централно азиатския басейни. Петролопроводът Баку – Тбилиси - Джейхан (БТД) е първият източник на каспийска енергия предоставена до прага на Европа.

Изложение:

Енергетиката е един от основните елементи на НТП, а също така има и важно районоорганизиращо значение, т.е. разположението на предприятията на енергетиката дава отражение върху териториалната структура на националното стопанство. Тя включва добива на енергийни суровини, производството, пренасянето и трансформирането на електроенергията. България трябва да се стреми към енергийна независимост, като диверсифицира източниците и доставчиците на енергия и увеличи енергийните запаси.

Като част от енергийната система, ядрената енергия трябва да се контролира, така че използването ѝ за мирни цели да не се превръща в конфликтна точка, засягаща пряко националната сигурност на една държава.

Възобновяемите енергийни източници са добър отговор на настоящите и бъдещи енергийни предизвикателства в световен мащаб, като сигурност на енергийните доставки и глобално затопляне. Използването на потенциала на вятъра, слънцето, биомасата, биогоривата и водородните технологии ще намали количеството на изхвърлени въглеродни емисии в атмосферата и ще осигури на страната ни енергийна независимост и алтернативни

Националната политика за енергийна сигурност има няколко основни елемента:

1. Стабилността на енергетиката като постоянен процес по предоставяне на жизненонеобходимите обществени услуги за функциониране на обществото като цяло в условията на възможни терористични заплахи, природни бедствия и значими промишлени аварии заема съществено място в осигуряването на националната сигурност.

2. Република България е заинтересувана от изграждането на обща енергийна политика на ЕС. Тя подкрепя реализирането на стратегическите инициативи на ЕС за изграждане на необходимата инфраструктура и разнообразяване на енергийните доставки. Инициативите се осъществяват чрез действащата система за финансиране и въвеждането на нови и по-ефикасни финансови инструменти, от които приоритетно могат да се възползват страните от Югоизточна Европа предвид високата зависимост от един източник и незадоволителната енергийна инфраструктура.

3. Приоритет за гарантиране на енергийната ни сигурност е изграждането и поддържането на междусистемни връзки с мрежите на съседни държави, както и разширяване капацитета на газови хранилища.

4. Република България подкрепя развитието на международните енергийни проекти в рамките на "Южен коридор", на първо място сред които е проектът НАБУКО, който е приоритет на ЕС. Подкрепяме и международния енергиен проект "Южен поток". Осъществяването им се съпровожда с експертиза за сигурност – гражданска, обществена, екологична и национална.

5. Развитието на ядрената енергетика има стратегическо значение за националната ни сигурност. При развитието ѝ стриктно се спазват изискванията за управление на ядрените отпадъци и извеждане от експлоатация и мерките за сигурност.

6. Приоритет в политиката за енергийна сигурност е повишаване на енергийната ефективност и насърчаване на енергоспестяването. Република България си поставя за цел значително намаляване на енергийния интензитет на брутния вътрешен продукт чрез подпомагане на политики, насочени към финансово стимулиране на енергийната ефективност, развитие на пазара на енергоефективни продукти и услуги, прилагане на регулаторни мерки и други механизми.

7. Енергийната сигурност на страната и повишаването на качеството на околната среда зависят от реализирането на политиката на Република България за увеличаване на дела на енергопроизводството на възобновяеми и алтернативни енергийни източници и заместването на електрическата енергия с природен газ.

8. Страната съдейства за технологичното развитие по отношение на ефективността на производството и внедряването на чисти въглични технологии, както и

за прилагането на технологични постижения, които са в съответствие с европейските изисквания и собствените икономически възможности.

9. Енергийната ни политика се основава на балансиран подход при комплексното използване на възобновяеми енергийни източници, ядрена енергия, природен газ, въглищни технологии и ВЕЦ за гарантиране на енергийната сигурност и икономическата ефективност.

10. Република България провежда ясна и последователна регулаторна политика за гарантиране интересите на националната сигурност, обществото и гражданите при функциониране и развитие на енергийните мощности, на преносната и разпределителните мрежи.

11. Изграждането на значимите енергийни проекти изисква както експертиза за влиянието върху националната сигурност, така и екологична оценка и оценка за съвместимост с предмета и целите за опазване на защитените зони, за гарантиране сигурността на гражданите, обществото и държавата.

12. Ресурсното управление на енергийната сигурност придобива първостепенно значение. Управлението на ресурсите е част от стратегията за предотвратяване на кризисни ситуации и условие за надеждно функциониране на ключовата и критичната инфраструктура: енергийна, транспортна, комуникационна и информационна.

13. Република България изпълнява ангажиментите по Директивата за защитата на европейската и националната критична инфраструктура, което включва задължително възможности за съвместна дейност между публичния и частния сектор, базирани на взаимен интерес и експертни умения на партньорите за гарантиране защитата на обществените интереси и потребности чрез ефективно разпределение на средствата, рисковете и ползите в този процес.

Заклучение:

Именно на базата на този анализ най-добре се вижда, че единственият вариант за достигане на енергийна сигурност в страната, а оттук и укрепване на националната сигурност е и изпълнението на заложената в енергийната стратегия на България до 2020 година задача за оказване на институционална подкрепа и мониторинг на проекти със стратегическо значение за енергийната сигурност, в т.ч. на инвеститори в нови централи (необходими за балансиране на производството от вятърните и соларните централи), както и на нова ядрена мощност като проект с преобладаващо участие на чужди инвеститори.

Литература :

1. СТРАТЕГИЯ ЗА НАЦИОНАЛНА СИГУРНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ
- 2.. ЕНЕРГИЙНА СТРАТЕГИЯ НА РЕПУБЛИКА БЪЛГАРИЯ ДО 2020 г..
3. http://europa.eu/rapid/press-release_IP-14-606_bg.htm
4. <http://www.csd.bg/?id=1360>
5. <http://www.nato.int/docu/review/2012/Food-Water-Energy/Energy-Security-NATO/BG/index.htm>

МЕТОДИ ЗА ПРЕВЕНЦИЯ НА ТЕРОРИЗМА В НАШИ ДНИ

Видьо Д. Делев

*Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” – гр. Шумен*

METHODS OF PREVENTION OF THE TERRORISM IN OUR DAYS

Vidyo. D. Delev

E-mail: vidyo.delev@abv.bg

Abstract: This report reveals some of the modern concepts of terrorism and anti – terrorism. There are analysis which improve a new directions to cope with it by using different resources.

Keywords: security, terrorism, conflicts, problems, influence.

1. Увод

Измененията в стратегическата среда за сигурност през ХХІ век изведоха световния тероризъм, който разпали множество огнища на национални конфликти с ниска интензивност, като един от най-актуалните проблеми за човечеството след края на Студената война и вече е на първо място в йерархията на заплахите от глобален мащаб.

Актуалността на темата и разглежданите проблеми се дефинират от това, че именно тероризмът на съвременния етап е една от най-големите заплахи за сигурността на всяка държава по света, а разглеждайки проблема в контекста на последните събития в Република България, актуалността е реална, защото бежанският поток за страната ни и масовото навлизане на сирийски граждани създава опасност за националната сигурност основно в три аспекта:

- икономически натиск върху бюджета;
- интеграционния проблем;
- възможност за инфилтриране на криминален контингент и терористи на територията на страната.

Република България поради своето геостратегическо разположение на Балканския полуостров е застрашена от реална терористична опасност, което повишава изискванията за готовност за провеждане на съвместни или национални мероприятия за борба с тероризма. Определените национални сили за борба с тероризма трябва да са с висока степен на окомплектованост, готовност и подготовка, да са снабдени със съвременни оръжия и специална екипировка и да се изграждат така, че да са напълно съвместими със силите на НАТО.

2. Изложение

Няма единно и универсално определение за тероризма.

Според тълковният речник той е “политика или дейност, при която целите се постигат чрез терор”. Понятието тероризъм произлиза от латинската дума “terere”, което значи “всявам страх”.

Според експерти тероризмът е предумишлено насилие, което е политически мотивирано срещу групи или лица с цел печелене на влияние или въздействие върху държавно решение.

На съвременния етап тероризмът започва да се отъждествява със стремежа за постигане на политически цели чрез насилие, заплахи върху обществото и държавата, и масови убийства на цивилни граждани.

Основна причина за възникване на съвременния тероризъм е отхвърляне на съществуващата политическа система, определени политически личности или политически решения.

За постигането на тези политически цели се цели създаване на хаос и дезорганизация в държавните органи и органите за националната сигурност. Търси се максимално влошаване на положението, за да се искат коренно различни нови политически решения и управление.

Политическият мотив може да бъде прикрита икономическа причина, като в сърцевината на проблема стои икономическото състояние и качеството на живот.

Другите причини са: слабо развитото здравеопазване, влошената околна среда, престъпността и несигурността в държавата, лошите битови условия за живот и липса на социална система за подпомагане.

Основните фактори за генериране на съвременния тероризъм са и:

- наложения нов геостратегически световен ред;
- агресивното поведение на определени индивиди;
- религиозната и етническа непримиримост.

На съвременния етап се открояват няколко тенденции в развитието на тероризма, като някои основни от тях са:

- тероризмът започва да придобива глобално значение, като се превръща от отделен регионален проблем в проблем на международната и световна сигурност;
- променя се съотношението, като все повече нараства броя на терористичните групи, действащи на религиозна основа спрямо тези, действащи на политическа основа;
- нараства броят на ранените и загиналите в терористичните актове, като през 2001 г. те са най-много: загинали 3295 и 2283 ранени;
- неравномерно разпределение на терористичните актове по света, но истинските цели са развитите страни;
- наличие на две основни форми – индивидуален и организиран тероризъм с тенденция за засилване на единичните прояви на тероризъм;
- насочване вниманието към оръжията за масово унищожение, информационните технологии, екологията и по-мощните средства за въздействие, което е изключително опасно за световната сигурност;

- най-често използваните методи в тактиката на терористичните организации са: убийство, самоубийствени атентати, бомбена експлозия, вземане на заложници и шантаж;

- повишаване нивото на подготовка на терористите чрез провеждане на специално обучение в създадени за целта училища;

Пример за това днес е групировката „Ислямска държава“ в Ирак и „Леванта“, свързана с „Ал Кайда“;

- организиране на терористични актове от малка група, а резултатите може да са стратегически и политически;

- липса на морални задръжки и участие на хора с различна култура, религия и образование по финансови причини.

Събирането и анализирането на информация от **военното разузнаване и агентурните мрежи** се смята за едно от най-важните задачи за антитероризма с военни средства. Трябва да отбележим значението на използване на информацията и взаимодействието с военното разузнаване. Трябва да отбележим и спецификата на проблема, а именно че информацията за подготовка на терористичен акт се добива много трудно и никога не може да се твърди безусловно, че е вярна.

Важно за антитероризма е **прекъсване на финансирането** на тероризма, една сложна задача, защото е трудно проследяването на паричните потоци, които постепенно преминават от отделни държави спонсори към добре прикрити частни корпорации и фирми.

От особено значение е провеждането на **психологически операции** и осигуряването на постоянен контакт с местното население.

Асиметричността в цялостната дейност на терористичните организации често води до това, че действията срещу него да са отговарящи и много рядко успешно превантивни.

Концепцията на НАТО за борба с тероризма е публикация на Военния комитет на съюза „МС-427“ от 2002 г. и развива способности в четири основни направления:

- Антитероризъм (antiterrorism /at/);
- Ликвидиране на последствията (consequence managements/cm/);
- Контратероризъм (counter terrorism/ct/);
- Военно сътрудничество (military cooperation /milsop/).

Актуално за борбата с тероризма на съвременния етап е наличие на две основни условия за постигане на успех:

- премахване на причините, които пораждат тероризма;
- извършване на превенция на тероризма.

Изследвайки същността на „мрежите на насилие“ откриваме, че действията на една такава мрежа са свързани с някои признаци. Успеем ли да ги идентифицираме или да нарушим механизмите за функционирането им, ще имаме успех. Някои от тези признаци са:

- прикрити връзки между отделни социални групи, откриваеми косвено, чрез анализ на финансови, политически и криминални прояви;
- покупки на оръжие или взривни вещества;
- неочаквани парични преводи и пратки от материални средства;
- нелегална имиграция и бежански потоци;
- контрабанда и нарушаване на обществения ред.

Следващо направление за превенция е **разузнаването**, което включва събиране и анализиране на всички видове информация.

Информацията за тероризма се добива трудно, тя е спорна и често непълна, затова от изключително значение е взаимодействието между всички елементи от националната сигурност за добиване на актуална и достоверна такава. Единствено комплексният подход и обединените усилия, които са добре ръководени и координирани ще имат успех.

Следващо направление е въздействие върху средата, пораждаща тероризма.

Нарастващата диспропорция в света, задълбочаваща разделението на бедни и богати е очевидна, другото разделение е на държави, имащи сигурност, сила и технологии и такива, които нямат такава.

Важно направление е подготовката на кадри и осигуряване на необходимото оборудване. Важността на това направление се определя от това, че човешкият фактор е решаващ за всяко едно противоборство.

Следващо направление за превенция на тероризма е „мрежите за сигурност“ синергично да обединяват усилията на съдебните, административните, политическите, икономическите законодателните и други субекти с цел опазване на националната сигурност и борбата с тероризма. Сътрудничеството трябва да е на такова ниво, което да повишава сигурността на всеки член от обществото и на държавата, като цяло. Критичен фактор тук е намирането на точен баланс между наблюдаемост и управляемост, контрола върху тях и информационно обработващите процеси в тях.

На съвременния етап буквално в днешния ден за Република България е важно полагане на усилия за бързо интегриране на емигрантите които са вече в страната ни, полагане на големи усилия за подобряване на техния материален, обществен и психологически статус. Ще бъде пагубно за националната ни сигурност да се допусне отчуждаване, затваряне и изолиране на това население, което може да доведе до междуличностни и расистки конфликти.

Разгледаните направления за превенция на тероризма показват, че само всеобхватният подход би донесъл успех след обединяване усилията на институциите за национална сигурност и обществото.

3. Заключение

Човечеството в днешния ден е изправено пред едно ново предизвикателство - тероризма, новия вид световна война, която се възползва от всички преимущества на съвременните технологии и прилага нетрадиционни асиметрични стратегии и тактики, които могат с отделни дори тактически действия да доведат до стратегически ефекти.

Обединените усилия на международната общност и провежданата глобална политика е необходимо да способстват за подобряване на средата за живот на хората по целия свят, да намаляват огромната пропаст между развитите цивилизации и бедните народи, което е една от основните предпоставки, генериращи тероризма на съвременния етап.

За да е ефективна борбата с тероризма трябва да се прилага комплексния подход, който да е плод на обединените усилия и сътрудничество в международен и национален план на демократичната общност.

Гъвкавостта на терористичните организации и тяхната бърза адаптивност към

новите условия на война изискват непрекъснато формиране, развитие и усъвършенстване на теоретичните постановки, нормативната база и всички направления за превенция на тероризма.

Изучаване на особеностите за възникване и развитие на тероризма и на международния опит в борбата срещу проявленията му ще създадат нови възможности за предприемане на адекватни мерки на национално ниво за превенция, за гарантиране на националната сигурност и утвърждаване на международен авторитет.

Литература :

1. www.geopolitika.eu/.../839 – asimetrichniyat – harakter - na-savremennite - konflikti. (24.11.2013 г.,15.40 часа)
2. Слатински,Н., Борбата с тероризма - предизвикателство за демократичните държави. сп.“Международни отношения“, № 1-2,стр.119-132.

К. М. Желев,
ТРАФИК НА ХОРА

Калоян М. Желев

*Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” – гр. Шумен*

HUMAN TRAFFICKING

Kaloyan M. Zhelev

E-mail : kokolincho@abv.bg

Abstract: *The globalising world hides a countless number of threats and the one we will focus on is human trafficking. This is a problem that concerns a big number of individuals despite their gender, age or residence and it is closely related to their safety.*

Keywords: *trafficking, types of human trafficking, victims, traffickers.*

1. Увод

Трафикът на хора е мащабно явление и за да стане ясно какво точно означава според източниците трябва да се раздели на три етапа. Първият етап разпознава трафика като изключително значим и на него започва да се обръща внимание по сериозно през XX век. Вторият етап обхваща 40-те години на XX век след най-голямата в историята на човечеството война, света се променя въвеждат се нови закони и законови актове, което засяга и разглеждания от нас трафик на хора. Третият етап е същинския етап и в него се включват различни протоколи които противодействат в пълна сила срещу трафика. Акцентира се върху различни случаи които доказват това престъпление и по този начин към протоколите се добавят нови наказателни точки които още по силно да наказват извършителите.

Трафикът на хора най-накратко може да се нарече процес при който един индивид или група от индивиди се въвеждат в положение за което не са съгласни и е против основните човешки права. Индивидите са принудени да участват без своето съгласие и да изпълняват целите на трафика. В това явление влизат различни обществени отношения и най-често се обхваща неприкосновеността на личността или пък личната свобода, която по принцип имаме за даденост, но във въпросните обстоятелства тя се отнема. Успоредно с трафикът на наркотици и оръжия на трето място се нарежда трафикът на хора.

2. Видове трафик на хора

Има много класации, които разглеждат различни видове трафик, но ще разгледаме по подробно трите основни вида: национален, международен и експлоатационен.

Започваме с националния който се организира на определена територия. В него се включват набирането, транспортирането, укриването и приемането на пострадалите. Набирането като понятие означава активна дейност която е средоточена към това да убеждава в някаква истина. Транспортирането от своя страна е прекарването на жертвата от едно място на друго лично от самия трафикант или от лице

част от групировката. Укриването е важна част от цялата дейност, защото са нужни много средства и посредници, а главната цел е жертвата да бъде в неизвестност от своите близки и органи на реда.

Международният трафик е престъпление с международен елемент и се характеризира с това, че държавата на произхода и държавата на експлатацията на жертвата се различават. Последствието от международния трафик е преместването на жертвата в пространството в което участват два предмета които са: самата жертва и границата която пресича. Именно затова в сравнение с вътрешния трафик, международния се нарича престъпление с два предмета.

Третият вид трафик който ще разгледаме е експлатациония. Този трафик е един от най-новите и може да се каже, че е доста нов за системата не само за България, но и на световно ниво. Този вид трафик представлява желанието на извършителя да използва жертвата, за да извлече било то материална или нематериална облага. Дееците не се интересуват от желанието на жертвата, а правят всичко възможно, за да постигнат желаната цел.

3. Цели на трафика на хора

Трафикът на хора има няколко цели и ще изброим и опишем някои от тях на които акцентират повечето източници, а те са: развратни действия, принудителен труд, принудително подчинение, отнемане на телесни органи, продажба на деца

Експлатацията с цел развратни действия е свързана с нарушаване на половата свобода и неприкосновеността на жертвата. Такъв вид трафик има за жертви предимно жени и при него се създават условия които включват съвкупление на жертвата с дееца или трето лице.

Целта, която сме посочили на второ място е принудителния труд. При този вид трафик, трафикантът принуждава жертвата в повечето случаи по зверски начин да извършва трудова дейност без значение от нейната сложност и чрез това нарушава всички правила на трудовия кодекс.

Принудителното подчинение представлява принуждаване на жертвата да извърши определено деяние, за което не е съгласна и е в разрез с волята ѝ. При такъв вид трафик жертвата превива на места съгласно чужда воля. Принудителното подчинение не дава на поробения възможност да прекрати цялото това действие и тук всичко зависи от интересите и целите на извършителя.

Последната цел, но не на последно място е търговията с новородени деца. Това тежко престъпление е свързано с новородените деца и тяхната продажба в сивия сектор, а извършителите много рядко биват залавяни. Процесът който обясняваме е жесток по своята същност и отнема дълъг период от време и въпреки това престъплението трудно се разкрива навреме. Новороденото дете се отнема от майката и се дава на други родители срещу заплащане.

4. Разграничаване на трафика на хора от други престъпления

4.1. Трафик на хора и сводничеството

Предизвикателство за всеки разследващ е да разграничи сводничеството от трафика на хора, защото в повечето случаи двете са свързани или доказателствата за разграничаване са твърде малко или липсват. Факт е, че липсва ясна граница, но това става често срещано явление и съдебната практика описва всичко това, което от своя страна е добре, защото опита става по-голям и дори малко разграничението се забелязва. Често обаче извършителите отвлечат жертвите си като ги използват за развратни дейности при което се експлатира е проституирането на засегнатите

като в по-голяма си част това са жени. На базата нажаплетените разледвания които са свързани с трафика на хора се заключава, че трафика всъщност поглъща сводничеството. Според други случаи от действителността двете престъпления са алтернативи или се намират в съвкупност.

4.2. Трафик на хора и престъпно прибиране на малолетен

Престъпното задържане на малолетни в чести случаи служи за изнудване и поставяне на изнудения в състояние на безисходица. Това престъпление се състои от два акта познати на съдебната практика. Първият акт е самото задържане на жертвата в случая малотен индивид. Тук може да включим постоянния контакт на малотния с извършителя. Вторият акт е необявяването от престъпника за местонахождението на жертвата като от този момент престъплението става факт.

4.3. Трафик на хора и потребление на детска проституция

Криминализирането на този вид проституция е голям напредък за съдебните органи, защото това прави възможно залавянето на много от извършителите на тези деяния. Случаите на детска проституция започват да стават чести. В този глобален свят много от границите са отворени и това прави трафика на децата използвани за такъв вид дейност по лесно за извършителите. Законът съди жестоко хора занимаващи се с такава дейност, но залавянето ѝ си остава също толкова трудно.

5. Жертви

Трафикът на хора е насочено срещу личната свобода и интереси на определения индивид. Това явление засяга най-висшите права на човека. Жертвите не се подбират по имена или възраст. Жертвите могат да бъдат от всички полове. Напрежението което дееците упражняват върху жертвите е огромно с цел те да се пречупят и да изпълняват само това което кажат. Често измъкнали се от трафика страдат от различни психически разстройства и преживяването остава следа до края на живота им. Социологически изследвания показват, че най-честите жертви са жени между седемдесет и двадесет и четири години като това са жени които не са завършили средно образование или пък са имали трудно детство. Жертвите са хора отблъснати по някакъв начин от обществото или стоят, ако може така се изразим в периферията на обществото, защото най-често такива хора нямат близки на които да разчитат или пък имат, но са далеч от жертвите.

6. Извършители

Тези обекти от пъзела са по силната страна в трафика и според специализираната литература и многобройни проучвания на хора занимаващи се с тази дейност данните за тях са оскъдни. Това което се знае със сигурност е, че експлататорите в 99% от случаите са мъже. Трафикантите не е задължително да членуват в някаква организация. В повечето случаи това са отделни личности с обособени цели. В по-разширени доклади се наблюдава участието на национални и транснационални групировки, които действат във всяка част на света. Извършителите са жестоки и безкруполни във всяко едно отношение и не се интересуват от мнението на жертвата. Не познават морала и уважението към себеподобните си, а търсят само лична изгода в много от случаите тя е финансова, защото в този глобален свят парите са водещи и всички се стремят към тяхното печелене. От този тип дейност извършителите печелят големи суми за сметка на много невинни животи.

7. Въпросът за трафика на хора в България

България е една от малките страни в Югоизточна Европа, но независимо от това трафика обхваща и нейните територии. По данни, България дори се намира на

едно от първите места по сексуална експлоатация на хора. Както добре знаем България има стратегическо географско положение, което привлича извършителите на подобни дейности. В България няма точно определен регистър които да посочва подробно случаите на трафик. Всичко, което се знае е на базата на проучвания от различни фондации, национални служби и други. Всяка една организация която осигурява данни го прави на базата на случай които е разкрива самата тя. Регионалните центрове по трафик на хора отчитат прогнози като една от тях е, че трафика вече по-малко се насочва към Югоизточна Европа. Много от организациите в страната не могат да вземат участие в пълна сила, защото или информацията е малко, или са възпираны от всякакъв вид институционални разпоредби свързани с предаване на информацията. По данни в България се наблюдават интересни характеристики 22.5 на сто през 2003 г. и 23.8 на сто през 2004 г. са жени над 26 години докато използването на непълнолетни за какъвто и да било трафик е сравнително малко. Жертвите на трафика в страната са предимно от малцинствата, защото те по-лесно биха били прилъганы. При малцинствата в България в частност ромското има различни традиции като уредени бракове и това може да се пресече с дейности по трафика и лесно да бъдат обвъркани.

Голяма част от случаите които засягат български граждани са разкрити по няколко известни начини. Първият и познат на всички начин са посолствата в тях жертвите намират убежище, а обучените специалисти по разпознаване и консултация са винаги готови да подадат ръка. Следващият механизъм са органите на реда. Те дават желаната сигурност на хора пострадали от подобна експлоатация и правят всичко възможно да върнат българските лица в страната.

Третият и не на последно място ефективен начин е завръщането след екстрадиция. Полицейските органи са добре запознати и обучени да действат в такива условия, действат адекватно и усета към потенциалните жертви е много засилен. Доста жертви предимно жени са били идентифицирани по този механизъм, целта на които е да предложи помощ.

Заклучение

Трафикът на хора е индустрия с милиони печални годишно, а жертвите са многобройни. Организираната престъпност се занимава с тази дейност и тя е сравнително безнаказана.

Трафикът на хора може да бъде определено като явление което е старо, но в същото това време и ново. Това деяние не е обикновено престъпление, то може да се каже, че е отношението на едно човешко същество към друго. Съвременният свят е изпълнен с много напрежение и трафика на хора е проявление което е резултат от това напрежение. Във всеки един случай на трафик на хора жертвата не избира да бъде експлатирана, а насилствено е използвана. Тя се намира в положение от което трудно може да излезе.

Литература:

1. Христо Попов. Издателска къща ЛИК София, 2007. Трафик на жени (причини, последствия и противодействия), 9 ст., 151- 153 ст.
2. Ива Пушкарлова. Сиби София, 2012. Трафик на хора (проблеми на наказателноправния режим), 11 ст., 40-65 ст.,157 ст., 191 ст.
3. http://www.veto.fyc-vidin.org/docs/trafik-general_info.pdf 25.09.2017 г

К. М. Желев

ВОДОИЗТОЧНИЦИТЕ КАТО ИЗТОЧНИК НА ЗАПЛАХА ЗА ЕКОЛОГИЧНАТА СИГУРНОСТ

Калоян М. Желев

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” – гр. Шумен

WATER SOURCES AS A SOURCE OF THREAT TO ENVIRONMENTAL SECURITY

Kaloyan M. Zhelev

E-mail: kokolincho@abv.bg

Abstract: *The water. One of the most important sources of life on the planet .It is vital for humans as well as for plants, animals, for the whole of nature. Without water the existence of life is impossible. It is the most valuable natural resource and has an important role in all ecosystems.*

The report that I will present will address the pollution of water and sources of water pollution and their classification. I will set out opportunities to solve environmental problems with water pollution.

Keywords: *environment, pollution, water.*

Увод

Водата. Един от най важните източници за живот на планетата.Тя е жизнено важна както за хората , така и за растения , животни , изобщо за цялата природа.Без вода съществуването на живот е невъзможен.Тя е най – ценният природен ресурс , и има важна роля във всички екосистеми.Замърсяването на водоизточниците може да доведе до сериозни последствия.Хората се нуждаят от сравнително малко вода за пиене , но водата е жизнено важна за съществуването им.По – голям процент от водата която се използва е предназначена за селското стопанство и промишлеността.Недостигът на сладка вода непрекъснато нараства.Около 1/3 от населението изпитва недостиг от питейна вода и причините за това са следните.

1. Населението нараства , а също се увеличава и развитието на отраслите който употребяват много вода.

2. Глобалното затопляне е също фактор който е от огромна роля за това , да се намалат дебитите на реките.

3. Прогресивно се замърсяват водоемите от промишлените предприятия , битови отпадъци и други отпадни води.

Като това води до нарастване и застрашаване на живота на хората и нарушаването на екосистемите.

Изложение

Под замърсяване на водите , повърхностни и подпочвени се има в предвид най – общо , неблагоприятното въздействие което човек и извършваната от него стопанска дейност действа върху състава на водата.Това ограничава използването на водата за цели за които тя е нужна в чисто състояние. Основния замърсител на водата е човекът. Водата в промишлените зони на големите градове е силно замърсена, поради изливането на голямо количество химикали в водните басейни. Най-много замърсяват предприятия в които водата се използва като средство за охлаждане ,филтриране или разреждане.Има 3 вида категории за използване на водата :

I категория – Водите могат да се използват за питейно битови нужди , във хранителната промишленост и в други промишлености изискващи ползването на вода с питейни качества.

II категория – Водите се използват за рибовъдство , културни и декоративни нужди .

III категория – Тези води се ползват за напояване и във селското стопанство , също и за промишлени нужди .

Източници на замърсяване на водите

Замърсителите на водата се класифицират като химични , биологични и физични.

Химичните замърсители са най-разпространени . Химичното замърсяване е най – устойчиво и трудно за преодоляване , като то се разпространява на най – големи разстояния.То бива органично и неорганично и се дели на токсично и нетоксично.

Органичното замърсяване на водата е свързано със попадане във водоизточниците и водоемите на органични вещества .Те постъпват там от битовите , селскостопанските или промишлените води.Такива вещества са именно нефт и всички нефтопродукти.Замърсяването с нефтени продукти е причинено от неволно разливане на петролни продукти във водата. Това се случва най-често когато някой танкер потъне или някъде стане катастрофа с цистерна в която има бензин или нафта. Резултатите са пагубни както за флората и фауната така и за човека. Както знаем нефтените продукти са силно токсични и при попадането във водата те я отравят и всички организми страдат от това.

Замърсяването с пестициди и изкуствени торове се дължи на целенасочената дейност на човека. Пестицидите представляват органични съединения, които трябва да предпазват селскостопанската реколта от паразити или да стимулират растежа на реколтата. Но тези вещества не са вредни само за паразитите а и за човека. Пръскането с такива препарати замърсява както почвата така и водата. Живите организми се отравят, а чрез подпочвените води пестицидите достигат и до водните басейни.Други такива органични вещества които замърсяват водата са от : кожарската промишленост, млекопреработващата, целулозната и др. Неорганичното замърсяване е свързано със постъпването във водата на минерални вещества, химични съединение и токсични вещества. Най-голям процент от такива замърсители идват от предприятията на металургичната , машиностроителната , рудо-, въгледобивната промишленост, заводите за производство на строителни материали и торове , и дърводобивната промишленост. Замърсяването с тежки метали се състои в отлагането на метали в водата. Това се причинява от металургичните комбинати. Последствията не са толкова фатални, но могат да доведат до отлагане на тежки метали в кръвта или във вътрешните органи на човека на животно или растение.

Физичното замърсяване на водата е свързано с наличието на радиоактивни вещества и топлина. Те са много опасни и попадат във водоизточниците като предизвикват радиоактивно замърсяване. Източниците от които биват изхвърляни тези замърсители са АЕЦ, болнични заведения, предприятия които работят с радиоактивни материали, също и от въоръжените сили. Топлината също е един от замърсителите на водите, тя загрява производствените води, които след това стават отпадни. Има два вида топлинно замърсяване изкуствено и естествено. Изкуственото затопляне се получава от промишлеността и при добив на електроенергия от – ТЕЦ и АЕЦ. Естественото топлинно замърсяване се дължи на големите горещини. Биологичното замърсяване се среща под влиянието на различни бактерии, вируси, гъбички и паразити във водоизточниците, те попадат в питейната вода от канализационните води и животновъдните фирми, като причиняват хепатит дизентерия, коремна тиф и други болести. Във водата попадат и яйца и ларви на червеи които се паразитират в храносмилателната система на човека. Микроорганизмите имат способността да се запазват за дълго време във отпадните води а в някои случаи и да се размножават. С някои от тях е възможно да се заразят и водните обитатели от където е възможно да попаднат отново в човешкия организъм. Епидемии от такъв характер са особено характерни за бедните страни от третия свят. Там са разпространени такива заболявания, които в развитите страни отдавна са забравени и не са проблем. Поради високото замърсяване на водите от различни източници, липса на пречиствателни съоръжения, бедността, липсата на хигиенни навици и познания у населението там са често срещани заболявания като коремния тиф например. Попадайки в питейната вода, тези вируси могат да доведат много лесно до възникването на различни епидемии и да се разпространят много лесно на много голямо разстояние заради начина, по който те попадат в битовите помещения.

Опазване на водите и методи за намаляване на техния разход При съвременните технологични процеси голяма част от отпадъчните и вредни за здравето на хората и животните вещества се извличат, изхвърлят и транспортират чрез водата и речните течения, попадат във водоемите или моретата и океаните. Всичко това съдейства за бързо и непрекъснато замърсяване на водите в тези обекти и превръщането им в негодни за задоволяване на редица нужди на човека и обществото. Водата, почвата и въздухът имат свойството да се самопречистват, но тази способност за самопречистване има своите граници. Ето защо замърсяването със отпадъчни вещества става опасно от момента във който тяхната концентрация във водата стане по голяма от способността за самопречистване. Опазването на водите включва няколко мероприятия - организационни, технически, икономически. Организационните мероприятия се изпълняват от държавните органи. Те се изразяват във това да се управлява, да се действа законодателно, да се определят допустимите норми за замърсяване на реките, реконструирането на пречиствателните съоръжения и също така да налагат санкции и да търсят отговорност на нарушителите.

Техническите мероприятия които предпазват водоизточниците от замърсяване. Към тях спадат пречистването на отпадъчните води, повторното им използване, създаване на оборотни системи за водоснабдяване, намаляването на водопотреблението. Към икономическите мероприятия спадат идеите за намаляване на водопотреблението и използването на водите повторно.

Намаляването на водопотреблението е възможно само чрез усъвършенстването на старите и въвеждане на нови технологии. Големият разход на вода във редица

предприятия се дължи на използването на водата при правотокова система на водоснабдяване. При нея водата от водоизточника постъпва направо в производствения процес и чрез пречиствателните съоръжения се пуска отново във водотока. Най-ефективен начин за намаляване на количеството на замърсените отпадъчни води в промишлените предприятия е въвеждането на обратното водоснабдяване. Тази система изключва изхвърлянето на отпадъчните води във водоемите и дава възможност за многократно използване във производството. Този метод намира най-широко приложение във металургичната промишленост, нефтохимическата и целулозно-хартиената. Замяната на водното охлаждане със въздушно и изпарително е също перспективен начин за икономия на вода. При изпарителното охлаждане, охлаждащата вода се заменя с кипяща.

Методите за пречистване са важна стъпка във борбата със замърсяването на водоизточниците, чрез тяхното прилагане се намалява попадането на вредни вещества във водоемите и приемането на същите от хората, животните и растенията. Използват се различни методи за пречистване: механични, химични и биологични. Чрез механичното почистване се отделят по-грубите, плаващи и несени от речните течения вещества. Има много и различни съоръжения за механично пречистване на водата. Най-често това пречистване става чрез прецеждане на отпадъчните води през решетки и сита, използват се и пясъкоуловители за задържане на минералните примеси. При масла, мазнини, от маслодобивните заводи и месокомбинатите се използват маслозадържатели. Друг ефективен начин при механичното пречистване е утаяването на примесите от минерален и органичен произход в съоръжения наречени утайтели.

Отпадъчните води от химическата, нефтопреработвателната и металургичната и други промишлености съдържат много киселини, соли и други химични вещества. Те биват подлагани на химическо пречистване. Химическото пречистване се дели на 2 процеса: неутрализация и окисляване. Неутрализацията се прилага при води, които съдържат различни видове киселини. Тя се извършва с поставяне на варно мляко във замърсените води, но могат да се използват и различни алкални регенти, съдържащи сода каустик и други. Окисляването се прилага за пречистване на води на които замърсителите могат да се използват отново - такива са водите от заводите от тежката промишленост. Окисляването се извършва най-често с хлор, кислород или озон.

Биологичното пречистване е широко използван метод за обработване на комунално – битовите води от хранителната, нефтопреработвателната, хартиено – целулозната и други промишлености. Биологичното пречистване се извършва от микроорганизми, използващи за своето развитие органични и неорганични съединения от отпадните води. Освен тези бактерии, се използват и някои водорасли и гъби. Като цяло биологичните процеси се основават на самопречистване, но може да се използват и биофилтри. Те са съоръжения, в които водата преминава през едрозърнести материали, като при работа на филтъра те се покриват с активна биологична ципа, която абсорбира органичните вещества от водата. Като филтриращи материали може да се ползват шлаки, въглища, чакъл и други.

Заклучение

Водата е символ на живота . Тя е средата, в която протичат всички биологични реакции, и без нея животът на земята е немислим. Ако човечеството желае да съхрани разнообразието от жизнените форми на земята и да спаси нашата планета от глобални бедствия и катаклизми, трябва да полага повече усилия за запазването и почистването на водите и водните ресурси на планетата. Като за това само ние, хората, можем да бъдем отговорни. Подобряването на екологичната обстановка е дълъг и непрекъснат процес който е важна част от жизнената дейност на хората във всяка страна.

Литература:

1. http://uard.bg/files/custom_files/files/documents/New%20knowledge/year2_n2/paper_bardukova_y2n2.pdf - Валиден към 25.09.2017
2. http://www.wecf.eu/download/2013/wsp/BG_WSP_Mod10.pdf - Валиден към 25.09.2017
3. <https://bg.wikipedia.org/wiki/%D0%97%D0%B0%D0%BC%D1%8A%D1%80%D1%81%D1%8F%D0%B2%D0%B0%D0%BD%D0%B5> – Валиден към 25.09.2017
4. Радослав Иванов. Замърсяване на водите и въздействие върху екосистемите. Химера 2015

С. А. Славчев,

ОРГАНИЗИРАНА ПРЕСТЪПНОСТ В СТРАНАТА И ИЗВЪН НЕЯ

Стилиан А. Славчев

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” – гр. Шумен

ORGANIZED CRIME IN THE COUNTRY AND OUTSIDE IT

Stilian A. Slavchev

E-mail: slavchev_1992@abv.bg

Abstract: *Globalization has dramatically increased the trans-border nature of the organized crime. Modern means of communication precondition the establishment of a network of criminal organizations. The geostrategic specifics of our region crossed by roads, connecting Europe and Asia naturally, predisposes its part in the routes used by the international crime.*

Keywords: *globalization, trans-border organized crime; network of criminal organizations.*

1. Увод

Понятието ”Международна престъпност” се използва за означаване на потоците от информация, пари, физически обекти, хора или други материални или нематериални средства през държавните граници, при което един от обектите не представлява държавата . Поради това международната престъпност се диференцира като форма на търговска дейност, осъществявана с противоправни средства, с използване на заплаха и физическа сила, изнудване, корупция, шантаж, и други методи на принуда, а също и чрез привличане на забранени стоки и услуги. Организираната престъпност е заплаха за икономиката и обществото в Европа. Реакцията на Европейския съюз във връзка с борбата срещу организираната престъпност е адаптирана към сложността на явлениято и е насочена към трафика на хора, оръжия и наркотици и към икономическата и финансовата престъпност. Тя обхваща новите измерения на организираната престъпност като компютърната и екологичната престъпност. Интегрираният подход направляващ действията на Европейския съюз, се разпростира от превенцията до правоприлагането. Той се базира основно на ефективното сътрудничество между властите на държавите членки и по-специално на правоприлагащите агенции, включващи обмяна на информация и взаимното съдействие при изземане и конфискации. Борбата срещу организираната престъпност е глобална и засяга много области от действията и политиката на Европейския съюз.

2. Дефиниране на понятията организирана и трансгранична престъпност

В реалния си живот всеки от нас се сблъсква с явления, които интерпретира като прояви на организирана престъпност, дори и без да е станал тяхна жертва, поради факта, че няма доверие в държавните институции. Това отчасти е мотивирано и от страха че и те са станали подвластни на вездесъщите престъпни мрежи. От държавните институции, отговорни за борбата с организираната престъпност, се очаква освен да имат сходно разбиране за нейния характер, но и да поднасят по такъв начин експертните си държавни решения, че те да се превърнат в основата за един по-информиран, по-структуриран обществен дебат, в който информационното изобилие свързано с организираната престъпност, няма да доведе до традиционно объркване и заглушаване на гласа на разума. Създаването на истинска и разумна обществена перспектива за организираната престъпност, която ще се отнесе по най-строгия и сериозен начин към проблема, неимоверно ще оправдае очакванията на обществото и всеки гражданин ще се чувства сигурен и защитен. Поради появата на нови и различни форми на организираната престъпност все повече се откроява значимостта на взаимодействие и сътрудничество между отделните държави в света и между народните организации, създадени за нейното ефективно противодействие. Глобализацията значително повиши трансграничния характер на организираната престъпност, като съвременните средства за комуникации създават условия за изграждане на престъпни организации от мрежов тип. Геостратегическата специфика на нашия регион, пресичан от пътища, свързващи Европа и Азия, естествено се вписва в маршрутите, използване от международната престъпност. Географското разположение и възможностите, които членството в ЕС на част от страните поражда допълнителен интерес от страна на трансгранични криминални мрежи за нелегален трафик на наркотици, хора, оръжие и стоки. Като следствие от икономическата и финансовата криза много криминални пазари се разшириха, организираната престъпност се приспособи успешно към новите реалности и в краткосрочен и дългосрочен план ще продължи да търси възможности за допълнителна експанзия. Острият недостиг на ликвидност в международния финансов сектор спомогна за значително увеличаване на финансовите средства на престъпните групи. Младите хора и етническите малцинства, населяващи икономически неразвити региони, са чувствително изложени на риск от привличане за участие в престъпни групи. Наркопрестъпността и нейното негативно влияние в много сфери на обществения и социалния живот се отнасят към факторите, застрашаващи сигурността и здравето на обществото. Тя е един от престъпните феномени, оценявани като заплаха за страните от Европейския съюз. Контрабандата с горива, алкохол, хранителни и нехранителни стоки нанася значителни вреди на икономиката. Това от своя страна има пряко отношение към социалната сигурност. В същността си контрабандата е трансгранична престъпна дейност, стимулирана от различията в пазарите и данъчните ставки в страните на региона. Престъпните структури инвестират значителни финансови средства поради реализирането на високи печалби.

Черно море И свързаните с него водни пътища създават допълнителна възможност за престъпните групи.

3. Последици от международната организирана престъпност

Честото нарушаване на граничния и митническият режим е възможно, при слаба държавност. Международната престъпност чрез дейността на престъпни организации е заплаха за устоите на съвременното общество. Акцентира се върху злоупотре-

реба с наркотици, производство, трафик и търговия. Създава се сложна мрежа. Въвлечат се предимно млади хора, чрез „зарибяване”. Международната престъпност създава средства за развитие на нови форми на престъпността. Тя може, да се окаже пагубно въздействие върху всяко общество, независимо от степента на неговото развитие и култура. Посредством корпорацията се подкопават основополагащите институции на държавата, независимостта на законодателната, изпълнителната и съдебната власт, разрушават се основни ценности гарантиращи нормално протичане на обществения живот. Новите глобални измерения на сигурността, правят все по-значимо сътрудничеството между държавите за противодействие на новите предизвикателства, надхвърлящи националните, двустранните и регионалните способности. Характерът и динамиката на съвременните предизвикателства създадоха ситуацията, държавата, независимо от ресурсите си, да не е в състояние да се справи самостоятелно с новите рискове и заплахи за сигурността. Решенията за повечето проблеми все повече трябва да се търсят в изграждането и укрепването на ефективни системи за колективна сигурност.

4. Обществена значимост на корупцията

Все още в България доминират обществените представи, че корупцията е широко разпространено явление на всички равнища на държавното управление и сред различни сфери на обществения живот. Към края на 20 век корупцията неизменно се възприема като един от най-сериозните проблеми на България. През 2004-2008г. в резултат на стабилната макроекономическа обстановка в страната, добрите темпове на икономически растеж и активната социална политика на правителството намалява актуалността на проблеми като безработица и бедност. Обаче значимостта на корупцията като проблем който засяга обществото се изостря и през 2008г. този проблем е на първо място в обществения дневен ред в страната. Условно могат да се очертаят три типа криминални структури, които имат различни исторически корени, развитие и отношение към използването на политическата корупция в своята дейност:

- Силовите предприемачи („силвите групировки”) са най-ярко предизвикващата внимание част от организираната престъпност. „Силвите групировки” са българският вариант на т.нар. модел на „предприемачество на насилието”. „златната ера” на силното предприемачество приключва с политическата и икономическата стабилизация през 1997г.

- Девиантните предприемачи чрез криминалните си структури осигуряват своето конкурентно предимство на пазара. При този тип организирана престъпност за разлика от обикновените фирми пазарното предимство се осигурява чрез спестяване на мита, данъци такси и криминални транзакции. От историческа гледна точка девиантните предприемачи възникват преди силвите и олигарсите. Те първи масово упражняват корупционни техники спрямо държавни служители – митничари, полицаи, данъчни и др. Плаща се не само да не им се пречи да работят престъпвайки всеки закон, но най-вече да се пречи на работата на конкурентите (митническите служби организират данъчни проверки и конфискуват техните стоки и т.н.).

- Олигарси - „олигарх” етикет по аналогия с Русия и Украйна в България започва да се използва за лидерите на някои от най-големите икономически групировки. Въвеждането на това понятие цели да покаже качествено различията модел на организирано криминално поведение при олигархичния тип структури спрямо

модела на силовите групировки. В българските условия използването на понятието олигарх има сериозни ограничения за разлика от страни като Русия, където вътрешният пазар бива защитен директно от държавата от чужди компании и предоставя олигоплоно или монополно положение на руските компании, в България това е много по-трудно. Българските олигарси са сериозно ограничени от гледна точка на възможности от големите международни компании, особено след присъединяването на страната към ЕС. Много често те дори да са успявали да осъществят контрол над някой вътрешен пазар,компаниите на българските олигарси в крайна сметка или продават бизнеса си на чужди корпорации, или губят пазарен дял. Много сектори на икономиката остават зависими от местното законодателство и тясно обвързани с държавните решения, които не позволяват пробиването на чуждестранни инвеститори без подходящ местен партньор. През последните няколко години подобни отношения се наблюдават при концесионирането на летища и пристанища, установяването на правни форми и др.

Заклучение

За да бъде преодоляно състоянието на несигурност е необходимо всички заедно да реагират в посока на възстановяване на нарушеното състояние на сигурност. Сътрудничеството в тази насока е от първостепенно значение и за страна като България, която по принцип не разполага с достатъчно ресурси и потенциал сама да осигурява сигурността си.

Литература

1. Център за изследване на демокрацията
2. www.nbu.bg/PUBLIC/IMAGES

Т. Т. Желязков,
КИБЕРТЕРОРИЗЪМ

Тихомир Т. Желязков

*Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” – гр. Шумен*

CYBERTERRORISM

Tihomir T. Zhelyazkov

E-mail: usus15@abv.bg

Abstract: *Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation.*

Keywords: *cyberterrorism, violent, act, intimidation.*

Въведение

През последните няколко столетия тероризмът е убил, наранил или постоянно брутализирай безброй човешки същества. Той е оставил озадачени и в недоумение много хора, както поради своята природа, така и във връзка с възможността си да контролира човешките умове и способността си да оцелява във времето и пространството. Правителства, учени и военни са блокирани в спорове за неговото определение. Тероризмът е едновременно престъпен, политически, икономически, психологически, социален, психологичен по същество и последствия.

Интернет пространството

Днес в интернет пространството, като съвкупност от независими информационно-технологични инфраструктури, телекомуникационни мрежи се впускат хора с цел взаимодействие, обмяна на информация и идеи. Киберпространството може да се разглежда като начин за доставяне и разпространяване на нови възможности за промени в обществото и културата чрез завоалирани идентичности, или като безгранична комуникация.

Начало на кибертероризмът

Информационните операции са координирани движения, дейности на компютърните мрежи, чрез които желаната информация лесно и бързо достига до нас. Но с напредването на съвременните технологии, учените създават нови програми и посъвършени компютърни „умове“, целящи да повлияят, сринат или манипулират процесите на вземане на решения на други автоматизирани системи, като в същото време се защитават собствените способности за това.

Прехода от 20 към 21 век, води до пренос на информация, която изведнъж придобива нови измерения. Главоземайващите темпове на развитие на технологиите, паралелно водят със себе си създаването на вируси и вредоносни програми, без да се допуска каквото и да било несъвършенство у тях. Възможност за използване на научно-техническите открития получават, както правителствени и военни инсти-

туции, така и терористи, за които интернет пространството е нова сцена за изява. Кибервойните създават произведенията си, по начин по който да съспят компютрите ни. В историята вече могат да влязат заплахите от изключване, блокиране и изтриване на държавни мрежи, ценни файлове и т.н.

Типове кибертероризъм

Кибервандализъм – може да бъде определен като масово проникване и обектообразяване на сайтове с политическа или пропагандна цел в резултат на което се постига международен или локален отзвук чиято цел е обикновено пропаганда целяща да подрони авторитета на дадена страна или организация.

Киберпрестъпления – целенасоченото блокиране на достъпа до мрежи или определени сайтове, интернет измами, разпространение на пиратски софтуер и друг вид интелектуална собственост.

Кибервойна – синоним на информационната война, която сама по себе си представлява, действия предприети с идеята да се постигне информационно превъзходство. Подразделение на информационната война е киберразузнаването.

Киберразузнаване – координиране на информация между HUMINT (човешко-разузнаване), SIGINT (сигнално-разузнаване), ELINT (електронно-разузнаване) и други с цел подобряване на комуникациите между различните звена.

Психологични операции (PSYops) – представляват координирани психологически действия с цел промяна на поведението или разбиранията на противника, за да бъдат постигнати целите на дадена страна или организация.

Електронно разузнаване (ELINT) – използване на всякакви електронни средства за блокиране, прихващане, и модифициране на вражески комуникации. Най-явният пример за успеха им са огромния брой подслушвателни мобилни постове и дори подводници които се придвижват в забранени зони. Рисковете са огромни, но събраната информация напълно ги оправдава.

Видове атаки

Със заемането на по-голямо пространство на кибервойната и тероризма в ежедневието ни се обособяват няколко вида мрежови атаки.

Прости - неструктурирани – провеждане на основни хакове срещу отделни системи, използвайки методи, създадени от някой друг.

Разширени - структурирани – провеждат се по-усъвършенствани атаки срещу множество системи или мрежи, като има вероятност да се създадат нови основни хакерски инструменти

Сложни - координирани – провеждат се координирани атаки с голяма сложност на проникване като целта е причиняване на масово нарушаване на интернет бариерите.

Потенциални атаки

Необходимо е да се отбележи, че тероризмът е заплаха, която още не е придобила конкретни очертания и за това едни сред най-вероятните потенциални атаки са:

- директна атака срещу Интернет инфраструктурата;
- атаки и модификации на SCADA системите;
- атаки на 3G мрежите и клетъчните комуникации - първия мобилен вирус (Fontal) който блокира GSM телефона е факт от Април, 2005;
- масов DNS hijack с цел пропаганда или за разпространение на злонамерен код;

- масови Интернет измами - атаки, които подронват авторитета на електронната търговия и носят огромни загуби;

- кражба на идентичност - преминаването към биометрични паспорти и RFID (Radio Frequency Identity Tags), определено ще отвори нови възможности за крадене на идентичности.

Факт е че в САЩ са били хакнати едни от най-големите, така наречени “data aggregators”, които съдържат и събират детайлна информация за всеки гражданин, а именно - LexisNexis и ChoicePoint.

Водещи организации, техните цели и принципи

Водещи терористични организации, стремящи се към кибертероризъм и движещи активно в тази дейност в последно време са „Хизбула“, „Хамас“, „Ал Кайда“ и др. Те използват компютърните системи и мрежи за обсъждане на своите планове, пропагандиране на идеи, провеждане на терористични актове и привличане на нови членове. При кибертероризма основните принципи в дейността на терористите се явяват - конспиративността и секретността при подготовката и провеждането на терористичните актове.

Основни мерки за справяне с проблема

Хвърляйки поглед върху терористичните тактики, то те всяват объркване и хаос. За това осъзнаването на риска от атаки и разбирането му водят до сериозно заемане с работата над електронната търговия и правителството. България е в изгодна позиция и тъй като е предприела една от първите стъпки към борба с кибертероризма за разлика от САЩ в момента до известна степен е силно защитена от блокиране. За защита от кибертероризма се създават различни концепции от страна на страдащите региони и се издигат мрежови защитни бариери, вируси и програми.

Заклучение

Заплахите и рисковете, които крие кибертероризмът все повече придобиват глобален характер. Това явление налага своето насилие не по-малко от другите видове тероризъм, за това мерките за защита на гражданите трябва да бъдат превантивни и отговарящи на удари от страна на терористичната инфраструктура.

Литература :

1. <https://en.wikipedia.org>;
2. <http://www.aktivnasigurnost.org>;
3. <https://nmitkov.wordpress.com>.

Т. Т. Желязков,
**МЕТОДИ ЗА ПРЕОДОЛЯВАНЕ НА ОБЩЕСТВЕНО-ПОЛИТИЧЕСКАТА
КРИЗА**

Тихомир Т. Желязков

*Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” – гр. Шумен*

METHODS OF OVERCOMING THE PUBLIC-POLITICAL CRISIS

Tihomir T. Zhelyazkov

E-mail: usus15@abv.bg

Abstract: *The Socio-political crisis of today can have long wasting effect on the people of not only the suffering country but its neighbor's. This is why it's important to understand the reasons behind this particular type of crisis, the consequences of it and the actions that can be used to avert it.*

Keywords: *socio-political crisis, compromise, consequence.*

Общи приложения

Обществено-политическата криза е тип криза, при която правителството е загубило доверието на населението на държавата си. За да бъде свалено се провеждат протести, а в отговор правителството използва силовите си апарати (армия, полиция и т.н), за да се задържи на власт.

Такъв тип кризи могат да възникнат във всяка държава по света. За целта на този доклад ще бъде обърнато по-специално внимание на предпоставките, както и превантивните мерки, които биха били направили избухването на кризата невъзможно. За да бъдат подплатени с факти, тези сценарии ще бъдат взети от обществено-политически кризи от последните девет години.

Най-често срещаната причина зад този тип криза е загубата на доверие от страна на гражданите към политическата прослойка. Непопулярни политически решения, проява на слабост във външната политика и нежеланието, или просто липсата на воля що се отнася до въвеждането на реформи, допринасят за това.

Този феномен не е изцяло деструктивен. Ако протестите са организирани и се стигне до диалог и двете страни са готови на компромиси то промяната е почти гарантирана. В повечето развити страни процеса завършва с този компромис. В някои, бивши колонии, държави с кървава история, процесът е отразен от управляващите със сила.

Ако се допусне да ескалира до първо ниво, въоръжени сблъсъци между двете страни, какъвто беше случаят с протестите на площад Тянанмън от 1989, Китай, то жертвите и от двете страни ще има и ситуацията може да разрасне в бунт.

Това, което правителството би трябвало да направи в този случай е да допусне провеждането на мирни протести и да подсили присъствието на полицията само

като гарант за безопасността на всички присъстващи. Също така в законодателството на повечето държави е задължително управляващите да се срещнат с лидерите на протестиращите и да изслушат исканията им седем дни преди предварително договорената дата на протеста. Ако се стигне до компромис то протестният митинг бива отменен.

Гореспоменатите причини могат да са породени от вътрешни, външни или смесени фактори. Вътрешните, заради политически лидер, който отказва да отстъпи заеманият от него пост, като например Робърт Могабе в Зимбабве, който бе на власт от 1980г. Битка между политически противници Андри Роджалина замества Марк Раваломанана като президент на Мадагаскар след дълги спорове. Доказването на корупционни практики в дадено правителство, какъвто е случая със Гонзало Санчес де Лозада, бивш президент на Боливия, който отиде в доброволно изгнание в Съединените щати след направено разследване.

Друга причина за вътрешни разногласия може да бъдат на религиозна основа или на базата на сблъсъци. Ситуацията във Сирия е с подчертан смесен характер, но тя официално започна като вътрешна на религиозна основа. През април месец, 2017г, тя отново се разпали въпреки опитите да се направят преговори между сегашното правителство на Башар Асад, бунтовниците и лидерите на третите заинтересовани страни.

Чрез обвиненията в използването на химическо оръжие външният фактор, Съединените щати извини бомбардировката над авиобаза, собственост на сирийската армия. След това действие други външни фактори, Русия чрез изостряне на отношенията със САЩ, заради опасността, която една бъдеща бомбардировка би представлявала за разположените в ключови авиобази руски военни части. А вътрешният фактор, президента Башар Асад отказва да поеме отговорност за химическа атака, за която в световната общност се спекулира, че въобще не се е състояла. И така на лице са вътрешен фактор, два по-заинтересовани външни и те със себе си водят други заинтересовани фактори чрез съюзите, в които членстват.

Едно решение на сирийската обществено-политическа криза е всички участници в нея да се съюзят, било то и временно, срещу терористите от Ислямска държава. След като този дестабилизиращ фактор за целият регион, а и за териториите извън него, бъде премахнат, то е редно ако не желаят външните фактори да участват в реконструкцията на пострадалата критична за сирийската икономика инфраструктура, то поне да не се явяват като възпиращ фактор.

Един конфликт между нежелаещото да прави отстъпки мнозинство и нежелаещото да се интегрира малцинство е често срещано явление, в повечето случаи произхождащо повече от нивото на жизненият стандарт на населението, отколкото от тяхната нужда за самоопределяне. Ако това малцинство чувства, че начина му на живот е застрашен то би могло да поиска организирането на референдум за отцепването на дадена територия, която малцинството счита за своя. Да бъде отцепена от държавата и или да бъде обособена в нова държава или да бъде присъединена към друга, каквито бяха исканията, стоящи зад протестите на коренното население на Амазонския регион Багуа (Bagua), и начина, по който тяхното движение за национално обособяване бе използвано като прикритие за трафик на наркотици от организацията „Сияйна пътека“, Перу.

Главните причини за кризите от смесен характер са икономически. Това е така поради процеса на глобализация. Икономиките на всички държави са взаимосвър-

зани. Те разчитат една на друга за суровини, стоки или работна ръка. На съдействие за технологични иновации, за обмяна на опит между специалисти, а дори и за обмяна на самите специалисти.

Корупцията е слабост за една държава, но тя може да бъде оръжие за друга. В сегашно време се наблюдават следните сценарии: Държава, износителка на суровини се опитва да изгради собствена индустрия и да се сдобие със собствена пазарна ниша. Това би я облагодетелствало, тъй като износът на една държава допринася за парите, вливащите се в нейният бюджет, чрез данъците, които търговците и собствениците на предприятия плащат.

Въпреки че Китай е държава производител на стоки, а не износител на суровини, ситуацията със нейният амбициозен проект, възобновяването на „Пътя на коприната“ е подобна. Новият „Път на коприната“ представлява масивен износ на стоки от Китай за целият свят. За тази цел трябва да се построи пътна мрежа, пристанища и други обекти от критичната инфраструктура.

Ако световните пазари бъдат залети с китайски стоки, то целият свят ще бъде дестабилизиран. Това е така, тъй като всички ще станат просто консуматори, а това е невъзможно на практика, тъй като без производство няма икономика, а без икономика няма покупателна способност.

Последици от обществено-политическата криза

Главните последици от този тип криза са:

Гражданско недоволство: Една обществено-политическа криза има три етапа на развитие. С ниско напрежение-когато местното население негодува, но правителството е стигнало до някакъв компромис и не се е стигнало до протест. Средна интензивност на риска, при която хората протестираят открито на улиците, тъй като смятат, че това е единственият начин да се постигне промяна. Висока степен на риск, където вместо да се стигне до преговори с лидерите на протестният митинг правителството решава да използва силовият си апарат и да отвърне с масови репресии. През този стадий рутината на държавата е прекъсната и това заплашва икономическата и стабилност и оцеляването на нейните граждани.

Неконкурентно способна индустрия и загуба на дял от световните пазари: Както беше изтъкнато при ситуацията със „Коприненият път“ на Китай, икономиката е гръбнака на съвременното общество. Ако инвеститорите не могат да получат възвращаемост на инвестициите си в дадена държава поради вътрешната и нестабилност то те ще намерят друго поле за изява. Между временно, конкуренцията ще бъде подтикната да заеме мястото на изпадналата в обществено-политическа криза държава и дори тя да разреши проблемите си преди да се стигне до гражданска война, най-вероятно нейните пазарни ниши ще са заети от друга държава износител на стоки или суровини.

Бедност, епидемии и глад измежду населението: Една държава е обществен договор. От една страна отделните граждани се съгласяват да отстъпят част от правата си в полза на обществото, а от друга страна държавата, която се явява като волята и интереса на обществото, трябва да гарантира останалите му права и неговото място в общият механизъм.

Риск от инвазия: В зависимост от характеристиките на региона, манталитета и културата народите, една такава криза може да бъде видяна като възможност за нови завоевания. Дори може да бъде приветствана от част от населението, малцин-

ства преселили се от нападащата държава, като знак, че ще се въдвори отново ред. Разединена държавата в криза има две възможни ситуации пред себе си – да се обедини пред агресора под лозунг за национално оцеляване, което ще подейства докато заплахата е явна, но няма да разреши проблемите, породили кризата и тя пак ще се възобнови, или да продължи да съществува в състояние на разединеност и да очаква страни съюзници да я спасят.

Ниска раждаемост: Демографски прираст има, когато бъдещите родители са сигурни, че тяхното дете не само ще оцелее, но ще има и бъдеще. Ако държавата е в състояние на перманентна криза и покупателната способност на населението е ниска то не може да се очаква да има висока раждаемост.

Бедност, обхващаща повече от една държава в даден регион: Ако една държава не може да осигури средства за нуждите на населението си тя взима заеми от Световната банка и други подобни организации. Проблемът е, че след взимането на заема има нужда от реформи, а те рядко се правят и в повечето случаи са срещнати с недоволство от населението. Такъв е и случаят със Гръцката финансова криза от 2010г, за която не е намерено решение и през 2017г.

Международна престъпност: Нестабилността на дадена държава ще окрили криминалните и елементи, които от своя страна ще направят всичко по силите си да разрастват дейността си извън границите на държавата си и по този начин ще дестабилизируют региона. Примери за това са Сомалийските пират, наркотичните картели на Колумбия, международната търговия с хора и др.

Война на регионално или глобално равнище: Почти всяка държава в днешни дни е част от икономически или политически съюз. Членките на НАТО трябва да спазват член 4-ти и 5-ти от Хартата на НАТО, които гласят, че ако една от държавите членки бъде нападната то това е атака срещу всяка една от тях. НАТО не е единственият голям съюз. Друг такъв е БРИКС, съюз между Бразилия, Русия, Индия, Китай и Република Южна Африка. Също така съществува и Арабската лига, която е на икономически принцип, но членовете и са едни от най-богатите държави на света и техният общ интерес не е нещо, което те биха рискували.

Заклучение

Въпреки че обществено-политическата криза не е ново явление в днешни дни е недопустимо да бъде позволено на която и да е държава да изпада в такова състояние. Светът е свързан с икономически нишки, подплатени с интереси на малки и големи държави и ако една от тях се скъса, то световното кълбо ще се разнищи.

Литература :

1. УАБ, *Държави в обществено-политическа криза*, 2009;
2. УАБ, *Обществено-политическа криза*, 2015;
3. Световната банка, *Местно управление и национална криза в Кот Д'Ивоар. Възможности и препятствия за общественото развитие и изграждането на мира*, 2008;
4. Ричард Смит-Бингхам, Марш и Мкленан, Глобалният център за рискови анализи, *Продължителността измежду безпорядъка намираща си път измежду общественото и политическо безпокойство*, 2016;

5. Отдел за икономически и обществени въпроси, Обединените нации Ню Уорк, *Глобалният социален доклад за Световната обществена ситуация 2011*, 2011;

6. Лоренза Белинда Фонтана, Мария Исабел Нава, *Разбиране за Обществените конфликти в Латинска Америка*, Ла Паз, Март 2013;

ARMS, TECHNOLOGIES, LOGISTICS

Tudor V. Tigănescu, Ovidiu G. Iorga, Marcel Sonu, Ana M. Harbu,

RESEARCH AND DEVELOPMENT OF A MULTI-PURPOSE LATENT FINGERPRINT RECOVERY CABINET

**Tudor V. Tigănescu, Ovidiu G. Iorga
Marcel Sonu, Ana M. Harbu**

*Military Technical Academy, Bucharest, Romania
viorel.tiganescu@mta.ro*

Abstract: *This paper presents an innovative solution for recovering latent fingerprints deposited on objects of interest for forensic investigation. The research effort focused on developing an automated equipment capable to use multiple methods of recovery of latent fingerprints and also transmit the acquired fingerprint in digital format in accordance to AFIS requirements.*

Keywords: *fingerprint, latent, AFIS, forensic, database*

1. Introduction

An important part of crime scene investigation consists of detecting, recovery and preservation of traces of individual presence in a area of interest. For identification of a suspect, some unique individual attributes can be acquired from the crime scene. While DNA contaminated objects are one of the most complex instrument for suspect identification, human fingerprints are accessible, low cost, universal and confident sources of individual identification.

Human fingerprints are markers of an individual identity which are unique, durable over lifetime and have a high degree of dissemination in the environment. Forensic identification by fingerprint analysis has been used since 20th Century and is still one of the most important instruments in human identification. A fingerprint in its specific sense is an impression left by the friction ridges of a human finger. The unique trace left by human fingers are based on the particular arrangement of the friction ridges on the contact surface of the finger. The ridges are formed by the distribution of dermal papillae and perpetuated into the epidermal layer. The anatomical role of the friction ridges is supposed to be in relation of amplifying the vibrations transmitted to receptive nerves

when contacting surfaces with fingers and also to enhance the grip on wet object/surfaces or slippery ones.

Before the use of digital acquisition and processing of images, some classification systems have been developed in order to ease the process of matchmaking the acquired fingerprint with the database entry. Classification systems include the Roscher system, the Juan Vucetich system, and the Henry Classification System. The Roscher system was developed in Germany and implemented in both Germany and Japan, the Vucetich system (developed by a Croatian-born Buenos Aires Police Officer) was developed in Argentina and implemented throughout South America, and the Henry system was developed in India and implemented in most English-speaking countries.

In the Henry system of classification, there are three basic fingerprint patterns: loop, whorl, and arch, which constitute 60–65%, 30–35%, and 5% of all fingerprints respectively. There are also more complex classification systems that break down patterns even further, into plain arches or tented arches, and into loops that may be radial or ulnar, depending on the side of the hand toward which the tail points. Ulnar loops start on the pinky-side of the finger, the side closer to the ulna, the lower arm bone. Radial loops start on the thumb-side of the finger, the side closer to the radius. Whorls may also have sub-group classifications including plain whorls, accidental whorls, double loop whorls, peacock's eye, composite, and central pocket loop whorls.

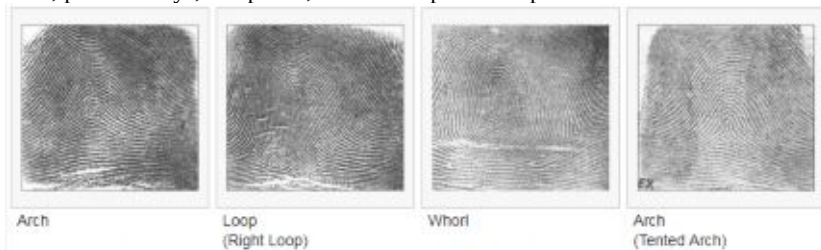


Figure 1. Anatomical patterns of human fingerprint

2. Latent fingerprint, recovery methods of latent fingerprint

According to Forensic Science, there are three types of fingerprints. D.P. Lyle, Forensic Science (ABA Fundamentals), p. 255 (2012):

- **Patent prints** are the most accessible, since are visible to the naked eye. The trace is generated by imprinting or removing a transfer substance (blood, grease, dust, wet paint) by contact between the finger and a surface;
- **Plastic prints** are three dimensional imprints caused by contact of the finger with a moldable surface (soap, clay, wax) and imprints a permanent trace of the fingerprint into the superficial layer of the material;
- **Latent prints** are the most abundant sources of fingerprint recovery, since may appear on any surface, but they are also the most difficult to detect and recover, since they are invisible. The imprint is generated by the transfer of the body excretions present on the finger (sebaceous grease, water soluble organic matter) on to porous or non-porous surfaces.

In order to recover latent fingerprints from **non-porous** surfaces, powders are used to recover the invisible imprint on the surface. The material should be finely powdered, non reactive and adherent to the grease from the finger but not to the surface (glass, painted

wood, plastics, marble, polished metals). Also, the color of the powder should be in contrast with the one of the surface in order to acquire a high definition fingerprint. In order to better preserve the imprint, magnetic powders are used, which are poured onto the surface and spread over the imprint with a magnet, avoiding contacting the traces with a brush.

Another method used for the same type of imprint recovery consists of using cyanoacrylate (superglue) vapors for fixation and revelation of the imprint. The methods imply the transport of the imprinted surface to the laboratory, and the operation is made in a special fumehood, in which the vapors are generated, circulated and in which polymerization occurs in presence of steam catalysis.

When the imprint of the finger is found on **porous** surface, some other methods are used. The methods are based on chemical interactions between a reactant and the oily residue left by human finger. The most important methods are iodine, silver nitrate and ninhydrin reactions.

Iodine methods rely on the property of solid iodine to sublime into reactive gas, that chemically interacts with the human trace generating brown colored traces. The main disadvantage of this method is that the color fades away. By using starch solution, the color can be preserved on the surface for several hours.

Silver nitrate reacts with the chlorine atoms present in human saline residue and when exposed to ultraviolet light (artificial or sunlight) turns to a persistent black color. This is the most suitable method for imprints left on paper.

The most used method for revealing human imprints on porous surfaces is based on the reaction of the ninhydrin with the oils in the latent prints. The reaction can take place by dipping the object/surface in the reactant or by circulating reactant vapors over the object. The reaction develops a bluish trace on the fingerprint traces. The main disadvantage of the method is caused by the slow kinetics of the reaction, up to several hours. In order to accelerate the reaction, the local air temperature can be risen, if the object/surface permits, up to 40°C.



Figure 2. Recovery methods for latent imprints (from left to right: iodine, silver nitrate, ninhydrin, magnetic power)

3. Design and development of a multi-purpose latent fingerprint recovery cabinet

In order to optimize the forensic laboratory setup, a multipurpose latent fingerprint recovery cabinet has been designed. This cabinet will have the following practical uses:

- Recovery of finger imprints by using iodine reaction fixed with starch;
- Recovery of finger imprints by using silver nitrate reaction;
- Recovery of finger imprints by using ninhydrin reaction catalyzed by temperature;
- Digital capture of the revealed images by integrated photographic equipment in optimal illumination conditions.

Based on the mentioned functionalities the cabinet will have the following technical specifications:

- The cabinet volume will be of 200 liters;
- The access door will have at least 50x50cm dimensions;
- The temperature inside the cabinet can be controlled and regulated up to 75°C (threshold $\pm 30^\circ\text{C}$);
- The humidity inside the cabinet can be controlled and regulated in the range of 20-80% absolute humidity;
- Automated door opening and warning system;
- Program control and record of the parameters in the range of 10-100 minutes;
- Pressure control and inside air circulation system;
- UV-source;
- Polarized light source;
- Sublimation/evaporation system for generation of water vapors, ninhydrin vapors and iodine vapors;
- Integrated parameters control and monitoring;
- Integrated evidence data, image acquisition and parameters recording and transmission system.

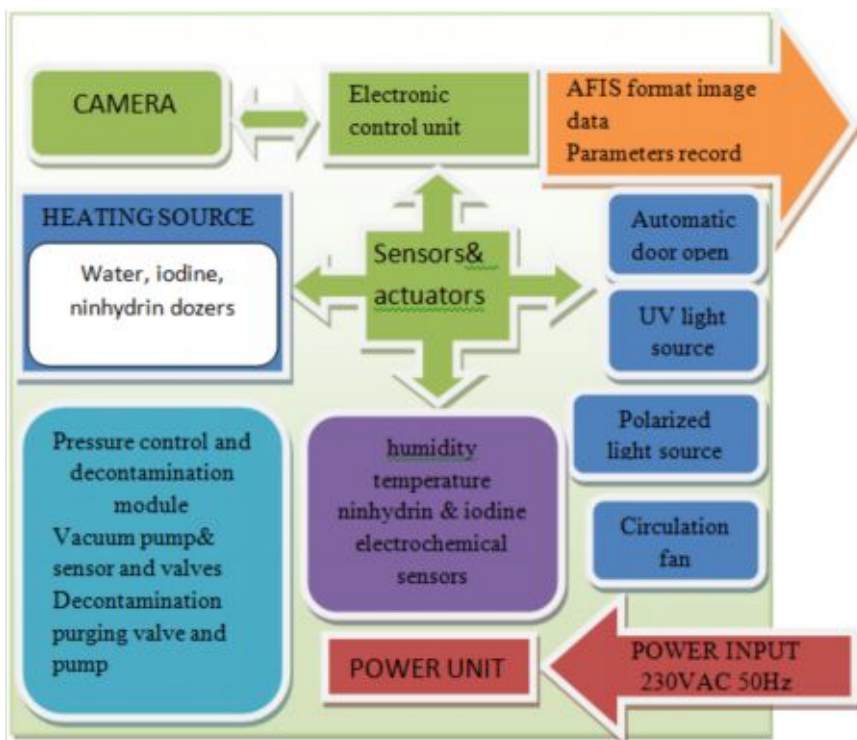


Figure 2. Functional scheme of the multi-purpose fingerprint recovery cabinet

The subsystem for temperature and gas control will consist of a heating source made of Kanthal enclosed in a stainless steel pipe and insulated by aluminium oxide powder, regulated via ECU by a temperature sensor (PT100). It will also have a electrical motor fan to uniform the temperature, humidity and chemical gradient inside the cabinet.

The cabinet will also have the following subsystems:

- Humidity generator and sensor
- Chemicals vaporisator and dozer to create the reactive atmosphere;
- Purging device with vacuum pump, droplet separator and air filter;
- Decontamination unit with air compressor (20bar max) and air tank (10l – 10bar)
- Electronic control unit (ECU) with integrated sensors and actuators for integrated control of the cabinet. The unit will also have data logging and transmission protocol via Ethernet/USB protocol.

4. Conclusion

In order to obtain detailed, reproducible forensic information regarding person identity, a lot of standardized equipment is needed. Latent fingerprint recovery is a complex technique which requires different approaches, with regard to the type of

support material, wheatear is porous or non-porous and also requires an evaluation of the integrity of the finger imprint on the respective media. Different recovery techniques are to be applied in every particular situation. The support equipment is voluminous and expensive. One multipurpose cabinet that can support recovery using powder, ninhydrin, iodine and cyanoacrilate reactions and also acquire standardized data proves to be a optimized and necessary equipment in a modern forensic laboratory.

References

1. D.P. Lyle, Forensic Science (ABA Fundamentals), p. 255 (2012):
2. Paul C. Giannelli, Edward J. Imwinkelried, Andrea Roth, and Jane Campbell Moriarty, Scientific Evidence, p. 949 (5th ed. 2012).
3. Feldman, Meloon, & Lambert, A New Method for Recovering Latent Fingerprints from Skin, 27 J. Forensic Sci. 806 (1982)
4. The Fingerprint Sourcebook by Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST).

Tudor V. Tiganescu, Ovidiu G. Iorga, Voicu E. Andreea, Ana M. Florea,
**RESEARCH, DESIGN, DEVELOPMENT AND BENCH TESTING OF A
HYBRID REACTIVE PROPULSION SYSTEM FOR SPACE LAUNCHER
APPLICATIONS**

**Tudor V. Tiganescu, Ovidiu G. Iorga
Voicu E. Andreea, Ana M. Florea**

*Military Technical Academy, Bucharest, Romania
viorel.tiganescu@mta.ro*

Abstract: *This paper presents the research and development of a new type of hybrid motor, equipped with an innovative inhomogeneous grain of solid propellant, an intelligent system capable of real time monitoring and controlling the oxidizer flow rate and motor functional parameters.*

Keywords: *Hybrid, propulsion, space, inhomogeneous, fuel.*

1. Introduction

Hybrid rocket motors are propulsion systems known since the early 20th century. The concept of such motors is that they use oxidant species and fuel that are in distinct solid state and are spatially separated from each other, resulting in a high degree of safety. Additional to safety, this type of motor can be easily designed environment friendly by using the appropriate non pollutant oxidant species and fuels. Compared to solid rocket motors, the technical advantages of this motor are the capability to be shut-off and reignited and to be throttle controlled. They also have an advantageous design compared to liquid rocket engines and they could prove to be more reliable. Compared to the more known bipropellant liquid motors the hybrid rocket motors present the following advantages:

- They have a less complex design due to a single propellant being liquid and so the installation for propellant delivery and the valves are reduced to half;
- The explosion hazard is reduced because only a small fraction of the two species involved in combustion can mass contact by any mechanical failure. The solid state of the fuel prevents this situation;
- The solid state of the fuel and the absence of oxidant species permit the inclusion of metal particles in the fuel grain, raising the specific impetus and the density of the fuel.
- Fuels in the solid state generally have higher density than those in the liquid phase, reducing overall system volume;
- Reduced combustion instabilities because they do not typically exhibit high frequency combustion instabilities that plague liquid rockets due to the solid fuel grain breaking up acoustic waves that would otherwise reflect in an open liquid engine combustion chamber.

- Thermal effect on the walls of the combustion chamber is reduced since the solid fuel grain acts like a thermal insulator.

Compared to solid propellant rocket motors, hybrid designs have the following advantages:

- Higher theoretical specific impulse - Possible due to limits of known solid oxidizers compared to often used liquid oxidizers;
- Less explosion hazard - Propellant grain is more tolerant of processing errors such as cracks since the burn rate is dependent on oxidizer mass flux rate. Propellant grain cannot be ignited by stray electrical charge and is very insensitive to auto-igniting to do heat. Hybrid rocket motors can be transported to the launch site with the oxidizer and fuel stored separately, improving safety;
- Fewer handling and storage issues - Ingredients in solid rockets are often incompatible chemically and thermally. Repeated changes in temperature can cause distortion of the grain;
- More controllable - Stop/restart and throttling are all easily incorporated into most designs. Solid rockets rarely can be shut down easily and almost never have throttling or restart capabilities.

2. Hybrid rocket motor configuration and oxidizer sources

A basic hybrid rocket motor consists of a combustion chamber where the solid fuel is situated, an oxidizer tank and a nozzle. The oxidizer is sprayed out into the combustion chamber and passes a central bore through the fuel grain where starts to combust, producing hot gases that are ejected through the nozzle, creating thrust. The heat melts, vaporizes and pyrolyses the surrounding fuel thus maintaining the combustion in direct relation with the regression rate of the solid fuel.

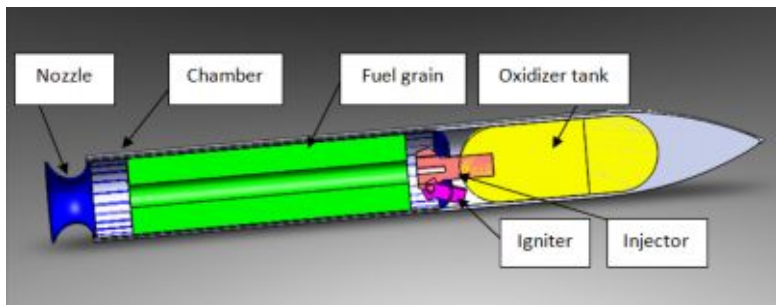


Figure 1. Hybrid rocket motor conceptual overview

As it is described in figure one, the system also can contain turbo pumps or another inert pressurized gas tank if the oxidizer used does not self-pressurize itself. The oxidizer is sprayed in the combustion chamber through an injector. The models for hybrid rockets also contain a pre-combustion and a post-combustion chamber. When starting or restarting the motor an igniting source is used. Some designs are

referred as Reverse Hybrids, meaning that the oxidizer is the solid deposited inside the combustion chamber while the fuel is deposited in liquid state into a storage tank.

The oxidizers used for hybrid rocket propulsion varies from cryogenic liquids like liquid oxygen (LOX), liquid fluorine (LF) to non cryogenic liquids like hydrogen peroxide (H_2O_2), nitrous oxide (N_2O), dinitrogen tetroxide (N_2O_4) etc. While LOX and LF offer some superior motor performance they also manifest disadvantages when regarding their cryogenic state, the need to be pressurized by other inert gas or turbopumps and the same disadvantage is present when using (H_2O_2). Dinitrogen tetroxide has the disadvantage that is corrosive, toxic and fumigating, thus being a dangerous chemical to use and handle.

The use of N_2O in hybrid rocket motors seems to represent the most feasible solution because of the following advantages:

- it is a saturated liquid at room temperature (51 bar at 20°C);
- it is a safe to use monopropellant, and can be used to start up the motor without the use of an additional liquid fuel;
- high stability at room temperature;
- reduced toxicity;
- it has high density and low pressure in storage;

3. Fuel selection

The solid fuels used in hybrid rocket motors consists mainly of short and long chain alkanes, thermoplastic or thermoelastic polymers. These materials have been tested in different configurations and with different kinds of oxidants. The first experimental designs used jellified gasoline (Soviet GRID 9-1932) or even cryogenic short chained hydrocarbons. These solution pose technical problems related to the structural integrity of the fuel. In 1951, Pacific Rocket Society tested the XDF-23, which consisted in a LOX-rubber propellant system. Although they succeeded reaching an altitude of 9 km, the slow burning rate of the polybutadiene (PB) used hindered future development. The next advancement was the use of polyethylene (PE) as a fuel, like the H_2O_2 -PE motor tested by General Electric in 1950's which demonstrated the easy throttling of hybrid motors but also that the regression rate of the fuel was unsatisfactory. Research conducted in the domain resulted in more elaborated organic fuels like polybutadiene acrylonitrile (PBAN) or polymethyl methacrylate (PMMA) doped with lithium, lithium hydride or magnesium. United Technologies Corporation, sponsored by NASA developed in the 1960-1980 period different motors using PB-PMMA and liquid oxygen-liquid fluorine mixtures or fuming nitric acid. The results were satisfactory, obtaining 380s for a 1.07m diameter motor. In Europe, ONERA also tested nylon and nylon derivated fuels. In Sweden, Volvo tested the use of fuming nitric acid and a mixture of aromatic amines and PB. In 1981-1995 Starstruck and Amroc tested several combinations of LOX and PB and hydroxi terminated polybutadiene (HTPB). They obtained up to 1.1 meganewtons of thrust. The main problem was the low frequency instabilities and the structural collapse of the complex, multiport wagonwheel shaped motor. After 2000, Lockheed Martin and NASA developed and flight tested some LOX-HTPB motors capable of delivering 270kN of thrust with the intended scope to replace a two or three stages

rockets of the same dimension. The HTPB fuels in conjunction with N₂O were the source of thrust in the Space Ship one vehicle built by Scaled Composites. They obtained a 80s burning time motor capable of thrusting a 3 person shuttle at a altitude of 114km, but they experienced some combustion instabilities.

The main challenge experienced by the research made in the domain was related to the slow burning of the polymer fuel. This is caused by the regression rate of the fuel which is dependent by the thermal properties of the polymer and the heat transfer from the burning front to the material to be melted, then pyrolysed/gasified. The solutions taken into account to overcome the impediment were the following:

- multi-port channel design – this solution intends to expand the reaction surface by creating multiple bores through the fuel grain. Even though the thrust of the motor raises, the overall volume efficiency of the motor drops caused by the large fraction of empty space inside the motor. The multiport grain design also encounters uneven burning of individual ports and structural collapse of the unburned fraction when the ports expand one to each other. The unburned fraction of the motor is estimated to be around 10% mass fraction of the total fuel. The design of multi-port fuel grain motor rocket requires usage of complex web support structure for the fuel and injectors for each port or a generous pre-combustion chamber with complex hydrodynamic design;
- addition of solid oxidizing particles in the fuel grain – this is the concept of tribrid rocket motor. The inclusion of self-decomposing oxidants leads to the growth of the heat transfer by surface reactions. The obvious disadvantage of this solution is that the fuel grain turns into a solid propellant, which cancel the possibility to stop the motor and the throttle capacity diminishes. The inherent safety of the hybrid motor is also canceled due to the crack vulnerability of the motor to cause overpressure and explosion of the chamber. Also this design causes instabilities in burning, pressure spikes and motor rattling;
- injection head with swirl injection design – this design intends to raise the local mass flux by injecting the liquid propellant into the port with a large tangential component, thus maximizing the regression rate of the solid fuel. The centrifugal effect develops a much intense interaction between the oxidant and the fuel. The disadvantages of this design are that the motors are of complex construction and also the burning parameters vary with time and space inside the combustion chamber.

Recent advances in the domain conducted in the domain use paraffin as a propellant. Space Propulsion Group and Stanford University conducted research and dozens of test with paraffin (C_nH_{2n+2}) waxes (n=16-45) and PE waxes (n=45-90). Paraffin waxes burn 3-5 times faster than classical fuels as PE or HTPB. The reason why the wax burns faster is related to the liquefying hybrid fuels theory (Stanford, 1997) in which these fuels burn by forming a liquid layer on their burning surfaces and creates the possibility of entrainment of mass transfer from the liquid layer into the stream of oxidant. The regression rate is the sum of both vaporization and entrainment of liquid droplets of fuel into the oxidant stream.

The advantages of paraffin wax solid fuel grain are the following:

- The fuel is non-toxic, non-carcinogenic, non-hazardous and environmentally friendly. The products of combustion are carbon dioxide and water;

- The fuel is inexpensive and easy to acquire;
- Easy to transport and process as being an inert material in a broad range of conditions;
- Easy processing due to the thermal properties of the material. No polymerization reaction takes place and is no need for curing agents;
- Ability to precisely adjust the regression rate of the fuel without dramatically changing the processing technique or the composition of the fuel;
- Paraffin waxes are hydrophobic, making them the ideal matrix for metal particle inclusion;
- Being chemically inert, they have an theoretical infinite storage life;
- The glass transition of the paraffin-based fuel is around -108°C , 40K lower than the glass transition of rubber like fuels. Since paraffins are crystalline, the glass transition effect on mechanical properties are less severe compared to those happening in cross-linked rubber;
- Paraffin fuels are approximately 17% much denser than liquid kerosene.

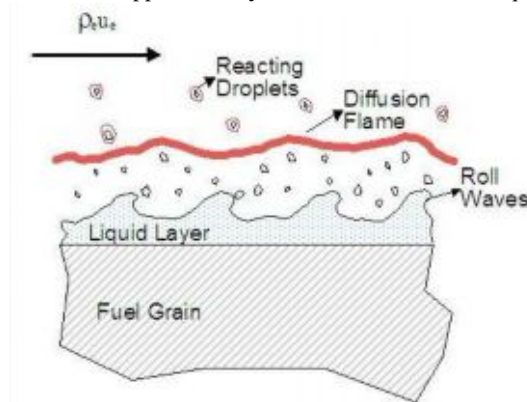


Figure 2. Entrainment mass transfer mechanism.

The advantages of using paraffin wax in hybrid rocket motors was evidenced in the tests conducted by Space Propulsion Group, where they obtained a 25kN of thrust using a 28 centimeter diameter motor and 100kN of thrust using a 56cm diameter motor capable of lifting more than 10 metric tons.

4. Design of the innovative hybrid rocket motor

We aim to develop and test a new configuration of hybrid rocket motor that will use state of the art solutions. In order to mitigate the shortcomings related to low regression rate and the combustion instabilities, our rocket motor will use a new type of inhomogeneous fuel grain made of two layers of PE paraffin wax doped with metal particles. Also, the combustion parameters will be controlled using an innovative system of real-time sensors mounted inside the chamber.

Compared to classic paraffin wax, the PE wax we intend to use has a superior melting temperature, thus preventing the fuel grain to liquefy and collapse inside the chamber. This will be the choice for the inner fuel grain layer, when the mass flux rate can be easily sustained, and another, metal particle doped paraffin wax outer layer, enhancing the regression rate when the interior section of the fuel grain becomes considerably large and the ratio oxidizer to fuel becomes overbalanced. The thermal characteristics of the paraffin waxes are illustrated in figure 3:

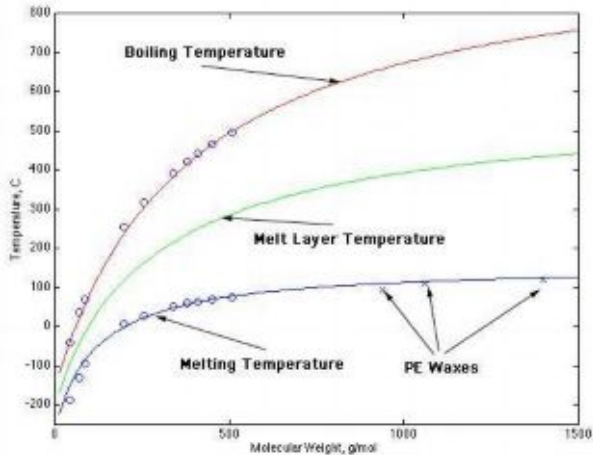


Figure 3. The relation between the molecular weight and the melting temperature of paraffin waxes (Arif Karabeyoglu, SPG Corp, 2008)

One distinct advantage of using paraffin wax is that can be easily casted when molten. On this property we intend to develop an innovative, two layered, gradient distributed metalized particle fuel grain. This new configuration will be designed in direct relation with the regression rate and will help in achieving constant combustion parameters and uniform thrust. The compensation of the expanding central bore will be made by a rising density of metal particles with the radius. This will be achieved by casting the motor in molten form under centrifugal force. The metallic particles will be micron sized and will be composed of aluminum, magnesium, cooper, etc. The innovative fuel grain is illustrated in figure 4:

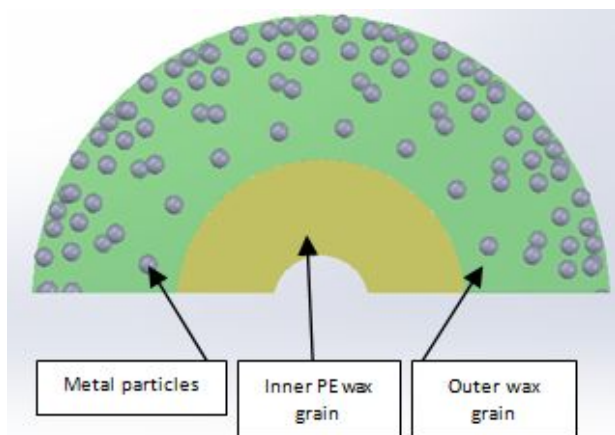


Figure 4. The innovative fuel grain

5. Command and control of the burning parameters

The combustion stability will be achieved by correlating the innovative design of the grain with a real-time control of the volume of oxidizer injected in the combustion chamber. In this regard it is intended to use sensors which would monitor the pressure and temperature in the combustion chamber and a real time acquisition and control system based on a new generation controller. The configuration of the system is presented in Fig 4 hereunder.

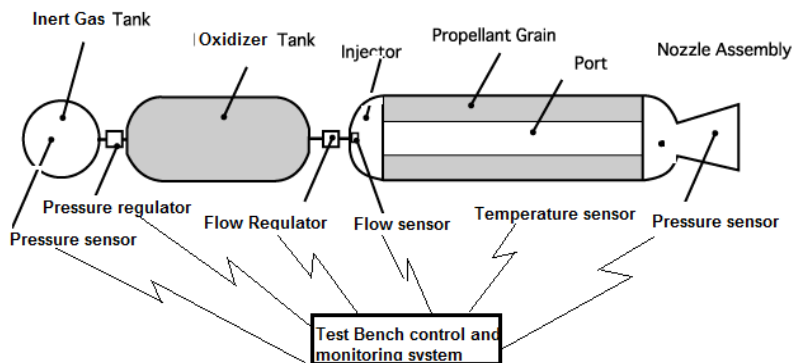


Figure 5. Block diagram of electronic circuit

For a long period of time one of the main problems of developing reliable control loops was the lack of sensors capable to withstand the harsh environment characteristic to space programs and furthermore the high temperatures characteristic to the rocket motor. There are new and promising materials such Gallium Nitride

which could solve these problems and the target of this project is to use sensors produced from this material in order to establish a reliable control loop for this application.

Proportional integral derivative (PID) control is the most commonly used control algorithm in the industry today. PID controller popularity can be attributed to the controller's effectiveness in a wide range of operation conditions, its functional simplicity, and the ease with which engineers can implement it using current computer technology. Model predictive control (MPC) is a multivariable control strategy that has been most widely applied in the process industries. The basis concept in MPC is that dynamic model of the process and available measurements are used to predict future process behavior.

The realization of digital control systems are dominated by the general-purpose microprocessor systems. Recent advances in reconfigurable hardware technology have made the FPGA (Field Programmable Gateway Array) a suitable platform for accelerating control actions computations. FPGAs are a good alternative to application specific integrated circuits (ASICs) for high speed embedded MPC applications since they offer much reduced low-volume cost, greater flexibility, and a shorter design cycle. The FPGA based-controllers offer advantages such as high speed, complex functionality, and low power consumption.

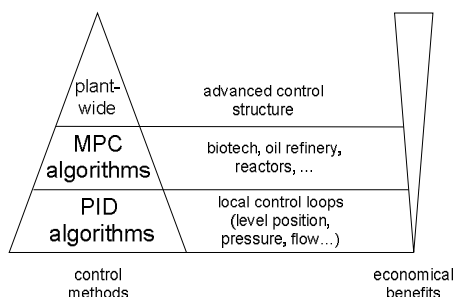


Figure 6. Analysis of the control model to be used

5. Conclusions

The rocket motor we aim to develop will bring innovative design in the attention of the international scientific community and practitioners in the domain. Both for Europe and Romania, our research effort will contribute to the domain of hybrid rocket propulsion and the applicability domains of launchers and nano-satellites. The solutions of hybrid rocket motors contribute to the broadening of spatial applications to smaller entities and for commercial applications of spaceflight.

References

1. D. Altman, R. Humble, Hybrid rocket propulsion systems, in: R.W. Humble, G.N. Henry, W.J. Larson (Eds.), Space Propulsion Analysis and Design, 1st ed., McGraw-Hill, New York, 1995, pp. 365–370.

2. Saito, W.; Takada, Y.; Kuraguchi, M.; Tsuda, K.; Omura, I.; Ogura, T.; Ohashi, H. High breakdown voltage AlGa_N-Ga_N Power-HEMT design and high current density switching behavior. *IEEE Trans. Electron. Dev.* 2003, 50, 2528–2531.
3. Guobiao Cai, Dalin Rao, Hui Tian, Optimal design of hybrid rocket motor powered vehicle for suborbital Flight, *Aerospace Science and Technology*, Volume 25, Issue 1, March 2013, Pages 114-124
4. C. Carmicino, F.Scaramuzzino, A.Russo Sorge, Trade-off between paraffin-based and aluminium-loaded HTPB fuels to improve performance of hybrid rocket fed with N₂O, *Aerospace Science and Technology* 37 (2014) 81–92

Andreea Voicu, Gabriela Toader, Mircea Teodorescu, Octavian Orban, Viorel Tigane-
cu, Traian Rotariu,

ECO-FRIENDLY POLYMERIC BINDERS FOR ENERGETIC FORMULATIONS

Andreea Voicu*, Gabriela Toader*, Mircea Teodorescu, Octavian Orban*,
Viorel Tiganeşcu*, Traian Rotariu***

* Military Technical Academy, Bucharest, RO ** Politehnica University, Bucharest, RO
traian.rotariu@mta.ro

Abstract: *In the context of worldwide efforts for greener munitions development, the aim of this paper is to present some experimental studies regarding synthesis and characterisation of new generations of greener and safer binders for energetic formulations. These binders can contribute to enhance the safety and reduce the environmental impact of the formulations in manufacture and recovery/reuse. The first class of binders was designed for recyclable explosive formulations. For this purpose, “smart” polymeric binders were synthesized based on acrylic acid and other acrylic monomers. Their main feature is they are soluble in water at slight alkaline pH allowing facile recovery of explosive fillers without using organic solvents, while maintaining their chemical and physical characteristics. A second class of binders based on polyurea was designed for use in solvent free pyrotechnic compositions. These polymers allow wet or dry pressing of the pyrotechnic compositions without using volatile organic solvents. The rubbery texture of the polyurea minimizes the risks associated to the dry pressing of other brittle binders and improves the safety characteristics while maintaining the performance.*

Keywords: *binders; polymers; environment; explosives; pyrotechnics*

1. Introduction

In the last few years people became more aware of the negative impact of their actions on the environment. International and European environmental legislation became harsher in order to avoid the irreversible damage of the natural environment. In this context, the development of safer and greener energetic formulations is mandatory on the way of reducing the effects on the environment and human health. On the other hand, the necessity of developing safer ammunition, finding reliable and efficient methods for the demilitarization and disposal of ammunition [1, 2] turned into a challenge for the researchers because this process is complex, dangerous and expensive. The removal of energetic materials, especially secondary explosives, is one of the most difficult steps in this process. Conventional methods are based on solvent solubilisation or water jet removal of explosives from the ammunition shell [2]. Following this process, the energetic material (EM) is extracted and then it can be neutralised or recovered, recycled and reused. Neutralisation of energetic materials usually involves open burning or open detonation, which are limited or no longer accepted in many countries. An alternative option is incineration in special designed facilities with subsequent air purification systems.

Another challenge of the EM recovery process is to maintain intact their physical and chemical properties.

Pyrotechnic systems, used in military applications but also for civilian purposes, involve the same safety and environmental requirements like ammunition systems. Consequently, the conventional manufacturing process of a pyrotechnic mixture is no longer satisfying these requirements. Typical pyrotechnic compositions contain around 10% of a natural or artificial hard polymeric binder that is compacted to a dense solid by molding in a die. The process of obtaining a pyrotechnic mixture implies the dissolution of the polymer in a solvent (ethylic alcohol, isopropyl alcohol, ethyl acetate, or acetone), the addition of the lacquer to the mixture of solid components, the granulation and finally the removal of the solvent. The granular composite is then pressed at high pressures in metallic dies or directly in pyrotechnic device cases. These conventional technologies described above imply many hazards associated to the use of a volatile and flammable solvent for the preparation of an explosive material, as well as the use of high pressures and metallic dies to load sensitive materials. The environmental burden is also of importance because of the inherent VOC emissions.

In this context, the purpose of this study was to synthesize a new generation of eco-friendly binders, which could allow facile recovery of the explosive filler, without using organic solvents, while maintaining its chemical and physical properties and also to investigate the possibility of developing a modern polyurea-based binder (from cross-linked pre-polymers) for pyrotechnic compositions which aims to join its excellent properties with the safety and performance requirements.

2. Materials and method

2.1. The Materials

2.1.1. Plastic bonded explosives experiments

Polymeric binder: Butyl acrylate (BuAc, FLUKA, 98%), 2-ethylhexyl acrylate (2EHA) – industrial grade, ethyl acrylate (EtAc, ALDRICH), acrylic acid (AAc, FLUKA, 99%), azobisisobutyronitrile (AIBN), N,N-Dimethylformamide (DMF, Merck). *Solubility tests:* Toluene, methanol, absolute ethanol, hexane, propylene glycol, acetone, petroleum ether, ethyl acetate, ethylene glycol, dimethylsulfoxide (DMSO), DMF and chloroform

2.1.2. Pyrotechnics experiments

Polymeric binder: Poly(propylene glycol)bis(2-aminopropyl ether) - Mn~2000 Da (PPG2000, Sigma Aldrich), Poly(propylene glycol)bis(2-aminopropyl ether) - Mn~4000 Da (PPG4000, Sigma Aldrich), triethylenetetraamine (TETA, Sigma Aldrich), Isophorone diisocyanate (IPDI, Sigma Aldrich). *Pyrotechnic composition:* Priming composition (based on barium peroxide and magnesium, Military Technical Academy) and ethanol (Sigma Aldrich) were used as received. Barium nitrate (Ba(NO₃)₂, Sigma Aldrich), magnesium (Mg, powder, Sigma Aldrich), barium peroxide (BaO₂, Sigma Aldrich), polyvinyl chloride (PVC, powder, Olchim S.A.), Phenol-formaldehyde resin (Iditol, UM Sadu Gorj).

2.2. Methods

2.2.1. Preparation of the polymeric binders for explosives

Mixtures of 2EHA, EtAc, and BuAc with AAc monomers were prepared in three different molar ratios 3:7, 5:5 and 7:3, each one containing the monomers (total volume 4mL), the initiator (1% versus monomers (w:v)) and solvent (16 mL). In order to elimi-

nate the oxygen from the flasks, nitrogen was purged in the solution for 15 minutes and then, the flasks were introduced in an oil bath at 65 °C and allowed the reaction to take place under magnetic stirring for 24h. The obtained polymers were precipitated in petroleum ether in polyethylene test tubes to avoid sticking on the walls.

Polymer/sand composite: The first trial of evaluating the behaviour of the binder designed for energetic materials consisted in using sand as inert filler. The polymer EtAc/AAC with 3:7 molar ratio was selected for this experiment: 0.306 g of EtAc/AAC were dissolved in 5 mL of DMF and then 5.794 g of sieved sand (0.1 - 0.2 mm fraction) were added. The mixture was allowed to dry partially for 1h, at room temperature, under slow mixing, and then it was granulated by passing it through a 1-mm sieve. The granules obtained were dried up to constant weight in an oven at 60 °C. 2-g portions of granular composite material were pressed at 1400 bar using a hydraulic press and a 10-mm diameter steel mould, in cylindrical shaped pellets.

2.2.2. Preparation of the pyrotechnic mixtures with polyurea binder

The pyrotechnic compositions were obtained by following these steps: ingredients drying; milling; granulometric sorting; dry mixing; lacquer preparation (for Iditol binder); wet mixing (for Iditol binder); partial drying; granulation; final drying and pressing. The first step consisted in the granulometric sorting of the solid components ($\text{Ba}(\text{NO}_3)_2$, BaO_2 , Mg and PVC). Only the 200 μm fractions were used further. The classical pyrotechnic composition using Iditol binder was prepared by mixing the solid components with the resin (50% ethanol solution), passing them through a sieve and allowing them to stay for 24 hours at 60 °C. The pyrotechnic compositions using polyurea binder were obtained in two stages: firstly TETA and PPG (PPG2000 or PPG4000) were mixed with the solid components, then IPDI was added and the mixture was stirred vigorously. The whole mixture was passed through a sieve and cooked in oven for 72 hours at 60 °C.

With the aim of studying the combustion and mechanical properties, cylindrical charges containing 2 g of each pyrotechnic composition were manufactured using a metallic mold (10 mm inner diameter). The pyrotechnic mixtures were pressed with a hydraulic press (PC1_P, PC2_P and PC3_P). In order to demonstrate that the compositions containing polyurea can be pressed by hand, wet pressing was performed using the same mold and the cylinders (PC2_H and PC3_H) where then allowed to dry for 72 hours at 60 °C. Hand pressing consisted of placing a load of 10 kg on the mold, in order to have the same loading pressure for all the samples. The reagents ratios in the composition for each pyrotechnic mixture are presented in Table 1.

2.3. Characterisation

In order to evaluate the safety and performance characteristics of the energetic mixtures, various analyses were performed. The polymers designed to be used as explosive binders were investigated by FT-IR and DSC means and trough solubility tests, as mentioned below.

FT-IR spectra were registered with a Bruker VERTEX 70 spectrometer with ATR device, using 32 scans at a resolution of 4 cm^{-1} and the characteristic frequencies of the molecules of each polymer were determined.

The glass transition temperature (T_g) of the synthesized polymers was determined by measurements with NETZSCH 204 F1 Phoenix apparatus, under nitrogen, at a heating rate of 10 °C/min. Samples weighing ca. 10 mg were heated/cooled between -80 °C and 150 °C, T_g being determined from the kink point during the second heating cycle.

Water absorption tests: Granular particles of each synthesized polymer were introduced in 200 mL of distilled water. After being maintained for 24h, at 20°C, the polymers were filtered, weighted and the water absorption percentage was calculated. Solubility tests: 20 mg of each synthesized polymer and 5 mL of solvent were introduced in sealed glass tubes.

Table 1: Composition of the pyrotechnic mixtures

Comp.	Oxidant		Fuel	Additive	Binder		
	Ba(NO ₃) ₂ [%]	BaO ₂ [%]	Mg [%]	PVC [%]	Iditol [%]	Polyurea (PPG2000) [%]	Polyurea (PPG4000) [%]
PC1_P	55	10	15	10	10	-	-
PC2_P					-	10	-
PC3_P					-	-	10
PC2_H					-	10	-
PC3_H					-	-	10

After being maintained for 24 h, at 20°C, polymer dissolution was observed. Solubility test – alkaline solution: An alkaline solution 1M with pH=14, was obtained by mixing 4 mg of NaOH and 200 mL of distilled water. Starting from this solution, alkaline solutions of pH 13, 12 and 11 were obtained. Afterwards, 20 mg of each polymer were introduced in 15 mL graduated glass tubes. The tubes were filled with alkaline solution and were sealed with septa tops and they were kept for 24 h at 20 °C, 30 °C and 50 °C. After 24 h the polymer dissolution was observed.

The pyrotechnic mixtures were characterized by using the following types of analyses: DTA, DSC, thermal vacuum stability, calorimetric bomb, burning experiments, determination of moisture content, mechanical properties, impact sensitivity and friction sensitivity. Their properties were also theoretically evaluated by using specialized NASA software - CEA (Chemical Equilibrium with Applications). The thermal behaviour and the stability of the pyrotechnic mixtures were analyzed through Differential Thermal Analysis (DTA) and Differential Scanning Calorimetry (DSC). An OZM 551 Ex Differential Thermal Analysis System was used and the samples (25-30 mg) were heated from 30 °C to 450 °C, with different heating rates: 10 °C/min, 15 °C/min, 20 °C/min and 25 °C/min. DSC was performed using a Perkin Elmer PYRIS Diamond DSC instrument. Samples having 2-5 mg were heated from 30 °C to 450 °C with different heating rates: 5 °C/min, 7.5 °C/min, 10 °C/min and 12.5 °C/min.

The pyrotechnic compositions were also subjected to the thermal vacuum stability test, which consists of artificial aging of 5 g of sample at 100 °C for 40 h [3]. Their chemical stability is reported as volume of gases released per grams of sample. The heat of combustion was evaluated using an AVL Ballistic instrument (calorimetric bomb). For this measurement, 2 g of each sample were initiated in a closed vessel using a hot wire. The specific volume of the gases released from the calorimetric bomb was measured using a Julius Peters gas-meter. For the burning experiments, a video camera, a lux meter

and a thermal camera were used in order to evaluate the behaviour of the pyrotechnic composition. For each composition, five measurements were performed and the average value was reported.

The burning rates of the pyrotechnic compositions were calculated by dividing the length of the cylindrical charges by the duration of their combustion.

The intensity of the light resulted during the combustion experiments was calculated by multiplying the illuminance (measured with the luxmeter) with the square of the distance between the instrument and the cylinders.

The temperature of the flame generated during the pyrotechnic compositions combustion was measured with a thermal camera. The moisture content of the pyrotechnic mixtures was measured using an Axis Thermobalance. For this analysis, 5 g of sample were heated at 100 °C for 2 h, and weighted every 150 s. For each composition, three measurements were performed and the average value was reported. The mechanical properties of the synthesized materials have been evaluated using a Brookfield CT3 texture Analyzer, equipped with a 4500 g cell and a TA4/1000 compression accessory. The tests were performed at room temperature, at a compression rate of 1 mm/s. The cylinder-shaped samples were compressed up to a strain of 90%. In order to obtain relevant results, five specimens of each composition were compressed and a compressive stress-strain diagram was plotted.

The impact sensitivity of the pyrotechnic compositions was evaluated using the Kast fall hammer instrument. In order to perform this measurement, 25 mg of sample were placed between two metallic cylinders fixed in a bigger metallic ring and then placed on a metallic support. The sensitivity to impact was evaluated as the energy (height multiplied with the gravity of the hammer) necessary to initiate 50% of the samples. The friction sensitivity was determined using a BAM Friction sensitivity instrument. The compositions were placed between a ceramic cylinder and a ceramic plate which were passed one over the other while the apparatus applied various pressing forces. The friction sensitivity is determined as the minimum applied force that initiates 50% of the samples.

In order to evaluate also theoretically the chemical equilibrium compositions and the thermodynamic properties of the new pyrotechnic compositions, CEA software (Chemical Equilibrium with Applications) was used.

3. Results and discussions

3.1. Polymeric binders for explosives

Following the procedures described above, 2EHA/AAC, BuAc/AAC and EtAc/AAC copolymers in different molar ratios: 3:7, 7:3 and 5:5, were synthesized. The conversions obtained are given in Table 2.

Table 2: 2EHA/AAC, BuAc/AAC and EtAc/AAC conversions

Molar ratio	Conversion 2EHA/AAC [%]	Conversion EtAc/AAC [%]	Conversion BuAc/AAC [%]
7:3	28.5	94.1	85.4
5:5	70	85.3	87.7
3:7	81.3	87.9	85.8

It was observed that the conversion increases with the amount of acrylic acid. In the case of 2EHA/AAC, after 24h, the polymer with 7:3 molar ratio was viscous and did not precipitate;

the polymer with 5:5 molar ratio precipitated and the polymer with 3:7 molar ratio was cloudy, viscous and did not precipitate. The best conversion of EtAc/AAC copolymer was obtained for a 7:3 molar ratio. After 24 h, the EtAc/AAC copolymer with 3:7 molar ratio precipitated; the polymer with 5:5 molar ratio precipitated (less than 3:7 EtAc/AAC) and the polymer with 7:3 molar ratio did not precipitate, was viscous and cloudy. Very good conversion rates were obtained (over 80%) for the BuAc/AAC copolymer.

Following FT-IR analysis, the characteristic bands of each polymer were observed. There were also observed the increase/decrease of characteristic peaks versus concentration.

Table 3 shows the values obtained for the glass transition temperatures (T_g). In the case of 2EHA/AAC copolymer, T_g decreases, from 57.8 °C to -25.9 °C, due to the content of AAC in the polymer. T_g value of 2EHA/AAC copolymer increases with the AAC content, AAC homopolymer having T_g ca. 105 °C. Also, if the amount of 2EHA increases, T_g of 2EHA/AAC copolymer decreases, 2EHA having a T_g around -50°C. The T_g variation shows copolymer formation.

Table 3: T_g values for 2EHA/AAC polymer

Molar ratio of the comonomers	T _g of 2EHA/AAC copolymers [°C]	T _g of EtAc/AAC copolymers [°C]	T _g of BuAc/AAC copolymers [°C]
7:3	-25.9	3.6	32.7
5:5	30.9	48.7	72.5
3:7	57.8	109.1	109.3

BuAc/AAC copolymer showed that T_g decreases in value, from 109.1 °C to -3.6 °C. This is due to the content of AAC in the copolymer. If more AAC is added, the T_g value of BuAc/AAC copolymer increases. More, if the amount of BuAc increases, T_g of BuAc/AAC copolymer decreases, BuAc having a glass transition temperature around -54°C. It is to note that in the case of large amounts of AAC, the value of T_g exceeds the T_g value of pure pAAc, although BuAc FT-IR spectra showed the presence of the copolymer. Probably, due to dehydration, intramolecular anhydride copolymer cycles form during DSC analysis, which yield higher T_g values than expected. Anhydride cycles stiffen chain and thus increase the T_g, which can reach 140 °C at a content of 100% cycles [5].

In the case of EtAc/AAC copolymer it can be observed that T_g value decreases from 109.3 °C to -32.7 °C. This is also due to the content of AAC in the polymer. Moreover, if the amount of EtAc increases, the T_g value of EtAc/AAC copolymer decreases, EtAc having a glass transition temperature around -24 °C. In this case it is also likely to occur anhydride cycles formation, as shown by the higher T_g value for the copolymer 3:7 versus the value reported in the literature for pAAc.

After characterising the synthesized copolymers, they were subjected to several solubility tests, as mentioned below.

The aim of this study was to find a polymer capable of dissolving in an alkaline solution, while being insoluble in water. Ammunition can be stored in locations with high humidity, transported on a rainy weather or at some point immersed in water, so the polymer must be waterproof. To determine the water absorption degree of the synthesised polymers, 30-40 mg of polymer were immersed in 200 mL distilled water for 24h. After 24h, the polymers were weighted and the water absorption degree was calculated. The results are shown in Table 4. The results indicate that the water absorption percent-

age is rather low. It can be also observed that the percentage value decreases while increasing the BuAc, EtAc and 2EHA comonomers ratios in the copolymer.

The synthesized binders should be soluble in an organic solvent, in order to be able to be used to coat explosive crystals. For this purpose, firstly, they have to be solubilised, then the lacquer obtained is mixed with the solid particles and, in the end, the solvent is evaporated. The copolymers obtained were introduced in different polar and non-polar solvents to determine whether they are soluble or not.

The solvents used were: toluene, methanol, absolute ethanol, hexane, propylene glycol, acetone, petroleum ether, ethyl acetate, ethylene glycol, DMSO, DMF and chloroform. The results obtained are shown in Table 5.

Table 4: Water uptake for the copolymers obtained after 24h of swelling

Copolymer	Molar ratio of the comonomers	Initial weight [mg]	Final weight after 24h [mg]	Water absorption [%]
2EHA/AAc	3:7	14.0	16.0	14.28
	5:5	6.4	7.1	10.93
	7:3	9.9	10.2	3.03
BuAc/AAc	3:7	30.5	40.4	32.45
	5:5	36.5	47.1	29.04
	7:3	37.4	39.5	5.61
EtAc/AAc	3:7	8.3	10.1	21.68
	5:5	10.0	12.0	20
	7:3	12.3	16.7	11.38

Table 5: Polymers solubility after 24h

Solvent	2EHA/AAc			EtAc/AAc			BuAc/AAc		
	3:7	5:5	7:3	3:7	5:5	7:3	3:7	5:5	7:3
Toluene	-	-	+	-	-	-	-	-	-
Methanol	-	-	-	-	-	-	-	-	-
Absolute ethanol	+	+	+	+	+	+	+/-	+/-	+/-
Hexane	-	-	-	-	-	-	-	-	-
Propylene glycol	-	-	-	+	+	-	-	-	-
Acetone	+/-	+	+	+/-	+	+	-	+	+
Petroleum ether	-	-	-	-	-	-	-	-	-
Ethyl acetate	-	-	+	-	-	+	-	-	+
Ethylene glycol	-	-	-	+	+	-	-	-	-
DMSO	+	+	-	+	+	+	+	+	+
DMF	+	+	+	+	+	+	+	+	+
Chloroform	-	-	-	-	-	-	-	-	-

*(-) polymers not dissolved; (+) polymers dissolved; (+/-) polymers partially dissolved

The central aim of this work was to obtain a binder which is soluble in an alkaline aqueous solution without modifying the physical and chemical properties of the explosive filler. The classical binders exhibit very good mechanical, physical and chemical properties, but during the recovery process of explosives at the end life of ammunitions, their properties change. For this test, 30-40 mg of each polymer was immersed in test tubes of 15 mL filled with alkaline solution. The tubes with polymer and alkaline solution were sealed and maintained for 24h at 20°C, 30 °C and 50 °C. The results obtained are presented in Table 6.

It is important to observe that EtAc/AAC polymer with 3:7 molar ratio dissolved in the alkaline solution with pH 11 at 30°C. At 50 °C, for the alkaline solution with pH 11, three polymers dissolved: 2EHA/AAC molar ratio 3:7, EtAAC/AAC molar ratio 3:7 and BuAc/AAC molar ratio 3:7.

With the purpose of evaluating the behavior of a composite containing the binder, cylindrical pellets containing EtAc/AAC (with 3:7 molar ratio) and sand (as inert filler) were obtained as described in *Methods section*. The cylindrical pellets were introduced in 100 mL alkaline solution with pH 11 at room temperature (20°C). After 24 h, the complete disintegration of the cylinders was observed (Figure 1). The alkaline solution became viscous indicating that the polymer was dissolved. The resulting solution was filtrated and the sand was recovered having the same granulometric properties.

Table 6: Polymers solubility after 24h

Solvent	Temp [°C]	2EHA/AAC			EtAc/AAC			BuAc/AAC		
		3:7	5:5	7:3	3:7	5:5	7:3	3:7	5:5	7:3
pH 14	20	+	+	+	+	+	+	+	+	+
pH 13	20	+	+	-	+	+	+	+	+	+
pH 12	20	-	-	-	-	-	-	-	-	-
pH 11	20	-	-	-	-	-	-	-	-	-
pH 13	30	+	+	-	+	+	+	+	+	+
pH 12	30	-	-	-	-	-	+	+	+	+
pH 11	30	-	-	-	+	-	-	-	-	-
pH 13	50	+	+	-	+	+	+	+	+	+
pH 12	50	+	+	-	+	+	+	+	+	+
pH 11	50	+	-	-	+	-	-	+	-	-

*(-) polymer not dissolved; (+) polymer dissolved



Figure 1: Polymer/sand composite disintegration

3.2. Polymeric binder for pyrotechnics

Two types of polyurea further used as binder in our pyrotechnic compositions were synthesized by mixing two amino functionalized compounds PPG2000 (or PPG4000) and TETA with an isocyanate component, IPDI. The introduction of TETA conducts to a cross-linked polymer network, which brings various advantages: a shorter reaction and curing duration enhanced mechanical properties and moisture resistance. The difference between the polyurea obtained by employing PPG2000 or PPG4000 consists in the malleability of the polymer. Thus, polyurea synthesized with PPG4000 is more flexible due to the longer aliphatic chains from its structure. Depending on the application for which it is designed, PPG2000 or PPG4000 can be utilized according to the necessary final properties of the pyrotechnic compositions. For these reactions we used 80% (wt.) PPG and 20% (wt.) TETA. The molar ratio between the isocyanate groups and the amino groups was 1:1 in both cases, and it should always have this value, even if the ratio between PPG and TETA may be different than here.

A theoretical study of the pyrotechnic compositions represents a prior stage in the development of a pyrotechnic composition, which provides information about their thermodynamic characteristics like heat of combustion and specific volume. The results obtained are illustrated in Table 7.

Table 7: Theoretical evaluation of the thermodynamic characteristics

Parameter	PC1_P	PC2_P	PC3_P
Combustion temperature - TTh. [K]	2750	3240	3250
Specific volume - $V_{0sp}Th$. [l/kg]	382	346	355
Heat of combustion - Q_vTh [kcal/kg]	750	683	697

These theoretical results can be related to the properties of the pyrotechnic composition and allow their primary evaluation. The experimental values obtained are presented in Table 8.

Table 8: Results for the heat of combustion/specific volume (condensed water)

Composition	Heat of combustion	
	Specific volume	
PC1_P	Q_v [kcal/kg]	702.6
	V_{0sp} [l/kg]	365.6
PC2_P	Q_v [kcal/kg]	644.9
	V_{0sp} [l/kg]	308.5
PC3_P	Q_v [kcal/kg]	670.4
	V_{0sp} [l/kg]	370.8

The heat of combustion and specific volumes experimentally determined are in good agreement with the theoretical evaluations made using CEA software. From the analysis of data from Tables 7 and 8, it is obvious that the polyurea-based compositions show slightly lower combustion heats and specific volumes, but they produce higher combustion temperatures, which is a very important feature for an illuminating composition, indicating that this material can provide good conditions for emission and excitation of the active species (barium chloride in this case) [6].

The loading density was calculated by dividing the pyrotechnic composition weight at the volume that it occupies after it is pressed and the average results are displayed in Table 9.

The loading density influences the burning rate, but this value it is also influenced by the chemical composition, the dimensions of the particles and the confinement. The average values of burning rates, flame temperature and light intensity obtained during experiments are also presented in Table 9.

Table 9: Combustion experiments results

Parameter	PC1_P	PC2_P	PC3_P	PC2_H	PC3_H
Loading density – ρ [g/cm ³]	1.66	1.67	1.91	1.4	1.4
Burning rate – V_c [mm/s]	2.73	1.12	0.93	1.26	1.44
Flame temperature – T [°C]	1383	1520	1436	1378	1366
Light intensity – I [lux·m ²]	636	638	263	331	404

The cylindrical charges were burned in vertical and horizontal positions in order to evaluate if there are any differences. Charges burned horizontally showed slightly higher values. PC3_P is more flexible than PC2_P due to the longer aliphatic polyether chains in its structure; consequently, PC3_P has the highest loading density. Higher loading densities led to lower burning rates. The polyurea slows down the combustion rate but pyrotechnic effect seems to be approximately the same as in the case of PC1_P. Therefore, for approximately the same effect, the combustion will last longer, and this could be an advantage in the performance of the pyrotechnic mixture.

The mechanical properties of the pyrotechnic compositions are closely related to the type of binder employed, but also to the loading density, size of particles, confinement or environmental conditions during mechanical tests [7].

All the types of pyrotechnic compositions prepared were subjected to compression tests in order to evaluate their mechanical properties.

The compression modulus was computed at 0.2% strain, and the average values were plotted (Figure 2, a). It is obvious that PC1_P is the most rigid composition, with a compression modulus of 1700 kPa. This mechanical behavior is confirmed also by the compressive stress-strain diagram (Figure 2, b), which indicates that the PC1_P samples were much more rigid than the other compositions. The fact that increasing the applied stress leads to an increased deformation for all the other samples, states for a rearrangement of their internal structure. PC2_P and PC3_P show higher values of the compressive modulus versus PC2_H and PC3_H, respectively (Figure 2, a). The difference between the samples pressed with the hydraulic press (PC2_P and PC3_P) and the ones pressed by hand (PC2_H and PC3_H) is also noticeable in Figures 2, b and Figure 2, c. PC2_H and PC3_H have a more compact structure, which allows them to deform, but not to break when higher stress is applied.

An important aspect regarding the safety of the pyrotechnic mixtures is represented by their thermal sensitivity. The thermal behavior of the pyrotechnic compositions was studied by means of DTA and DSC analysis. DTA showed that PC1 is stable up to approximately 270°C and PC2 and PC3 up to approximately 240°C. The decomposition temperature (temperature sensitivity) varies according to the heating rate of the sample, as illustrated in Table 10. It can be noticed that the pyrotechnic compositions containing polyurea present a similar thermal behavior and they start the decomposition process earlier than PC1, due to the fact that they have a higher content of aliphatic chains in their structure.

Table 10: DTA results for the pyrotechnic compositions

Heating rate [°C/min]	PC1 decomposition temperature [°C]			PC2 decomposition temperature [°C]			PC3 decomposition temperature [°C]		
	Start	Onset	Top	Start	Onset	Top	Start	Onset	Top
10	237	262	269	201	231	238	198	223	239
15	230	269	277	180	236	244	206	229	246
20	235	273	282	174	243	253	205	233	249
25	237	279	291	205	251	260	204	238	256

The DSC analysis provided more accurate values of the decomposition temperatures. The results are displayed in Table 11.

Table 11: DSC results for the pyrotechnic compositions

Heating rate [°C/min]	PC1 decomposition temperature [°C]	PC2 decomposition temperature [°C]	PC3 decomposition temperature [°C]
5	263.6	237.3	244.6
7.5	273.0	244.0	252.0
10	275.1	250.9	253.0
12.5	280.9	261.8	256.0

The DTA and DSC results are in good correlation, showing similar values for the self-ignition temperature. It can be noticed that when the heating rate increases, the decomposition temperature increases too [8]. It is very important to know these values in order to establish which should be the safety measures that must be taken into account for these new pyrotechnic compositions.

Another analysis that can provide information about the thermal stability of these materials is represented by the vacuum stability test. If the pressure increases considerably, it means that the material is unstable and generates a high quantity of gaseous products.

The new pyrotechnic mixtures released an insignificant quantity of gaseous products during tests: PC1 has a specific volume of 0.934 cm³/g, while PC2 and PC3 have 0.625 cm³/g and 0.361 cm³/g specific volumes. Therefore the last two mixtures show a much better stability than PC1.

In terms of safety, there are two other tests that are usually performed on the pyrotechnic materials: sensitivity to impact and sensitivity to friction. The impact sensitivity provides information about the minimum energy required to initiate the decomposition of an energetic material. The average values of these energies for the pyrotechnic compositions are: 33 J for PC1, 40 J for PC2 and 36 J in case of PC3. The rubbery/plastic texture of the polyurea binder makes these compositions less sensitive to impact than PC1.

The same behavior was observed during the friction sensitivity tests, when there were no ignitions observed, even with the highest load, corresponding to 350 N.

The moisture content of the pyrotechnic compositions is a parameter that influences the performance of these materials. PC2 (0.13% moisture) and PC3 (0.27% moisture) have a lower content of humidity than PC1 (1.8%) due to the high hydrophobic character of polyurea.

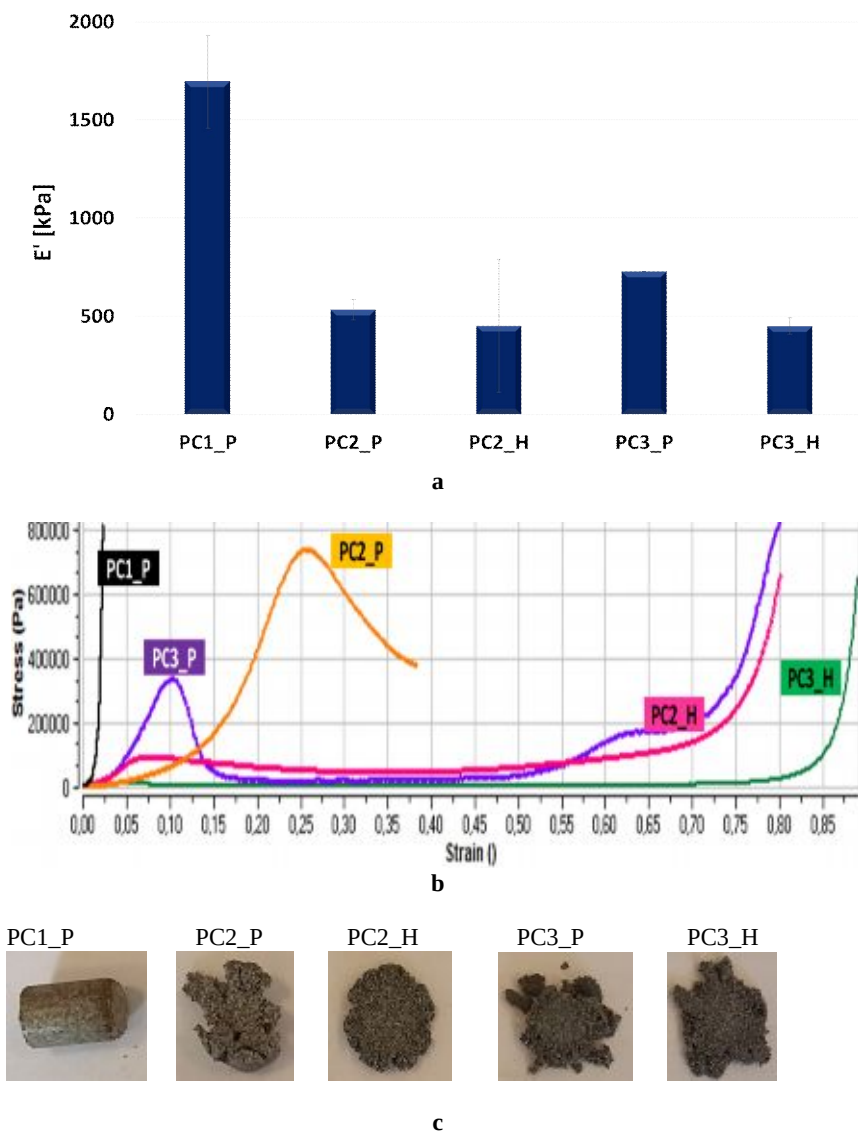


Figure 2: Compression tests

a) Average values of the compressive modulus (E' [kPa]) for the investigated compositions; b) Compressive stress-strain diagram; c) digital photographs of the compressed samples

4. Conclusions

Copolymers of acrylic acid and alkyl acrylates in different ratios were synthesized and characterized by FT-IR and DSC. The spectra analysis confirmed the presence of the specific absorptions for each monomer and the initial molar ratios of the comonomers used for obtaining each polymer. The DSC thermograms indicated how the values of T_g vary versus the content in homopolymer components. Furthermore, it was noticed that T_g 's value increases with the increasing molar ratio of AAc binder. For BuAc/AAc and EtAc/AAc copolymers, it has been observed that T_g for the copolymers with 3:7 molar ratios exceeds the T_g for pure AAc, although FT-IR spectra show the presence of BuAc and EtAc units in the copolymers. This is probably due to dehydration with formation of intra-molecular anhydride copolymer cycles during DSC analysis, which led to higher T_g values than expected. Further, it was intended for the polymers to be insoluble in water at neutral pH and soluble in weak alkaline solutions. The water uptake, the solubility in various organic solvents and also in alkaline solutions was determined. The water absorption tests showed that the percentage of absorbed water is rather low. As expected, it can be seen that the percentage of absorbed water increases with the increasing percentage of AAc units. Solubility tests in various organic solvents indicated that the solvent in which all nine synthesized polymers dissolve is DMF. The test regarding the solubility in an alkaline solution indicated that the EtAc/AAc copolymer with 3:7 molar ratio dissolved in an alkaline solution with pH 11 at 30 °C. Also, at 50 °C, other two polymers dissolve: 2EHA/AAc with 3:7 molar ratio and BuAc/AAc with 3:7 molar ratio. In order to see the behaviour of the EtAc/AAc copolymer with 3:7 molar ratio selected for further tests as binder for a filler material, the polymer was mixed with sand. It was observed that the composite pellets obtained were completely disintegrated in alkaline solution (pH 11) and the sand was recovered in the original granular size range. Thus, nine copolymers based on acrylic acid and other three comonomers: 2-ethylhexyl acrylate, butyl acrylate and ethyl acrylate were synthesized, using various molar ratios. The EtAc/AAc copolymer with 3:7 molar ratio was found to be soluble in an alkaline solution with pH 11 at 30 °C, while two other copolymers, 2EHA/AAc with 3:7 molar ratio and BuAc/AAc with 3:7 molar ratio, were found to be soluble in a pH 11 alkaline solution at 50 °C.

A new type of solvent-free binders were employed in pyrotechnic compositions and they were compared with a classical solvent-based binder. One-step preparation process, ease of reagents mixing, fast curing, homogeneity (no pores, voids or cracks), lower sensitivity, lower hygroscopicity, are a few of the advantages brought by a polyurea binder. The safety and performance characteristics of these three compositions were evaluated by performing tests and analysis specific to pyrotechnic compositions: burning experiments, thermodynamical and thermal analysis, thermal vacuum stability, compression tests, sensitivity to impact, sensitivity to friction and moisture content. These compositions were designed to generate a green color flame and it seems that the values obtained from these analyses fulfil the requirements of this type of materials. Combustion experiments showed that polyurea binders slow down the burning rate, maintaining meanwhile the flame temperature and the light intensity; thus, the same effect can be obtained for a longer period of time.

Thermal analysis and vacuum stability tests revealed that the polyurea-containing pyrotechnic mixtures are stable at temperatures above 200 °C. They also proved to have lower sensitivity to impact and friction. The compression measurements showed that their mechanical behaviour varies with their texture (rigid or flexible polyurea). The

advantage is that polyurea binder brings a series of advantages in terms of safety and performance and this material can be successfully employed in pyrotechnic compositions, and further, these new pyrotechnic compositions may be designed according to the type of application for which they are manufactured.

Acknowledgments

The work has been funded by the Romanian National Research Programs – UEFISCDI PNII Programme - Projects no 278/2014 and 305/2014.

References

1. **, STANAG 4518, Safe Disposal of Munitions, Design Principles and Requirements, and Safety Assessment, Edition 1, 2001.
2. W.G. Proud, M. Arrigoni, J.B. Ribeiro, T. Rotariu, *Greener And Safer Energetic And Ballistic Systems*, MTA Publishing House, 1st edition, 2016.
3. ***, STANAG 4556, Explosives: Vacuum stability test, 1999.
4. K.L. Kosanke, R.C. Dujay, B.J. Kosanke, *Journal of Forensic Science*, 51, no. 2, 2006, p. 296-302.
5. Eisenberg, T. Yokoyama, E.J. Sambalido, *J. Polym. Sci. Part A-1: Polym. Chem.* 7, 1969, p. 1717–1728.
6. I.S. RISTIC, Z.D. Bjelovic, B. Hollo, K. Meszaros Szecsenyi, J. Budinski-Simendic, N. Lazic, M. Kicanovic, M., *Journal of Thermal Analysis and Calorimetry*, 111, no. 2, 2012, p. 1083-1091.
7. S.K. Wang, C.S.P. Sung, *Macromolecules*, 35, no. 3, 2002, p. 883-888.
8. T. Zecheru, A. Lungu, P. Iordache, T. Rotariu, *Combustion, Explosion, and Shock Waves*, 49, no. 2, 2013, p. 204-214.

Marek Gąsiorowski, Bartosz Fikus,
**ESTIMATION OF MORTAR SHELL TRAJECTORY
USING THEORETICAL MODEL**

**Marek Gąsiorowski
Bartosz Fikus**

*Faculty of Mechatronics and Aerospace, Military University of Technology, Warsaw, Poland
marek.gasiorowski@wat.edu.pl, bartosz.fikus@wat.edu.pl*

Abstract: *In the paper the approach to modeling and results of simulations of unguided artillery shell is presented. Basing on the literature and self - conducted investigations the characteristics of physical model were identified. Using results of experimental investigations, the under investigation model and characteristics were verified, which proved acceptable accuracy of whole modeling process.*

Keywords: *numerical simulation, external ballistics, flight's dynamics*

1. Introduction

One of the approaches applied in estimation of ballistic potential of weapon is the theoretical simulation of projectile's flight. Obviously, its results are not as reliable as these obtained by the experimental investigations, but the main advantage of theoretical modeling are low costs, time consumption and possibility of simulations of whole process in various conditions. Low cost of calculation process can be significantly reduced using previously estimated characteristics for similar flying systems. In comparison to distributed – parameters theoretical models (using e.g. finite volume method in solution of systems of partial differential equations for estimation of aerodynamic characteristics), in used approach, the aerodynamic properties of objects are estimated using previously obtained, and approximated by proper expressions, data [1, 2]. These data are the most often estimated in the experimental way (due to lack of numerical tools in the past), so this approach to determination of characteristics is relatively accurate. Similar approach is also applied in commercial software (e.g. PRODAS [3]). Finally, the whole problem of estimation of projectile's trajectory is reduced to solution of proper system of ordinary differential equations. Moreover, using the correction coefficients, evaluated from selected experimental results, it is possible to ensure the acceptable accuracy of results, which can be applied in fire control systems. Taking into account the above – mentioned advantages of under consideration approach to the problem of estimation of ballistic potential of artillery, in presented work the theoretical approach to modeling of flight of mortar shell was shown.

2. Physical and mathematical model of the problem

During the development of physical model of the flight (Fig. 1) the projectile was treated as the rigid body, characterized by 6 degrees of freedom (6 DOF flight model). As the result of the first part of works, the physical quantities defining projectile construction, environment of its motion and relation between projectile and surrounding environment were established.

In presented investigations it was assumed that the motion of shell is the effect of external resultant force, which consists of aerodynamic force R_A and gravity force G :

$$\bar{F}_R = \bar{R}_A + \bar{G} \quad (1)$$

For low altitudes of flight, the gravity force can be assumed as the constant:

$$\bar{G} = m \bar{g} \quad (2)$$

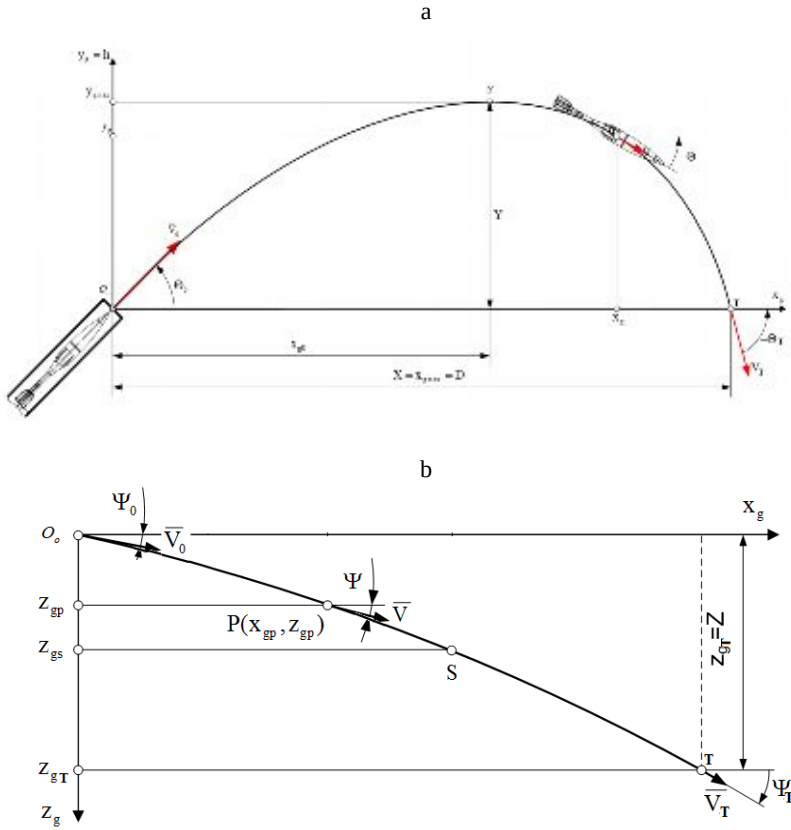


Figure 1. Sketch showing the motion of projectile in accordance with 6 DOF model (a – vertical plane; b – horizontal plane).

The aerodynamic force consists of three components:

$$\left. \begin{aligned} X_a &= C_{xa} \frac{\rho V_a^2}{2} S \\ Y_a &= C_{ya} \frac{\rho V_a^2}{2} S \\ Z_a &= C_{za} \frac{\rho V_a^2}{2} S \end{aligned} \right\} \quad (3)$$

In above – presented expressions the X_a , Y_a , and Z_a denotes drag, lift and side force, respectively. C_{xa} , C_{ya} , C_{za} are the coefficients of previously mentioned forces; ρ , V_a and S are air density, velocity of projectile relatively to surrounding medium and projectile's cross – section area. Presented quantities are expressed in the reference frame related with the flow ($0x_a y_a z_a$).

Moreover, the projectile rotates due to acting of the following aerodynamic torques:

$$\left. \begin{aligned} M_x &= m_x \frac{\rho V_a^2}{2} SL \\ M_y &= m_y \frac{\rho V_a^2}{2} SL \\ M_z &= m_z \frac{\rho V_a^2}{2} SL \end{aligned} \right\} \quad (4)$$

M_x , M_y and M_z are the components of aerodynamic torque, expressed in the reference frame related to the projectile ($0xyz$); m_x , m_y , m_z are the coefficient of torques, L is the characteristic length.

The sketch of forces and torques acting on the projectile and applied reference frames were shown in the Fig. 2.

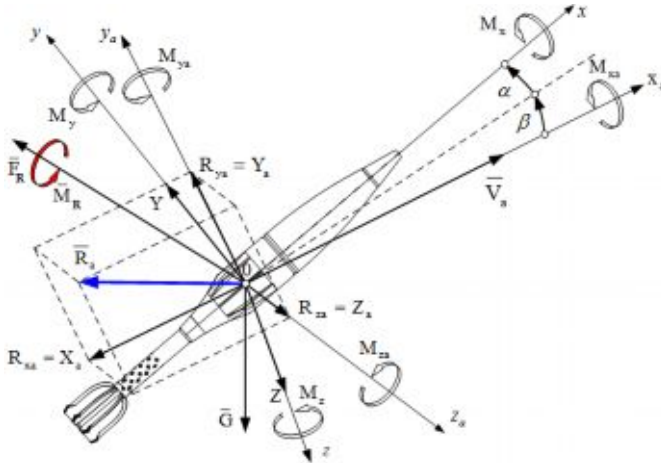


Figure 2. Sketch of forces and torques acting on the projectile.

Values of derivatives of aerodynamic characteristics with respect to the flight's parameters were determined theoretically. Using these derivatives it is possible to estimate values of coefficients of aerodynamic forces and torques:

$$\left. \begin{aligned} C_{xa}(Ma, \alpha, \beta) &= C_{xa0}(Ma) + C_{xa}^{\alpha^2}(Ma)(\alpha^2 + \beta^2) \\ C_{ya}(Ma, \alpha) &= C_{ya}^{\alpha}(Ma)\alpha \\ C_{za}(Ma, \beta) &= C_{za}^{\beta}(Ma)\beta \\ m_x(Ma, \bar{\omega}_x) &= m_x^{\bar{\omega}_x}(Ma)\bar{\omega}_x \\ m_y(Ma, \beta, \bar{\omega}_y) &= m_y^{\beta}(Ma)\beta + m_y^{\bar{\omega}_y}(Ma)\bar{\omega}_y \\ m_z(Ma, \alpha, \bar{\omega}_z) &= m_z^{\alpha}(Ma)\alpha + m_z^{\bar{\omega}_z}(Ma)\bar{\omega}_z \\ \bar{\omega}_x &= \omega_x \frac{L}{V}, \bar{\omega}_y = \omega_y \frac{L}{V}, \bar{\omega}_z = \omega_z \frac{L}{V}, \end{aligned} \right\} \quad (5)$$

where C_{xa0} denotes coefficient of drag force for angle of attack and slide angle (α and β) equal to 0; $\omega_x, \omega_y, \omega_z$ are the components of projectile's angular velocity.

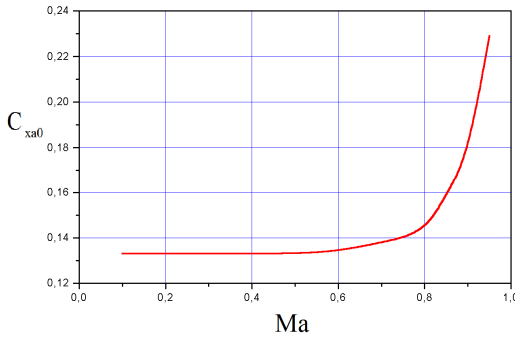
Additionally, taking into account projectile's symmetry, the following relations can be used:

$$\left. \begin{aligned} Y_a^{\alpha} &= -Z_a^{\beta}; & Y_a^{\beta\omega_x} &= -Z_a^{\alpha\omega_x}; \\ M_y^{\beta} &= M_z^{\alpha}; & M_y^{\omega_y} &= M_z^{\omega_z}; \\ M_y^{\alpha\omega_x} &= M_z^{\beta\omega_x} \end{aligned} \right\} \quad (6)$$

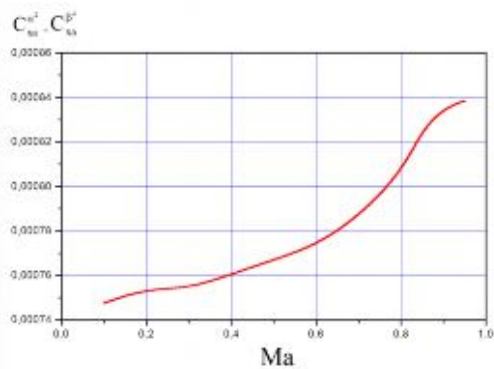
The atmosphere applied in presented model is accordant with ISO Standard Atmosphere [4].

In the Fig. 3 and 4 the selected dependences of above – mentioned quantities, as the function of Mach number Ma , were shown.

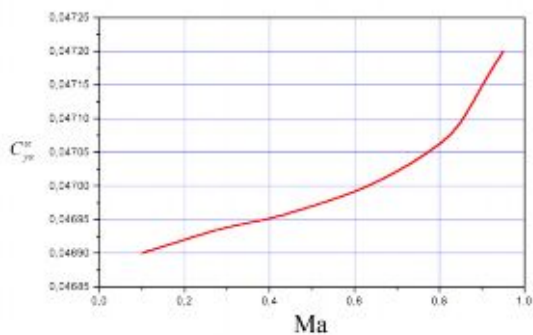
a



b



c



d

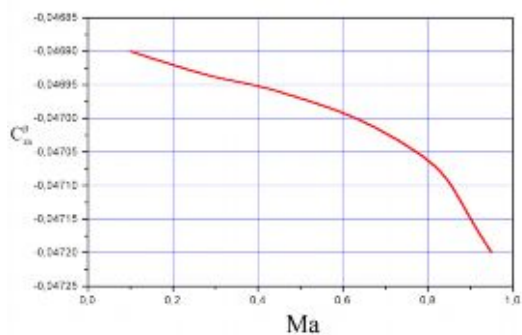
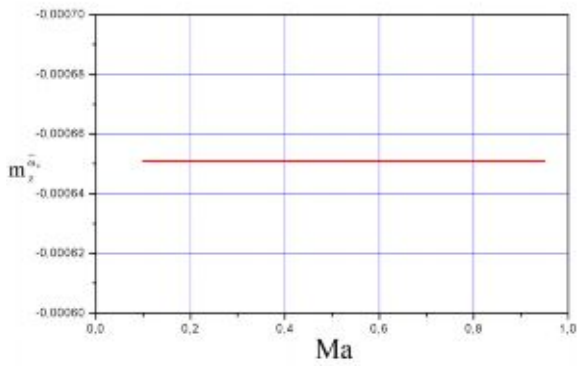


Figure 3. Selected derivatives of aerodynamic coefficients as the function of Mach number ($a - C_{x\alpha 0}$, $b - C_{x\alpha}^{a^2}$, $c - C_{y\alpha}^a$, $C_{z\alpha}^{\beta}$).

a



b

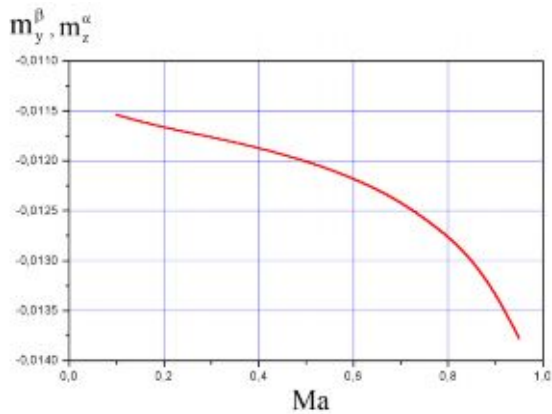


Figure 4. Selected derivatives of aerodynamic coefficients as the function of Mach number (a - $m_z^{\omega_z}$, b - m_y^{β} , m_z^{α}).

In order to obtain the flight parameters of investigated projectile, it is necessary to solve the following system of equations:

- dynamic equations of translational motion:

$$\left. \begin{aligned} \frac{dV}{dt} &= -\frac{X_a}{m} - g(y_g) \sin \Theta \\ \frac{d\Theta}{dt} &= \left[(Y_a^\alpha \alpha + Y_a^{\beta\omega_x} \beta \omega_x) \cos \gamma_a - (Z_a^\beta \beta + Z_a^{\alpha\omega_x} \alpha \omega_x) \sin \gamma_a \right] \frac{1}{mV} - \frac{g}{V} \cos \Theta \\ \frac{d\Psi}{dt} &= - \left[(Y_a^\alpha \alpha + Y_a^{\beta\omega_x} \beta \omega_x) \sin \gamma_a - (Z_a^\beta \beta + Z_a^{\alpha\omega_x} \alpha \omega_x) \cos \gamma_a \right] \frac{1}{mV \cos \Theta} \end{aligned} \right\} \quad (7)$$

- dynamic equations of rotational motion:

$$\left. \begin{aligned} \frac{d\omega_x}{dt} &= \left[M_x^{\omega_x} \omega_x + (I_y - I_z) \omega_y \omega_z \right] \frac{1}{I_x} \\ \frac{d\omega_y}{dt} &= \left[M_y^\beta \beta + M_y^{\omega_y} \omega_y + M_y^{\alpha\omega_x} \alpha \omega_x + (I_z - I_x) \omega_x \omega_z \right] \frac{1}{I_y} \\ \frac{d\omega_z}{dt} &= \left[M_z^\alpha \alpha + M_z^{\omega_z} \omega_z + M_z^{\beta\omega_x} \beta \omega_x + (I_x - I_y) \omega_x \omega_y \right] \frac{1}{I_z} \end{aligned} \right\} \quad (8)$$

where I_x, I_y, I_z denotes components of momentum of inertia of projectile.

- kinematic equations of rotational motion:

$$\left. \begin{aligned} \frac{d\vartheta}{dt} &= \omega_y \sin \gamma + \omega_z \cos \gamma \quad \left(\vartheta \neq n \frac{\pi}{2} \right) \\ \frac{d\gamma}{dt} &= \omega_y - (\omega_x \cos \gamma - \omega_z \sin \gamma) \tan \vartheta \\ \frac{d\psi}{dt} &= (\omega_y \cos \gamma - \omega_z \sin \gamma) \frac{1}{\cos \vartheta} \end{aligned} \right\} \quad (9)$$

- kinematic equations of translational motion:

$$\left. \begin{aligned} \frac{dx_g}{dt} &= V \cos \Theta \cos \Psi \\ \frac{dy_g}{dt} &= V \sin \Theta \\ \frac{dz_g}{dt} &= -V \cos \Theta \sin \Psi \end{aligned} \right\} \quad (10)$$

Above equations should be supplemented by the additional expressions, which flows from the transformations between reference frames:

$$\left. \begin{aligned}
\beta &= \arcsin[\cos \Theta \sin(\psi - \Psi) \cos \gamma + \\
&\quad + \cos \Theta \sin \vartheta \cos(\psi - \Psi) \sin \gamma - \sin \Theta \cos \vartheta \sin \gamma] \\
\alpha &= \arcsin\left\{\left[\cos \Theta \sin \vartheta \cos(\psi - \Psi) \cos \gamma - \sin \Theta \cos \vartheta \cos \gamma + \right. \right. \\
&\quad \left. \left. - \cos \Theta \sin(\psi - \Psi) \sin \gamma\right] \frac{1}{\cos \beta}\right\} \quad \left(\beta \neq n \frac{\pi}{2}\right) \\
\gamma_a &= \arcsin\left\{\left[\sin \Theta \sin(\psi - \Psi) \cos \gamma + \cos \Theta \cos \vartheta \sin \gamma + \right. \right. \\
&\quad \left. \left. + \sin \Theta \sin \vartheta \cos(\psi - \Psi) \sin \gamma\right] \frac{1}{\cos \beta}\right\} \quad \left(\beta \neq n \frac{\pi}{2}\right)
\end{aligned} \right\} \quad (11)$$

3. Results

As the result of solution of presented system of ordinary differential equations, the trajectory of under investigation shell was obtained. The calculations was conducted for two values of initial angle of elevation (Θ_0) and four values of initial velocity. The results of theoretical calculations was compared with tabular results, which are close to experimental data. These data were summarized in the Table 1. Moreover, as the exemplary result of modeling, in the Fig. 5, the trajectory of the projectile for two values of initial velocity and $\Theta_0 = 45^\circ$ were shown.

Table 1.
Comparison of the results of calculations with the tabular data

No.	Initial velocity V_0 [m/s]	Initial elevation angle [deg.]	Tabular maximum altitude [m]	Tabular maximum range [m]	Maximum altitude obtained from calculations [m]	Maximum range obtained from calculations [m]
1	325	45	2107	7227	1942	6441
2	325	85	4079	1285	3739	1141
3	270	45	1580	5605	1492	5131
4	270	85	3065	987	2875	900
5	211	45	1023	3764	987	3540
6	211	85	1996	656	1914	612
7	154	45	570	2166	559	2095
8	154	85	1119	378	1092	357

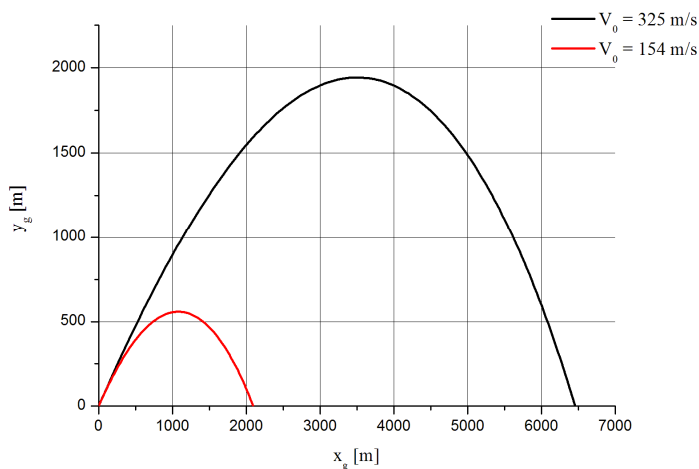


Figure 5. Trajectory of projectile for two values of initial velocity and one value of initial angle of elevation $\theta_0 = 45^\circ$.

4. Conclusions

The results of works showed the acceptable accuracy of presented model. In case of the shortest available range the relative error of range estimation was about 6 %. For the maximum range available for considered weapon, this error was equal to 11 %. The most probable reason of discrepancies can be error of estimation of ballistics characteristics of the flying object. Introduction of proper correction coefficients would reduce obtained divergence.

References

1. Gacek J., Modeling and investigations of dynamic properties of ballistic objects (in Polish), Military University of Technology, Warsaw, 1992.
2. Lebediew A. A., Czernobrowkin L. S., Dynamics of flight (in Russian), Moscow, 1973.
3. PRODA3 v3 user manual.
4. The ISO Standard Atmosphere, ISO 2533, 1975.

Sandru Vasile,

COMPARATIVE ANALYSIS OF SURFACE BASED AIR DEFENSE SYSTEMS' FIRE CONTROL UNIT

Şandru Vasile

Air Force Academy Henri Coandă, Braşov, Romania

Email svasile1966@yahoo.com

Abstract: *This paper provides a comparative study regarding the importance of fire control systems and the need to develop and automatization of Ground Based Air Defense units. The systems comparison is based on the SWOT method and multi-criteria analysis for three of the Anti Aircraft Artillery systems. The results obtained highlighted the importance of anti-aircraft artillery firing effectiveness using Fire Control Unit.*

Keywords: *Performance criteria, effectiveness, Fire Control Unit, SWOT.*

1. Introduction

Anti-Aircraft Artillery combat missions consist of firing against the enemy's aerial means, land and surface of the water targets for neutralization / destruction of:

- a) planes, missile planes, UAVs, glider planes, helicopters, paratroopers and other aerial targets;
- b) tanks, armoured vehicles, artillery selfpropelled installations, infantry and other ground targets;
- c) human force, marine (fluvial) assault, barges, pontoon bridges and other naval targets from coastal districts.

The principles which underline the firing procedures in Air Defense field are: assurance of firing effectiveness, meaning the most frequent target destruction, assuring the firing economicity, meaning destroying the target in the shortest time using minimum rounds consumption, the firing simplicity, which will finally determine clear and easy to remember orders, using rules of firing without complicated calculus – which will allow quickly decision making and advisably fire opening in complex situations, without affecting the effectiveness and the economicity [2]. Accuracy, spontaneity and continuity are the most important requirements in order to achieve the firing effectiveness [3].

2. Basic features of Air Defense guns

The anti-aircraft firing system is characterized by a number of parameters and specific features, which show entirely the possibility to accomplish the mission and assure, at the same time, the command subsystem orientation for improvement or reconfiguration. [1]

The main characteristics of antiaircraft guns are: the power, the mobility, the firing accuracy, the reliability of weapons ammunition functioning and also the weapons and ammunition safety operation [3].

a) *The power* is influenced by the single hit effect which depends on: the round's kinetic energy, the angle of incidence (the optimal one is 90° and gets lower for 60°), the caliber (increases according to the armour thickness), the round's weigh and shape, the disruptive charge (more powerful explosive, like trimethylenetrinitramine compared to TNT), the fuse (by its safety functioning at the right time).

Also the power can be influenced by the rate of fire: theoretical (the number of rounds which can be shot in a time unit, 1 minute, without the loading, sighting and firing correction time) and practical (real time rounds number). The rate of fire increases if the components are smaller, fewer and for low caliber rounds, but it gets lower for big, heavy rounds, for long actions and big components. Another power influencing factor is the effective firing range.

b) *The mobility* depends on: the weapon's weight, the moving means and the rapidity of passing from the fighting position to the marching position and vice versa.

c) *The firing accuracy* influences the effect on target assuring a reasonable ammunition consumption and depends on plenty of factors such as:

- the recoil force which influences directly the angle of curvature;
- the barrel's vibrations, which influence the trajectories dispersal;
- the manufacturing conditions
- the level of processing and smoothing the mechanisms;
- the barrel's attrition – the loading chamber widening leads to the decrease of the muzzle velocity, so the dispersal increases and the accuracy decreases;
- the sights devices must be correctly operated and assembled;
- the position of the gravity center – presumes checking implies the elastic connection;
- the ammunition – the homogeneity of the charging powder, the difference between humidity and temperature, changing the normal round's and powder weight influence the firing accuracy;
- the atmospheric conditions and taking them into account in calculating the firing elements (the air density and temperature, the wind direction and speed, the atmospheric pressure);
- calculating the firing elements is influences by the quality of checks done before the firing and the accuracy of establishing the target's current position elements (the quality of operators training);
- the fire execution to be done at the maximum effective range, and the firings by direct sighting to be corrected.

d) *The reliability of the guns and ammunition functioning* is influenced by the following factors:

- working in high temperature variations;
- the equipment submission to hard and long efforts;
- the different attrition level of components and mechanisms;
- the different reliability of mechanical, electrical, electronical, hydraulic and pneumatic components;
- fire incidents;
- the existance of doubled mechanisms (ex. the fire starting mechanism);

- the properly exploitation of guns.
- e) *The safety functioning of weapons and ammunition (S) is influenced by:*
 - the simplicity of weapons and ammunition building;
 - the cannon's type: automatic, semiautomatic and non-automatic;
 - compliance with the exploitation and maintenance rules;
 - the convenience of system servicing.

3. Benchmarking according the Air Defense systems

3.1. The SWOT analysis of Air Defense systems

Comparative study, according to strengths next to weaknesses, opportunities, and threats was performed with SWOT method taking into account three Air Defense systems, marked with C_1 for 2x35 mm. size Oerlikon Air Defense system, C_2 for 2x35 mm. size Gepard system, and C_3 for PZA Loara one. At the same time the strengths are noted with $S_1, \dots, S_5$, weaknesses with $W_1 \dots W_4$, opportunities with $O_1, \dots, O_3$, and threats T_1, T_2 . Weighting were calculated using multi-criteria analysis. [5] [9]

The SWOT analysis results for the proposed artillery systems are presented in tabel nr.1.

Table 1.
The SWOT analysis results

System	Strengths	Weaknesses
	(S) P_i	(W) P_i
C_1	S_1 : 13.95; S_2 : 46.80; S_3 : 5.04; S_4 : 1.50; S_5 : 22.8.	W_1 : 40 ; W_2 : 9; W_3 : 20.7; W_4 : 2.
C_2	S_1 : 12.4 ; S_2 : 46.8; S_3 : 6.48 ; S_4 : 1.35; S_5 : 28.5.	W_1 : 35; W_2 : 8; W_3 : 13.98; W_4 : 1.6.
C_3	S_1 : 15.5; S_2 : 52.0 S_3 : 6.48; S_4 : 1.2 S_5 : 25.65.	W_1 : 35; W_2 : 8; W_3 : 13.98; W_4 : 1.6.
	Opportunities	Threats
	(O) P_i	(T) P_i
	O_1 : 33.33; O_2 : 33.33; O_3 : 33.33.	T_1 : 50; T_2 : 50.

The criteria proposed in order to define the strengths (S) are:

- S_1 : the fought target velocity (V_t);
- S_2 : the effective range (R_e);
- S_3 : the crew protection (P_s);
- S_4 : camouflage (C_s);
- S_5 : the movement velocity (V_a).

Determining the weight of every criterion is made with the next formula:

$$\Gamma_i = (p+m+0,5+\Delta p)/(-\Delta p + N_{\text{crit}}/2) \quad (1)$$

where:

p - the sum of obtained points (on the line) by the took into account element;

m - the number of outclassed criteria by the took into account criteria;

Δp - the difference between the score of the took into account element and the last leveled one;

$-\Delta p$ - the difference between the score of the took into account element and the first leveled one;

N_{crit} - the number of considered criteria.

The criteria according the weaknesses (W) are:

- W_1 : rebuilding the combat readiness (R_w);

- W_2 : the weight (G_w) ;

- W_3 : the movement on the battlefield (D_w);

- W_4 : the system functioning depending on temperature (T_w) .

Founding the weigh of every criterion is made with the same formula (1).

The final results of the SWOT analysis and the multicriterial analysis for the Air Defense systems are represented in figures 1for C_1 , 2 for C_2 and 3 for C_3 .

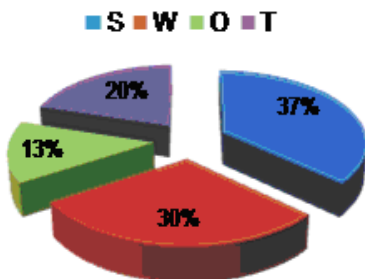


Figure 1. The SWOT / C_1 diagram

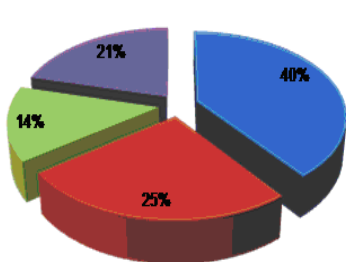


Figure 2. The SWOT / C_2 diagram

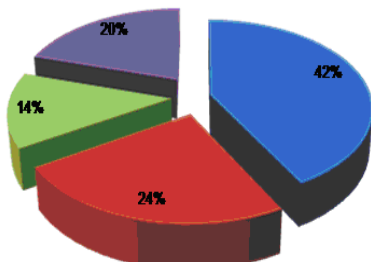


Figure 3. The SWOT / C_3 diagram

3.2. The multicriterial analysis applied for Fire Control system

For this benchmarking of three of the fire control systems, I used the advanced multicriterial analysis, method which was created by the proffesor F. Zwichy

and used for the foundation of a possible endowment decision based on some criteria and the procurance of solutions classifications [1].

The criteria of the analysis illustrated in figure 4 are:

1. The ability to integrate with other systems (C);
2. The number of managed targets (N);
3. Choosing the primary targets (P);
4. Endurance for jamming (B);
5. The time of data processing (T).

The results explanation. Explaining the results, it can be observed that the fire unit of the PZA Loara complex is on the first place after the benchmarking choosing their criteria and weigh was created by the operator's view (the Air Defense soldier).

The classification resulted from the upper benchmarking emphasizes that the modern fire control systems, adapted to requirements which are in countinuously battlefield changing, accurate and a little sensitive to enemy betrayal actions, prevail.

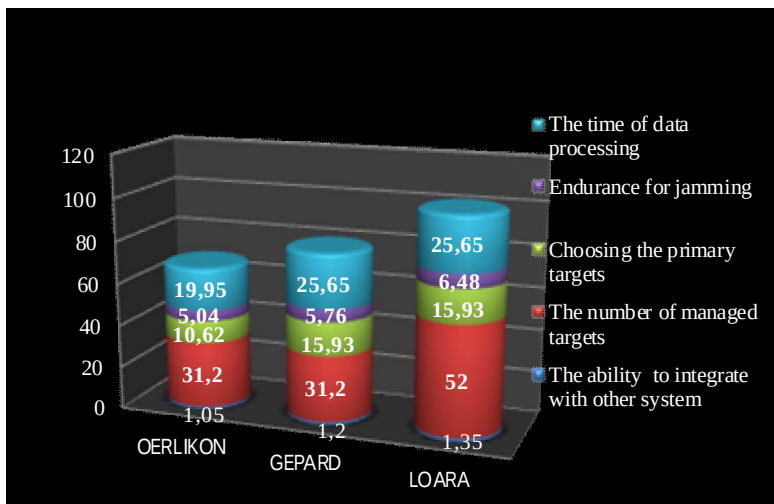


Figure 4. The diagram / the result of the multicriterial analysis

4. The simulation of fire control with the MATLAB programme

The scenario will consist in an ideal situation when there are no friction and the velocities are constant.

I started from the hypothesis that the muzzle velocity of the round is 1100 m/s, the elevation angle noted ε and the azimuth angle noted β will be constant. The target is straight-line uniform flying with a velocity of 200 m/s at a constant altitude of 2000m from the ground.

In this scenario there are four cannons, coordinated by two Fire Control systems, one for each two guns. The fire will be open when the target will be at a distance of 4000 m. or a smaller one.

In order to realise this graphic representation I used the following algorithm:

- In plan, the round's trajectory is presented in the figure 5.

The round's movement is divided into two components:

a) On vertical: the movement is done with the initial velocity v_{0y} and the acceleration $a = -g$:

$$v_y = v_{0y} + at = v_{0y} - gt \quad (2)$$

$$v_y = 0 \Rightarrow t_{urcare} = \frac{v_{0y}}{g} = \frac{v_0 \sin \varepsilon}{g} \quad (3)$$

b) On horizontal: the movement is uniform with the velocity v_{0x} . [3]

$$x(t) = x_0 + v_{0x} t \quad (4)$$

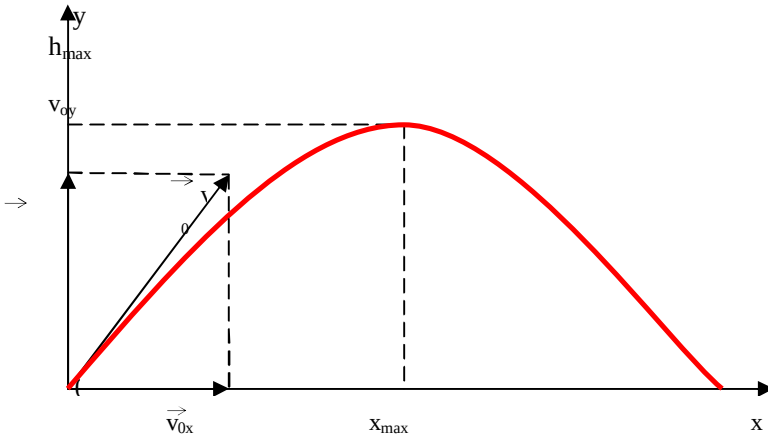


Figure 5. Projectil trajectory

Finally, the precise equation of the trajectory in plan will be:

$$y = -\frac{g}{2} x^2 + x \cdot v_0^2 \sin^2 \varepsilon \quad (5)$$

a) On vertical: the movement is done with the velocity v_z :

$$v_x = v_{0x} - gt \quad (6)$$

In order to achieve the target, ε must have a specific value so that $h_{\max} > 2000$ m.

.

b) On horizontal: the uniform movement has a component on the v_{0xy} direction:

$$dxy(t) = dxy_0 + v_{xy}t \quad (7)$$

The cannons will be arranged in the battlefield like in the figure 6:

Theoretically, when the Fire Control system is calculating all of the data and send the fire command, all the four projectiles hit the target. The situation is represented in the figure 7 a.

Practically, the chances that all the projectiles hit the target are small. This happens because of the external factors, such as the attention and rapidity of the operator to open the fire at the right time. I represented this situation, by a programme of azimuth angle errors β in the figure 7 b.

.

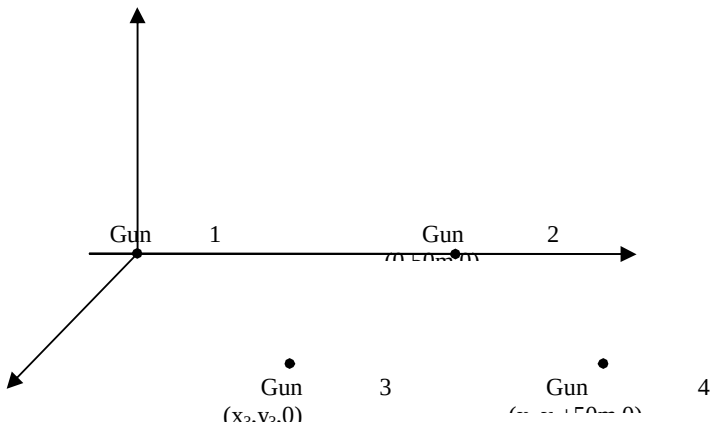
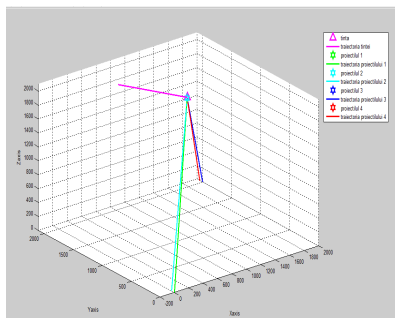
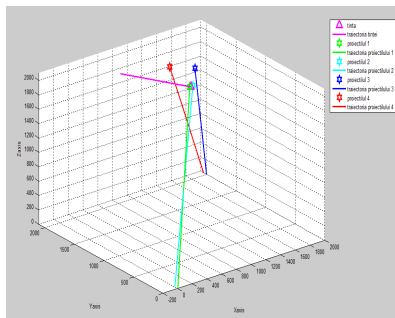


Figure 6. The cannons arrangement



a)



b)

Figure 7. The situations of combat the target: a) practical b) theoretical

CONCLUSIONS

Creating this type of analysis adapted to the domain of the paper sends the following message:

Regardless the established actions, the decissional process must include the following elements: build on strengths, remove the weaknesses, explore the opportunities, and clear the threats. [10]

The modern battlefield is influenced by the countinuously developing and perfectoning technologies. The modernization of the enemy aerial vectors endowments involves and forces the Air Defense to be more and more performant in order to succesfully achieve the new standards, to provail in the direct fight. If the work is done centralized, the chances to combat the target are considerably increasing.

The developing of the Air Defense fighting systems will be accelerated by adding computers, informational systems, and different technologic achievements. All these will have a decisive word in winning the armed fight.

The fire control systems assure the determination of accuracy and taking into account the target's parameters, the own instalation's features, the ballistic correction according to the field and used ammunition, and also the real firing weather conditions on the battlefield, in order to find the ballistic equation which assures the meeting between the two mobiles, the proyectil and the target and the continuously maintaining of the weapons on the calculated position.

The high reaction velocity of the Fire Control system allows the discover the target, the threat identify, the quick directing of the cannon on the chosen combat target, the stable maintaining on the following direction, the introduction of new data and precised corrections, the sight and the firing in order to combat the ground targets and the aerial ones. In order to allow the quickly execution of the upper operations, the entire Fire Control system must have: sturdiness, simplicity, easy exploitation and working possibilities in regimes conditions (automatic, semiautomatic, manual and combined).

The comparison of these systems is based on the SWOT method and the multicriterial analysis for three of the Air Defebse systems Oerlikon noted C_1 , Gepard noted C_2 and PZA Loara noted C_3 . The obtained results show the importance and

necessity to develop and automatize the Fire Control systems in the Air Defense field regarding to Antiaircraft Artillery.

References

1. Ene, C., Cioacă, C., (2014), *Rachete antiaerene autodurijate*, Editura Academiei Forțelor Aeriene, Brașov.
2. Roatiș M., (2003), *Manualul instrucției artileristului antiaerian din forțele terestre*, Sibiu.
3. Șandru Vasile, Maxim I., (2013), *Teoria tragerilor antiaerene*, Editura Academiei Forțelor Aeriene, Brașov.
4. Tudorache, T. *MATLAB pentru inginerie*, disponibil pe [http:// www. tmt. ugal.ro/ crios/Support/ANPT/Tutoriale/MATLAB_IN_INGINERIE.pdf](http://www.tmt.ugal.ro/crios/Support/ANPT/Tutoriale/MATLAB_IN_INGINERIE.pdf), [accessed: 6.06. 2017].
5. Vasile Șandru, (2016), *Studiul caracteristicilor tehnice decisive ale sistemelor de apărare antiaeriană ce stau la baza deciziei de extindere a duratei de utilizare*, Editura Academiei Forțelor Aeriene, Brașov, pp107-112.
6. <http://www.pitradwar.com/wp-content/uploads/2012/03/LOARA.pdf>, [accessed: 5.03.2017].
7. [http:// militarium. net/i ndex- phoption com_ contentviewarticleid 21 samobiezny- zestaw – przeciwlotniczy – pza – pzs – loaracatid 7 polskie – projektyitemid 9/](http://militarium.net/index.php?option=com_content&view=article&id=21&Itemid=9), [accessed: 15.03.2017].
8. [http://wiadomosci. onet.pl/tylko-w-onecie/ system-obrony-polskiego-nieba-na-finiszu/z3ym3mq](http://wiadomosci.onet.pl/tylko-w-onecie/system-obrony-polskiego-nieba-na-finiszu/z3ym3mq), [accessed: 15.03.2017].
9. http://www.shiva.pub.ro/PDF/PI/Laborator_1.pdf [accessed: 3.06. 2017].
10. http://www.strategvest.ro/media/dms/file/Ghiduri%20metodologice/Prezentare_a_naliza_SWOT.pdf [accessed : 10.06.2017].

Lyubomir Lazov, Erika Teirumnieka, Edmunds Teirumnieks, Hristina Deneva,
DANGERS OF IRRADIATION OF MILITARY STAFF WITH LASER LIGHT

**Lyubomir Lazov, Erika Teirumnieka, Edmunds Teirumnieks,
Hristina Deneva**

*Rezekne Academy of Technologies, Faculty of Engineering
Address: Atbrivosanas aleja 115, Rezekne, LV-4601, Latvia*

Abstract: *Each passing year the use of lasers by the military continues to grow. Many armies from different countries are using a wide variety of lasers for specific combat tasks and actions. Traditional troops, such as infantry, artillery, naval and airborne subdivisions, now recognise the laser as a major operational element in increasing the accuracy and effectiveness of combat. Lasers are also a part of various trainings related to the educational process of the army staff.*

The purpose of this report is to provide useful and adequate information needed to minimise dangers associated with laser radiation in military and training activities of the Army. The assessment made in the report is based on the ability of laser beam to cause biological damage to the eye during laser system's malfunction or inability to protect the military staff from laser radiation. International classification of laser systems (from Class 1 – considered as safe to Class 4 – very dangerous) and Standard for Laser Product (DIN EN 60825 – 1:2001-11) is used about some estimates and calculations.

Key words: *laser, laser safety, maximum permissible exposure, laser hazard classification*

1. Introduction

Artificial optical radiation sources are widely used by the military: Searchlights, Lighting at military airfields, Infrared communication systems, Laser target designators, High Energy Lasers (HEL) and others. During combat operations, commanders may need to take decisions on the level of laser radiation and to weigh the risk of real injury, death or other hazards. In this report we will only deal with the physical aspects of laser hazards for proper staff training and not with combat guidance.

How much exposure to laser light is hazardous during military activity or exercises for the military personnel? To answer this question, you have to take into account the output characteristics of the laser. Those characteristics include wavelength, output energy and power, size of the irradiated area, and duration of exposure. If you are using a pulsed laser, you must also consider the pulse repetition rate [1].

The output power of modern day lasers ranges from milliwatts (mW) to megawatts (MW) in cases where they deliver continuous output power, or even petawatts (10^{15} W) for short pulse lasers. In military terms, lasers with continuous output powers greater than 20 kW are classified as High Energy Lasers (HEL). Output powers in the range of kilowatts or even megawatts allow the creation of laser beams with potentially harmful intensity over distances of up to several hundred kilometres. These beams can be used to heat up targets, which then may lead to structural failure of the target object. Such beams can cause irreparable eye damage and the blindness of enemy soldiers and officers. The dangers of laser radiation for army staff can occur in the following three cases: training, military combat, as well as setup and service of laser sources and systems.

2. Maximum permissible exposure and nominal hazard zone

Sensitivity to a given wavelength varies significantly from person to person.

Maximum permissible exposure (MPE) limits indicate the greatest exposure that most individuals can tolerate without sustaining injury.

The MPE is usually expressed in terms of the allowable exposure time (in seconds) for a given irradiance (in watts/cm²) at a particular wavelength. Table 1 gives the maximum permissible exposure for the eye for a variety of lasers operating at different irradiance levels. For example, for an argon laser operating at 0.514 μm, the MPE is 2.5 · 10⁻³ W/cm² for an exposure time of 0.25 seconds; 16.7 · 10⁻⁶ W/cm² for an exposure time of 600 seconds; and 1 · 10⁻⁶ W/cm² for an exposure time of 3 · 10⁴ seconds. Knowing the MPE values is useful for determining the optical densities for glasses or windows and hence for the protection of military personnel.

Table 1. Maximum permissible exposure limits MPE level W·cm⁻²

	0.25 s	10 s	10 min	500 min
CO ₂ (CW) λ = 10.6 μm	-	100 · 10 ⁻³	-	100 · 10 ⁻³
Nd:YAG (CW) λ = 1.33 μm	-	5.1 · 10 ⁻³	-	1.6 · 10 ⁻³
Nd:YAG (CW) λ = 1.064 μm	-	5.1 · 10 ⁻³	-	1.6 · 10 ⁻³
Nd:YAG (Q swiched) λ = 1.064 μm	-	17.0 · 10 ⁻⁶	-	5.1 · 10 ⁻⁶
GaAs Diode CW λ = 0.840 μm	-	1.9 · 10 ⁻³	-	610.0 · 10 ⁻⁶
HeNe (CW) λ = 0.633 μm	2.5 · 10 ⁻³	-	-	17.6 · 10 ⁻⁶
Krypton-(CW) λ = 0.647; 0.568; 0.530 μm	2.5 · 10 ⁻³ 31 · 10 ⁻⁶ 16.7 · 10 ⁻⁶		364 · 10 ⁻⁶ 2.5 · 10 ⁻³ 2.5 · 10 ⁻³	28.5 · 10 ⁻⁶ 18.6 · 10 ⁻⁶ 1.0 · 10 ⁻⁶
Argon (CW) λ = 0.514 μm	2.5 · 10 ⁻³		16.7 · 10 ⁻⁶	1.0 · 10 ⁻⁶
XeFl-(Eximer CW) λ = 0.351 μm	-	-	-	33.3 · 10 ⁻⁶
Xel-(Eximer CW) λ = 0.308 μm	-	-	-	1.3 · 10 ⁻⁶

[Reference: ANSI Z136.1-1993]

Another quantity of interest in laser safety is called the **nominal hazard zone (NHZ)**. This zone describes the region within which the level of direct, reflected, or scattered (diffuse) laser radiation is above the allowable MPE. Table 2 lists nominal hazard zones for three common lasers, for a direct laser beam, a laser with a focusing lens attached, and diffusely scattered laser light. From the laser safety theory it is known that, in order to calculate *NHZ*, it is necessary to know the technical characteristics of the laser performing the laser radiation in the space. The data used in the *NHZ* calculations for the three lasers listed in Table 2 are given in Table 3 [2].

Table 2. Nominal Hazard Zones (NHZ) for Various Lasers

Laser type	Exposure Duration	Nominal Hazard Distance (m)		
		Direct	Lens on Laser	Diffuse
Nd:YAG	8 h	1410	11.4	1.4
	10 s	790	6.4	0.8
CO ₂	8 h	399	5.3	0.4
	10 s	399	5.3	0.4
Argon	8 h	25 200	1700	12.6
	0.25 s	505	33.6	0.25

Table 3. Laser Criteria Used for NHZ Calculations

Laser Parameter	Nd:YAG	CO ₂	Argon
Wavelength, λ μm	1.064	10.6	0.488; 0.514
Beam divergence, ψ mrad	100	500	5.0
Beam size at aperture, a mm	2.0	2.0	1.0
Beam size at lens, b mm	2.0	20.0	2.0
Beam size at aperture, a mm	6.3	30	3
Beam size at length, f_0 mm	25.4	200	200
MPE, 8 h ($\mu\text{W}/\text{cm}^2$)	$1.6 \cdot 10^3$	$1.0 \cdot 10^3$	1.0
MPE, 10 s ($\mu\text{W}/\text{cm}^2$)	$5.1 \cdot 10^3$	$1.0 \cdot 10^3$	-
MPE, 0.25 s ($\mu\text{W}/\text{cm}^2$)	-	-	$2.5 \cdot 10^3$

In the laser safety theory [3] it is shown that the NHZ for a laser of given power P and exit beam diameter b is given by the formula:

$$(1) \quad NHZ = \frac{f_0}{b} \left(\frac{4P}{\pi(MPE)} \right)^{1/2}$$

Below, based on a specific example, we will show how to calculate HNZ for a given laser and a given MPE.

If we have a CO₂ laser with a P power of 500 W, diameter of the output beam $b = 3$ cm and convex lens with focal length $f_0 = 20$ cm, we can specify the nominal hazard area (NHZ) by using formula (1)

$$NHZ = 5.32 \text{ m}$$

This value agrees with the entry in Table 2 for a CO₂ laser with exposure duration of either 8 h or 10 s using the lens-on-laser.

The time of exposure depends on whether the exposure is accidental or intended. For accidental exposures, 0.25 s is generally assumed for laser beams from 400 nm to 700 nm and 10 s or 100 s for all other wavelengths, where eye is the exposed organ. It is possible to calculate maximum power through a specified aperture for these exposure durations, before the MPE is exceeded. The results of such calculations are presented below (Table 4) for eye exposure to a continuous wave (CW) laser. Further guidance on the assessment of MPEs is available in IEC TR 60825-14.

Table 4. Maximum power through variable aperture [4]

Wavelength range (nm)	Limiting aperture (mm)	Exposure duration (s)	MPE (Wm^{-2})	Maximum power through aperture (mW)
180 – 302.5	1	10	3.0	0.0024
$\geq 302.5 - 315$	1	10	3.16 - 1000	0.0025 – 0.79
305	1	10	10	0.0079
308	1	10	39.8	0.031
310	1	10	100	0.079
312	1	10	251	0.20
$\geq 315 - 400$	1	10	1000	0.79
$\geq 400 - 450$	7	0.25	25.4	0.98
$\geq 450 - 500$	7	0.25	25.4	0.98
$\geq 500 - 700$	7	0.25	25.4	0.98
$\geq 700 - 1050$	7	10	10 - 50	0.39 - 1.9
750	7	10	12.5	0.49
800	7	10	15.8	0.61
850	7	10	19.9	0.77
900	7	10	25.1	0.97
950	7	10	31.6	1.2
1000	7	10	39.8	1.5
$\geq 1050 - 1400$	7	10	50 - 400	1.9 - 15
$\geq 1050 - 1150$	7	10	50	1.9
1170	7	10	114	4.4
1190	7	10	262	10
$\geq 1200 - 1400$	7	10	400	15
$\geq 1400 - 1500$	3.5	10	1000	9.6
$\geq 1500 - 1800$	3.5	10	1000	9.6
$\geq 1800 - 2600$	3.5	10	1000	9.6
$\geq 2600 - 10^5$	3.5	10	1000	9.6
$\geq 10^5 - 10^6$	11	10	1000	95

3. Laser safety classification

The classification of lasers is based on the concept of Accessible Emission Limit (AEL); these are defined for each laser class [5]. AEL takes into account not only the output of the laser product but also human access to the laser emission. Lasers are grouped into eight classes: the higher the class, the bigger the potential to cause harm. The risk could be greatly reduced by additional user-protective measures, including additional engineering controls, such as enclosures.

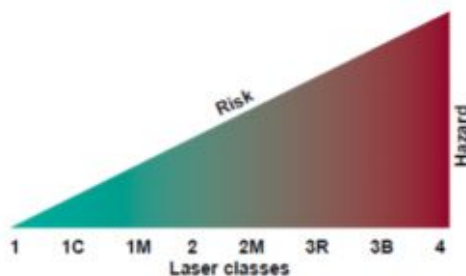


Figure 1. Eight lasers classes: the higher the class, the greater the potential to cause harm [6]

Class 1

Laser products that are considered safe during the use, including long-term direct intrabeam viewing, even when using optical viewing instruments (binoculars). Users of Class 1 laser products are generally exempt from optical radiation hazard controls during a normal operation. User maintenance or service might result in a higher level of radiation.

Class 1M

Safe for the naked eye under reasonably foreseeable conditions of operation, but may be hazardous if the user employs optics (telescopes) within the beam.

Class 1C

A laser product which is designed explicitly for contact application to the skin or non-ocular tissue. The irradiance or radiant exposure levels may exceed the skin MPE as necessary for the intended treatment procedure. During operation, ocular hazard is prevented by engineering means, i.e. the accessible emission is stopped or reduced to below the AEL of Class 1 when removed from the contact with the skin or non-ocular tissue.

Class 2

Laser products that emit visible radiation and are safe for momentary exposures, even when using optical viewing instruments, but can be hazardous for deliberate staring into the beam. Class 2 laser products are not inherently safe for eyes, but protection is assumed to be adequate by natural aversion responses, including head movement and the blink reflex.

Class 2M

Laser products that emit visible laser beams and are safe for short time exposure only for the naked eye; possible eye injury for exposures when using loupes or telescopes. Eye protection is normally provided by aversion responses, including the blink reflex.

Class 3R

Class 3R lasers — rated in power from 1 milliwatt to 5 milliwatts — cannot injure a normal person when viewed with the unaided eye but may cause injury when the energy is collected and put into the eye as with binoculars.

Direct intra-beam viewing is potentially hazardous, but practically the risk of injury in most cases is relatively low for short and unintentional exposure; however, it may be

dangerous in case of improper use by untrained persons. The risk is limited because of natural aversion behaviour for exposure to bright light in case of visible radiation and by the response to heating of the cornea in case of far infrared radiation.

Viewing of Class 2, 2M or visible-beam 3R laser products may cause dazzle, flash-blindness and afterimages, particularly in low ambient light. This may have indirect general safety implications resulting from temporary disturbance of vision or from startle reactions. Visual disturbances could be of particular concern when performing safetycritical operations, such as working with machines or at height, with high voltages or driving.

Class 3B

Lasers of 5 miles to 500 miles are dangerous to the eyes, causing damage when viewed without eye protection. This laser class requires a dangerous goods label and may have dangerous mirror reflections. Eye protection requires a dangerous goods label.

Class 4

Laser products above 500 mW for which direct viewing and skin exposure is hazardous within the hazard distance and for which the viewing of diffuse reflections may be hazardous. These lasers also often represent a fire hazard. Eye and skin protection is required.

If the opponent uses Class 3B and Class 4 lasers, a risk assessment must be performed to determine the protection measures required for safe operation.

Optical radiation is absorbed in the outer layers of the body and, therefore, its biological effects are mostly confined to the skin and eyes, but systemic effects may also occur. Different wavelengths cause different effects depending on the part of the skin or eye that absorbs the radiation, and the type of interaction involved: photochemical effects dominate in the ultraviolet region, while thermal effects prevail in the infrared region. Laser radiation can produce additional effects characterised by a very rapid absorption of energy by tissue, and is a particular hazard for eyes where the lens can focus the beam (see Table 5).

Table 5. Laser hazard for eyes at different wavelengths [7]

Wavelength (nm)		Eye
100 — 280	UVC	Photokeratitis; Photoconjunctivitis
280 — 315	UVB	Photokeratitis; Photoconjunctivitis; Cataracts
315 — 400	UVA	Photokeratitis; Photoconjunctivitis; Cataracts Photoretinal damage
380 — 780	Visible	Photoretinal damage (Blue Light Hazard); Retinal burn
780 — 1400	IRA	Cataracts; Retinal burn
1400 — 3000	IRB	Cataracts
3000 — 10 ⁶	IRC	Corneal burn

4. Biological effects of optical radiation on the eye

Light entering the eye passes through the cornea, aqueous humour, then through a variable aperture (pupil), as well as through the lens and vitreous humour to be focused on the retina (Fig. 2). The optic nerve carries signals from the photoreceptors of the retina to the brain.

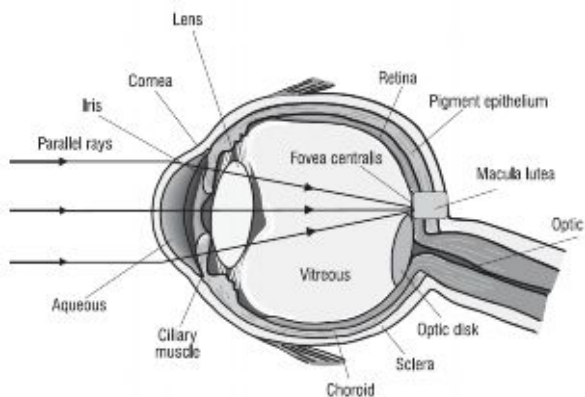


Figure 2. Schematic diagram of the eye [8]

Certain areas of the eye absorb more light in one spectral region than in others. Absorption of laser radiation above a certain level leads to a tissue injury. Figure 3 shows some absorption characteristics of the eye for different electromagnetic radiation wavelengths from 100 nm (UV-C) to 1 mm (IR- C).

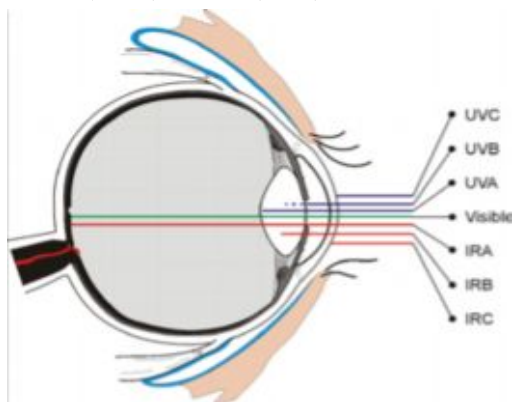


Figure 3. Penetration of different wavelength through the eye [9]

Effects on the eyes from different wavelengths [9]:

- **Ultraviolet radiation: UVC (100–280 nm); UVB (280–315 nm); UVA (315–380 nm)**

UVR falling on the eye is absorbed by the cornea and lens. The cornea and conjunctiva strongly absorb the UVR at wavelengths shorter than 300 nm. UVC is absorbed in the superficial layers of the cornea, while UVB is absorbed by the cornea and lens. UVA passes through the cornea and is absorbed in the lens. Responses of the human eye to acute overexposure to UVR include photokeratitis and photoconjunctivitis

(inflammation of the cornea and conjunctiva, respectively), more commonly known as snow blindness, arc-eye or welder's flash. Symptoms, ranging from mild irritation, light sensitivity and tearing to severe pain, appear within 30 minutes to a day depending on the intensity of exposure and are usually reversible in a few days. Chronic exposure to UVA and UVB can cause cataracts due to protein changes in the lens of the eye. Very little UV (less than 1 % UVA) normally gets through to the retina due to absorption by the anterior tissues of the eye. However, there are some people who do not have a natural lens as a result of cataract surgery, and, unless there is an implanted artificial lens which absorbs it, the retina can be damaged by UVR (at wavelengths as short as 300 nm) entering the eye. This damage is a result of photochemically produced free radicals attacking the structures of the retinal cells. The retina is normally protected from acute damage by involuntary aversion responses to visible light, but UVR does not produce these responses: persons lacking an UVR absorbing lens are therefore at higher risk of suffering retinal damage if working with UVR sources. Chronic UVR exposure is a major contributor to the development of corneal and conjunctival disorders, such as climatic droplet keratopathy (an accumulation of yellow/ brown deposits in the conjunctiva and cornea), pterygium (an overgrowth of tissue which may spread over the cornea) and probably pinguecula (a proliferative yellow lesion of the conjunctiva).

- Visible radiation (380 -780 nm)

Because the eyes act to collect and focus visible radiation, the retina is at greater risk than the skin. Gazing at a bright light source can cause retinal damage. If the lesion is in the fovea, e.g. if looking directly along a laser beam, severe visual handicap may result. Natural protective measures include an aversion to bright light (the aversion response operates in about 0.25 seconds; the pupil contracts and can reduce retinal irradiance by about a factor of 30; and the head may involuntarily be turned away). If retinal temperature increases by 10–20 °C, it can lead to irreversible damage due to denaturation of proteins. If the radiation source covers a large part of the field of view so that the retinal image is large, it is difficult for the retinal cells in the central region of the image to shed the heat quickly. Visible radiation can cause the same type of photochemically induced damage as UVR (although, at visible wavelengths, the aversion to bright light can act as a protective mechanism). This effect is more pronounced at wavelengths around 435–440 nm, and so it is sometimes called the 'Blue-Light hazard'. Chronic exposure to high ambient levels of visible light may be responsible for photochemical damage to the cells of the retina, resulting in poor colour and night vision. Where radiation enters the eye in an essentially parallel beam (i.e. very low divergence from a distant source or a laser), it may be imaged onto the retina in a very small area, concentrating the power tremendously and resulting in a severe damage. This focusing process could in theory increase the irradiance on the retina compared to that falling on the eye by up to 500 000 times. In these cases, the brightness can exceed all known natural and man-made light sources. Most laser injuries are burns: pulsed high peak power lasers can produce such a rapid rise in temperature that cells literally explode.

-IRA

Like visible radiation, IRA is also focused by the cornea and lens and transmitted to the retina. There it can cause the same sort of thermal damage as the visible radiation can. However, the retina does not detect IRA, and so there is no protection from natural

aversion responses. The spectral region from 700 to 1400 nm (IRA) is sometimes called the ‘retinal hazard region’. Chronic exposure to IRA may also induce cataracts. IRA does not have sufficient amount of energetic photons for there to be a risk of photochemically induced damage.

-IRB

At wavelengths from around 1400 nm to 3000 nm, the aqueous humour is a very strong absorber; longer wavelengths are attenuated by the vitreous humour, thus the retina is protected. Heating of the aqueous humour and iris can raise the temperature of the adjacent tissues, including the lens, which is not vascularised and so cannot control its temperature. This, along with direct absorption of IRB by the lens, induces cataracts.

-IRC

Far-infrared radiation ranging from 3000 nm to 1 mm IRC is absorbed by the cornea, and so the main hazards are corneal burns. The temperature in adjacent structures of the eye may increase due to thermal conduction, but heat loss (by evaporation and blinking) and gain (due to body temperature) will influence this process.

5. Eye protection

In light of the foregoing considerations, it can be concluded that the eyes are exposed to a huge risk of injury from laser radiation if exposures exceed exposure limits.

In addition, it must be known that PPE (Personal Protective Equipment) safety goggles only guarantee protection for a particular laser source and a specified distance for which they are specified. To adequately address the real dangers and recommendations of the Safety Advisor, he / she must know the intentions and technical parameters of the laser operative and tactical weapons available to the opponent. This is particularly important if there are multiple sources that require different types of protective eyewear, e.g. different wavelength lasers require their own unique eyewear.

The level of attenuation of optical radiation provided by protective eyewear in the hazard spectral region should be, at least, sufficient to decrease the exposure level below applicable MPEs [10].

The absorption coefficient σ_i is a property of the absorbing medium and the wavelength of the light. For eye filters (used in laser safety goggles) where the absorption coefficient for the filter is known and the filter thickness is predetermined, the product $\sigma_i x$ is replaced by a quantity called the **optical density**, described by the symbol OD . In that case, with the base 10 replacing the base e , Lambert’s law takes the following form:

$$(2) \quad E_x = E_0 10^{-OD}$$

where E_x is the irradiance after travelling through a thickness x ;

E_0 is the irradiance incident on the absorber.

Since the transmission of light through an absorber is defined as the ratio of E_x/E_0 , we can rewrite Equation 2 in a form commonly used with optical filters

$$(3) \quad T = 10^{-OD}$$

where OD – optical density;

T – transmission.

Thus, if the OD of a filter is known, the transmission through the filter can be calculated from Equation 3.

Another useful equation involves a sample calculation for the minimum optical density (*OD*) required for a specified laser power and recommended *MPE*:

$$(4) \quad OD = \log_{10} (E_0 / MPE)$$

Luminous transmittance and colour of the environment as seen through the protective filters are important characteristics of eyewear, which may affect the operator's ability to perform the required operations without compromising non-optical radiation safety. Protective eyewear should be correctly stored, regularly cleaned, and subjected to a defined inspection regime.

Conclusion

For the implementation of laser safety measures in the army, much of the trust lies in the education and training of staff: military personnel is trained to obey instructions and orders. When undertaking the risk assessment, as required by the Laser Safety Directive, consideration must be given to the military staff and to the fact that it may not always be possible to ensure that the exposure levels are below the exposure limit values.

Therefore, one approach used in this sector is Probabilistic Risk Assessment (PRA). This can be used to quantify the "probability" of risk. Various values may be adopted as a part of the PRA. However, an event with a probability of 10^{-8} is considered acceptable, even for an adverse event which, if it happened, could have catastrophic consequences. The use of PRA is complex and requires specialist expertise. However, a benefit for the military is that it may permit the use of artificial optical radiation in situations that might not be considered acceptable with a less rigorous assessment.

In order to use laser beams as weapons, a significant amount of laser output power is necessary. The output power depends heavily on the actual target. For the so-called soft targets, the minimum power to cause harm can be very low. Blinding lasers, for example, are designed to blind the human eye temporarily or permanently [11]. As the eye is very sensitive, these weapons require only a small amount of output power. Blindness can be caused in several ways: apart from burning the retina, a laser pulse can also break blood vessels inside the eye or cause a process of slow decline of the retina. At a distance of some meters, even an output power of a few milliwatts can damage the eye because the ocular focuses the beam onto the retina. This dramatically increases the intensity of the beam. Blinding lasers were used in the Falklands conflict and in the Iran/Iraq war of 1980s [12]. However, in 1995, these weapons were officially banned under International Humanitarian Law. If the aim is to destroy hard targets rather than to blind the enemy, however, the laser requires an output power which is many orders of magnitude higher than that of blinding lasers. As mentioned above in this article, many countries and research institutes develop and test lasers with continuous output power over 20 kW or impulse power over 1 kJ [13]. As stated above, the use of blinding laser weapons is illegal under International Humanitarian Law. In particular, these weapons violate the Fourth Protocol (1995) to the Convention on Prohibitions or Restriction on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. This protocol outlaws the use and transfer of laser weapons which are intended to cause blindness. Additionally, the signatories are obliged to take the necessary steps to prevent blindness caused by other laser weapon engagements [14]. However, the protocol is not applicable if collateral blinding occurs as a result of military laser applications that are otherwise considered legitimate. As a consequence, the protocol might be applicable to High Energy Lasers (HEL) weapons only, if they are

especially designed for blinding purposes. Nevertheless, the protocol seems to have had some positive effects so far. The protocol the first step towards a comprehensive ban of all laser weapons. This would be the first step towards preventive arms control, a concept which was developed to ban the introduction of new destabilising weapon systems [15].

Whether and to what extent a complete ban is realistically achievable is obviously another question.

References:

1. Measurements of Optical Radiation Hazards, A reference book based on presentations given by health and safety experts on optical radiation hazards, Gaithersburg, Maryland,

USA, September 1–3, 1998, Munich: ICNIRP/CIE-Publications, 1999. ISBN 978-3-9804789-5-3.

2. Engineering Technology, Inc. Laser Safety, Waco, Texas, 1993.

3. PD IEC/TR 60825-8:2006, Safety of laser products. Guidelines for the safe use of laser beams on humans.

4. Directive 2006/25/EC Artificial Optical Radiation.

5. BS EN 60825-1:2007 Safety of laser products. Equipment classification and requirements; PD IEC/TR 60825-13:2006 Safety of laser products. Measurements for classification of laser products

6. Ubiquitous Lasers, Training Centre Public Health England, 2016

<https://www.phe-protectionservices.org.uk/nir/courses/>

7. Laser Safety Guide, Marshall, W. and Sliney, D. (editors), Laser Institute of America, Orlando, FL, 2007.

8. The Physics Classroom: Anatomy of the Eye
<http://www.physicsclassroom.com/Class/refrn/U14L6a.html>

9. Princeton University: Laser Safety Training Guide
<http://web.princeton.edu/sites/ehs/laserguide/index.htm>

10. LIA Guide for the Selection of Laser Eye Protection, Sliney, D. (editor), Laser Institute of America, Orlando, FL, 2007

11. A Peters, “Blinding Laser Weapons: The Need to Ban a Cruel and Inhumane Weapon”, Human Rights Watch Arms Project, September 1995, vol. 7, no. 1, , pp. 1–49

12. J H McCall, Jr, “Blinded by the Light: International Law and the Legality of Anti-Optic Laser Weapons”, Cornell International Law Journal, vol. 30, no. 1, 1997, pp. 1–44

13. US Defense Threat Reduction Agency, “Section 11: Lasers and Optics Technology”, in US Department of Defense, Developing Science and Technologies List, Ft. Belvoir, 2000, <http://www.dtic.mil/mct/DSTL/Sec11.pdf>.

14. ICRC, “Treaty database of the International Committee of the Red Cross”, <http://www.icrc.org/ihl.nsf/WebFULL?OpenView> – viewed May 2005.

15. T Petermann, M Socher & C Wennrich, *Präventive Rüstungskontrolle bei Neuen Technologien. Utopie oder Notwendigkeit?*, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 3, Edition Sigma, Berlin, 1997.

INFRARED LASERS IN THE MILITARY ACTION

Lyubomir Lazov, Erika Teirumnieka, Edmunds Teirumnieks, Hristina Deneva

Rezekne Academy of Technologies, Faculty of Engineering
Address: Atbrivosanas aleja 115, Rezekne, LV-4601, Latvia

Abstract: Lasers are widely used in the military sphere. In the long term, they will be expanded through the creation of laser weapons systems. However, this still has to overcome a number of technological problems.

IR-systems of military designation are being developed in many countries. According to experts, in a number of states 3/4 of all produced IR-devices are intended for military purposes. Significant allocations for the research and production of military-grade infrared equipment show that in the armies of these states disclosing and using the high potential of infrared devices are considered to be very important.

The review article discusses some specific applications of the infrared lasers, such as Laser location, Laser systems of antimissile defence, Tactical Laser Systems, and others. It also provides assessment of the effect of laser radiation on the object depending on various factors.

Key words: Laser, Tactical Laser Systems, Laser systems of antimissile defence, Laser location

0. Introduction. Main Directions of Laser Technology

Infrared technology is a field of applied physics and technology, including the development and use of devices whose operation is based on the use of infrared (IR) radiation (electromagnetic radiation in the wavelength range from 0.77 μm to 1 mm) and its physical properties. Infrared technology includes: impulse and non-continuous lasers; devices for detecting and measuring infrared radiation, detecting ground, sea and air targets on their own thermal radiation in the infrared range of waves; observation and photographing in the dark, remote measurement of the temperature of bodies by their thermal radiation; hidden signalling, ground and space communications, infrared sights, range finders, devices for homing on the target shells and missiles.

There are active and passive infrared (IR) devices. Active devices use special sources of infrared radiation to illuminate (irradiate) targets. As such, floodlights are used, closed with light filters that are transparent to infrared rays and that do not transmit visible light, or IR lasers. Passive devices work by using their own infrared radiation objects (targets).

The main advantages of infrared technology are relative concealment of work, high resolving power and reliability with relative simplicity of design, as well as small dimensions and weight. Perfection of receivers and various methods of infrared filtering expands the possibilities of using infrared technology, especially at high altitudes and in outer space.

Its shortcomings include the dependence of the range of action on atmospheric conditions, the interfering effect of solar radiation, etc.

Over the last 10 to 15 years, infrared lasers are being introduced into the military equipment of the United States, France, Britain, Japan, Germany, Switzerland, and other

NATO countries at an accelerated pace [1,2]. These countries have enormous financial resources for projects and research in this scientific field.

Like all weapons, laser weapons have countermeasures and also have appropriate advantages and disadvantages. The advantages of using laser weapons in military affairs depending on the tasks to be solved (the targets being hit) include the following:

- Achievement of the goal at the speed of light;
- Targeting without waiting (both in height and in the side directions);
- Quick targeting opportunities (compared, for example, with missiles or missiles already launched to reach the target);
- Absence of the possibility to shoot down a striking beam (as a projectile or a rocket) can not be distracted by a heat trap, is resistant to jamming systems, etc.;
- Low price in comparison with some classical means of destruction;
- Ability to control the energy of the shot, which allows hitting different targets;
- High localisation of destruction, which makes it possible to use such systems, for example, in urban conditions without incidental losses;
- Relative silence of the shot and invisibility for the eyes (for IR, UV ranges, especially pulsed lasers);
- Logistic support of the combat use of laser weapons (especially on the basis of solid-state lasers) is much simpler than for a number of classical systems of defeat;
- Given the possibility of multiple rounds, certain types of laser weapons have the advantage of mass, which is important for aviation and other equipment.

Laser weapon has the following disadvantages::

- Impossibility of shooting behind obstacles, as well as limiting the range of firing at ground targets by the visible horizon;
- Sharp deterioration of damaging properties under unfavourable weather conditions, dust, smoke, etc.
- Problem of stability of the spot on the target and exposure time;
- In certain cases, a relatively large size (for chemical lasers).

Currently, lasers are widely used in various military systems. The directions of using lasers in the military sphere can be divided into four categories:

- Supporting combat operations,
- Guidance and use as an auxiliary element for the means of destruction,
- Repression of purpose (countering the enemy's electronic-optical means)
- Immediate defeat.

The following main directions have been developed, according to which laser technology is being introduced into military affairs. These areas are

- Laser location (ground, airborne, underwater);
- Laser communication;
- Laser navigation systems;
- Laser weapons;
- Laser missile defence and anti-space defence systems.

In the present report, we will discuss only a few specific applications of lasers in warfare, namely Laser location, Laser systems of antimissile defence, Tactical Laser Systems, and Laser radiation on the object

1. Laser Location

Laser location is an area of optoelectronics that deals with the detection and location of various objects by means of electromagnetic waves of the optical range emitted by lasers. The creation of laser systems has opened new perspectives in locating technology [3]. Basically, laser location is carried out by an active method. The objects of laser detection are primarily tanks, ships, rockets, satellites, industrial and armed structures.

At the heart of laser location, as well as in radar, there are three basic properties of electromagnetic waves:

- Ability to reflect from objects

The purpose and the background on which it is located reflect the radiation incident on them in different ways. Laser radiation is reflected from all objects: metallic and non-metallic objects, forest, land, water. Laser locator is inherent in a greater detection ability than radar, i.e. the shorter the wave, the higher it is. The power of the reflected signal P_r is inversely proportional to the wavelength of the fourth power of the laser radiation.

$$(1) \quad P_r \approx 1/\lambda^4$$

- Ability to propagate rectilinearly

With the help of a narrow-focus laser beam that is used to view a location, you can register the bearing of a moving object.

This direction is found basing on the location of axis of the optical system which forms laser radiation. The narrower the beam, the more accurately the bearing can be determined.

Simple calculations show that, in order to obtain divergence θ of about 1.5 degrees when using radio waves in a centimetre range, you need to have an antenna with a diameter of about 10 m. Such an antenna is difficult to put on a tank and even more so on a flying device, therefore a needs to use shorter waves, i.e. electromagnetic waves of the optical range emitted by lasers.

The divergence θ of the beam of a solid-state Nd: YAG laser is known to be only 1.0 to 1.5 degrees and without additional optical systems.

Dimensions of the laser locator are much smaller than the size of the analogous radar. The use of small optical systems will make it possible to narrow the laser beam to several angular minutes, if necessary.

- The ability of laser radiation to propagate at a constant speed (light speed $c = 3.10^8$ m/s) makes it possible to determine the range to the object.

With the impulse distance measuring method, the following relation is used:

$$(2) \quad L = ct/2$$

where L is the distance to the object,

c is the propagation velocity of the radiation,

t is the time of passage of a pulse to the target and back.

This relationship shows that the potential accuracy of the range measurement is determined by the accuracy of measuring the time of passage of the energy pulse to the object and back. It is quite clear that the shorter the momentum, the better.

Firstly, the zone of action. It is understood as the area of space in which observation is conducted. Its boundaries are determined by the maximum and minimum range of action and the limits of the survey by elevation and azimuth. These dimensions are determined by the designation of a military laser locator.

Another parameter is the time of the review. It refers to the time during which the laser beam produces a single view of a given volume of space.

The most important parameter of the locator is the ability to determine the coordinates, i.e. Location of surface, air and underwater objects. Here, the decisive role is the possibility of separately determining the coordinates of closely located targets, which determines the resolving power of the locator, which is defined by the length of the laser radiation λ , repetition rate of the impulses ν and their duration τ .

These characteristics of the laser locator are much better than those of the radar.

2. Battle Lasers. Laser Systems of Antimissile Defence

One of the first tasks set before the laser developers was the fight against strategic weapons of mass destruction - warheads of ballistic missiles, and later against the missiles themselves in the active phase of flight, since at that time there were no alternative means of counteraction for these purposes at all. This goal has allowed us to focus enough resources on the development of power laser systems

Regardless of the type of carrier, all laser complexes to defeat the purpose of moving targets must have an energy source that provides all systems in the complex, including the main laser source (HPL) and laser for a backlight of the target, the formation and control system ray for its guidance and retention on the target in the process of impact, system of searching, capturing and tracking the target, as well as many other auxiliary systems (see Figure 1).

For laser weapons, unlike most other applications of lasers in military science, powerful lasers are used [4, 5, 6]. Some of such lasers, already used or possible for combat use, are the following:

- Excimer lasers emit in the wavelength spectral range 193 (ArF) -351 (XeF) nm, i.e. almost at the boundary of the transparency of the atmosphere or in an area where it is not transparent. Radiation power – megawatts in continuous mode;

- Chemical HF and DF lasers. The HF laser emits at a wavelength of $2.6 \pm 3.1 \mu\text{m}$ (the transparency of the atmosphere in such a spectral range is about 10%), the DF laser emits in the spectral range 3.6 - 4.2 μm (almost 100% atmospheric transparency near 3.9 μm). Radiation power of a DF laser is megawatts in continuous radiation mode;

- Chemical oxygen-iodine laser emits at a wavelength of 1315 nm (95% transparency of the atmosphere). Radiation power in continuous mode is megawatts;

- Gasdynamic CO₂ laser. It emits at a wavelength of 10.6 μm (atmospheric transparency is about 95%). Radiation power in the continuous mode of operation is megawatts;

- Solid-state Nd: YAG and Yb: YAG lasers. Emission wavelength of an Nd: YAG laser (for a YAG crystal) is 1064 nm, for Yb: YAG is 1031 nm (almost 100% transparency of the atmosphere). Radiation power of the order of 100 kW (in modular design);

- Ytterbium fiber-optic lasers. Radiation wavelength is 1070 nm (almost 100% transparency of the atmosphere), radiation power is tens of kilowatts in the quasi-continuous mode of operation.

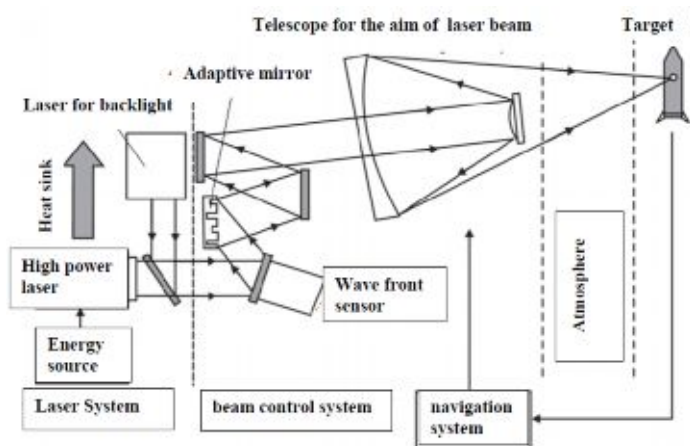


Fig. 1. Schematic diagram of the laser complex

Since the mid-nineties, a new type of NHL - the chemical oxygen-iodine laser - has been actively developed. The wavelength of the HKLE emission ($\lambda = 1,315 \mu\text{m}$) occurs in the spectral transparency window of the atmosphere, and also corresponds to the working range of fiber optics. This means that there are no fundamental limitations for the use of lasers of this type in various atmospheric and extra-atmospheric conditions. A shorter wavelength cause's reduction in the diffraction limit, and a small density of the active medium in the resonator cavity is a high optical quality of the laser beam.

The Airborne Laser (ABL) project is based on a continuous chemical oxygen-iodine laser with a capacity of several megawatts designed to destroy ballistic missiles with nuclear warheads in the active section of the trajectory, aboard a wide-body aircraft (Boeing 747-400F). The structural design and appearance of the Boeing 747F aircraft with a continuous chemical oxygen-iodine laser on board includes: Nose Mounted Turret; Bea Control System; Active Ranging System CO₂ Laser; Battle Management; Separation Bulkhead; Solid State Illuminator Laser; High Energy Laser Modules (Fig. 2).

In order to raise the temperature of the missile's hull to a critical point, it is necessary to focus a laser beam of sufficient intensity on the same spot for several seconds. Because of diffraction effects and interactions with the atmosphere, however, the beam is only focusable to a certain degree. As a consequence, it is imperative to supply an output power of several megawatts. The ABL's laser is a chemical oxygen-iodine laser (COIL). The invention of COIL dates back to the 1970s, but as its working principle is complex, other lasers can be used more easily if output powers in the kilowatt range or below are required. Hence COILs have not matured into a standard tool so far. In a COIL, several toxic chemicals (e.g. hydrogen peroxide) react with each other in order to deliver the energy that is needed to create the beam. To ensure the safety of the crew, it is necessary to seal the crew compartment air tightly from the actual laser. Since all of the laser's optical elements are extremely sensitive to misalignment, it is planned to use an automated sensor-actor system to work against the vibrations in the airplane. An adaptive optics system using a deformable mirror is supposed to compensate the turbulence in the

atmosphere between the ABL and the target. Otherwise the turbulence distorts the beam. To finally shape and direct the laser beam, a 1.5 m diameter telescope will be used. The telescope will be gimbal-mounted on the aircraft's nose (see Figure 1). The engagement of the ABL begins as soon as the missile passes the cloud cover. The missile is detected by a system consisting of three other lasers and several infrared sensors [7, 8].

Another possible task of combat employment of this complex was the defeat of satellites in a near-earth orbit.

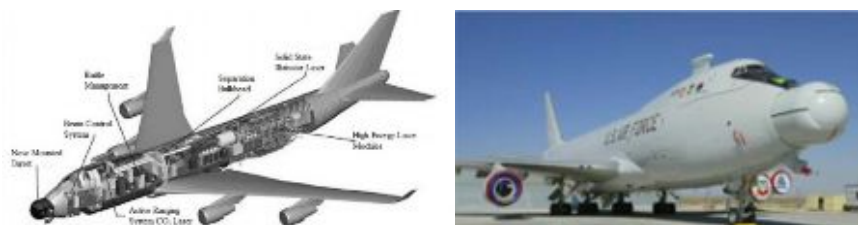


Fig. 2. Planned setup of ABL. Source: Boeing website.

The ABL project was brought to real trials, recognised as "limitedly successful," and at the end of December 2011 it became known that the US Department of Defence had closed the ABL development program. The laser development program had been conducted for 16 years, and its financing amounted to \$ 5 billion. According to the Pentagon, the ABL program was closed due to its high cost, small practical value of the technologies created and the need to cut defence spending.

To date, there is little information on the development of the ONE for the destruction of ballistic missiles or their warheads. The interest of developers of laser weapons of directed action seems to have finally shifted towards less powerful, more compact and rational (tactical) laser systems.

The review article explores some specific applications of laser infrared lasers, laser defence systems, Tactical Laser Systems and others.

3. Tactical Laser Systems

By the end of 1990s, as interest in the "strategic" tasks of using high-energy lasers in anti-ballistic missile systems declined, discussion on their possibilities in solving more limited concepts of tactical laser systems (Advanced Tactical Laser) began, firstly, on the basis of a chemical oxygen-iodine laser, and later, starting from the end of the first decade of the new century, on medium-power fiber and solid-state lasers (up to 100 kW). This has stimulated the transition from gigantism of the first generation of laser systems to more efficient and compact mobile systems designed for wider use.

An Advanced Tactical Laser (ATL) based on an oxygen-iodine laser with a power of 50 to 75 kW installed on board the NC-130H aircraft can be considered as an example of a "tactical" system. ATL can be used in reconnaissance and sabotage operations to destroy vehicles, communication lines and communications, and the destruction of energy infrastructure at distances of 8 to 10 km. The advantages of ATL are high resolution to identify a target localised with accuracy of less than a meter, as well as high mobility of a medium-sized aircraft with an ATL mounted on it.

Auxiliary laser systems of directional action "non-lethal weapon"

This laser weapon is used as an accompanying weapon, which increases the total power to counteract and prevents hostile actions.

Examples of "non-lethal weapons" are the means of limiting escalation and temporarily disabling equipment, such as laser dazzlers (dazzler), used to fight rebels, terrorists, to overthrow demonstrations and to protect infrastructure objects, i.e. in conflicts of low intensity. The laser dazzler emits a high intensity laser beam in the visible range, usually in the blue-green area, for temporary loss of the enemy's ability to view, without causing long-term damage and injury to the eyes of the object [7].

The choice of parameters, such as power, size of the spot on the target, and laser power density, depends on the task. The focusing optics is intended to achieve a nominal distance at which the required level of exposure to the eye is achieved, and the laser power density of the target [8].

To date, only one restricting international legal instrument applies to the use of laser weapons. It is the Protocol on Blinding Laser Weapons (UN, 1995) [9]. This protocol prohibits the use of laser weapons specifically designed for use in hostilities solely or including, in order to cause permanent blindness to the organs of vision of a person who does not use optical instruments. Such a weapon, which specifically causes permanent blindness to a person, relates to the forbidden, but there are no restrictions on lasers that are designed to kill a person.

4. Evaluation of the Effect of Laser Radiation on the Object

The defeat of targets is based on converting the energy of the laser beam into heat, which leads to ablation or melting of the material in the zone of action. The interaction depends on: the diameter of the laser beam and the shape of the surface of the object; laser power; the amount of radiation exposure to the target; radiation wavelength and material properties [10].

It is preferred to defeat the ICBM by its initial phase of acceleration of the flight. At the same time, fuel tanks and shell of ICBMs, which have less thermal protection in comparison with warheads, are struck. Besides, in addition, at the acceleration stage, the internal pressure in the fuel tanks is high and there is an additional load on the casing due to friction in the atmosphere

This facilitates the damage to the rocket by a laser beam: less power or exposure time is required, since it is not necessary to completely ignite the shell, and it is enough to damage it only to a certain level.

The specific energy of laser radiation E , kJ / m², required for heating the plate with thickness δ during the time of action before its destruction, is:

$$(3) \quad E = [c_p \cdot (T_m - T_0) + L_m] \cdot \rho \cdot \delta,$$

Where T_0 is the initial temperature, K;

T_m is melting point, K;

c_p is the specific heat of melting, KJ / kg.K

ρ is the density of the material, kg / m³

Then, taking into account the duration of the effect, the laser power density required for destruction,

$$(4) \quad I = E / \tau$$

Where I is laser radiation power density, kW / m²,

τ is the time of action (pulse duration) of laser radiation.

The effect is determined by the duration of the laser pulse τ and the temperature conductivity of the material χ , m² / s. It is possible to determine for which time the thickness δ , m of the substance will melt:

$$(5) \quad t_{\text{ext}} = \tau = \delta^2 / \chi,$$

where $\chi = a / \rho \cdot c_p$

a is thermal conductivity of the material, kW / m.K

Thermodynamic characteristics of some structural materials are given in Table. 1

When estimating the threshold of laser radiation destruction, it was concluded that design elements of aviation and rocket systems can be limited to simpler ratios for thin plates.

Table. 1 Thermophysical characteristics of certain materials

Materials	Melting temperature $\rho \cdot 10^3$, kg/m ³	Heat of melting c_p , kJ/kg.K	Boiling temperature a , kW/m.K	Heat of evaporation χ , m/s
Aluminium	933	393	2772	1.09
Titanium	1941	315	3560	1.00
Steel	1720...1790	205	3135	0.64
Carbon	-	-	4300	5.92

Let us determine what energy of laser radiation E is sufficient to destroy (evaporate) a layer of carbon heat protection in a thickness of 1 cm, heated almost to the temperature of destruction:

$$E \approx (\rho \cdot \delta \cdot \pi \cdot d^2 \cdot L_m) / 4$$

For carbon steel plate: $E \approx 2,6 \cdot 10^7$ J

Less stringent laser power requirements can be considered for the purposes of earlier damage to ICBMs on active trajectory sites, although in this case the laser should be located in outer space and under the conditions of direct visibility of the take-off rocket. In this case, the energy threshold of destruction is significantly reduced, for example, for a thickness of 0.5 cm of aluminium shell of tanks or propulsion installation of ICBM we obtain:

$$E = [c_p \cdot (T_m - T_0) + L_m] \cdot (\rho \cdot \delta \cdot \pi \cdot d^2 \cdot L_m) / 4 = 2,0 \cdot 10^5 \text{ J}$$

The energy threshold for the rocket carrier elements was two orders of magnitude lower than that for a warhead, but it should be borne in mind that the effect in this case is carried out at substantially large distances between the laser and the target (many hundreds and thousands of kilometers) with great relative velocities of displacement and from mobile platforms.

Yet, despite the obvious technical difficulties in implementing the task of anti-ballistic missile defence with the help of lasers, this did not stop the development of new laser systems for anti-missile defence.

It is anticipated that such systems will be able to detect and infect many different objects, such as cruise missiles, unmanned rockets and unmanned aerial vehicles, as well as ground objects, cars, missile launchers at horizontal distances from 8 to 25 km.

5. Conclusions

The main advantages of laser-based direct-energy systems are the following: light speed impact, near-zero level of accompanying damage, simultaneous multiple target defeat or quick re-targeting, resistance to electromagnetic interference, and no effect of gravity. Such systems also allow destroying flying objects silently, thus preventing panic.

Although the initial cost of developing and manufacturing laser weapons is higher comparing to kinetic weapons systems, the operating costs of direct-energy systems are negligible. This is due to the fact that, while conventional weapons systems are single-use (bullets, shells, mines, rockets), laser weapons have virtually unlimited ammunition.

Laser systems also have limitations related to the need to localise the target in the line of sight, requirements for the positioning of the laser spot on the target housing, as well as problems of atmospheric signal attenuation and turbulence.

Over the past ten years, success has been achieved in the development of powerful lasers, their efficiency has been multiplied several times, and the possibilities of mobile implementations of laser systems of the megawatt class have been demonstrated. Nevertheless, laser energy-directed systems today are in the stage of development and improvement, and only the future will show if they can become full-fledged combat systems.

The use of laser weapons in the future also depends on the development of the theory and practice of military operations.

Reference:

1. D. Litovkin Laser weapons development in full swing in U.S. and Russia, December, (2014)
2. V. V. Apollonov. American journal of modern physics 1 (1), (2012)
3. V. V. Apollonov. High power lasers and new applications. International journal of engineering research and development, v. 11, issue 03, March (2015).
4. Further information about LiDAR applications can be found at P S Argall & R J Sica, 'Lidar (Laser Radar)', in T G Brown et al, (eds), Optics Encyclopedia: Basic Foundations and Practical Applications, volume 2 G-L, Wiley-VCH, Weinheim, 2003, <http://pcl.physics.uwo.ca/pclhtml/pub/LidarPapers/Argall-Encyc-Optics.pdf>
5. "Airborne Laser System (ABL) YAL 1A," United States of America, Airforce-Technology.com, Accessed Google cached copy at <http://webcache.googleusercontent.com/search?q=cache:ZpsyFt9Wu7gJ:www.airforce-technology.com/projects/abl/+&cd=1&hl=en&ct=clnk&gl=in>
6. "Airborne Laser (ABL), Missile Threat," <http://missilethreat.com/defense-systems/airbornelaserabl/>
7. J. Stupl, Neuneck G. High Energy Lasers: A Sensible Choice for Future Weapon Systems?, Security Challenges, Volume 1 Number 1 (2005), <https://www.regionalsecurity.org.au/Resources/Files/vol1no1StuplandNeuneck.pdf>
8. A Peters, 'Blinding Laser Weapons: The Need to Ban a Cruel and Inhumane Weapon', *Human Rights Watch Arms Project*, vol. 7, no. 1, September 1995, pp. 1-49.
9. J H McCall, Jr, 'Blinded by the Light: International Law and the Legality of Anti-Optic Laser Weapons', *Cornell International Law Journal*, vol. 30, no. 1, 1997, pp. 1-44 here: pp. 5 - 6; Peters (as in n. 7), p. 3.
10. G Neuneck, 'Physik und Abrüstung - Neue Waffentechniken und Rüstungskontrolle', *Physik in unserer Zeit*, vol. 32, no. 1, 2001, pp. 10-17;

K Tsipis, 'Laser Weapons', *Scientific American*, vol. 245, no. 6, 1981, pp. 51–57.
10. V. Veiko, Petrov A., Introduction of Laser technology, Petersburg 2009
<http://books.ifmo.ru/file/pdf/460.pdf>

С. С. Евлогиев, И. Г. Кацев,

ПРЕГЛЕД НА СЪВРЕМЕННИТЕ ОПТИЧЕСКИ ПРИБОРИ ЗА РАЗУЗНА- ВАНЕ, ПРЕДНАЗНАЧЕНИ ЗА ИЗПОЛЗВАНЕ ОТ АРТИЛЕРИЙСКИТЕ ПРЕДНИ НАБЛЮДАТЕЛИ

**Сашо С. Евлогиев
Ивелин Г. Кацев**

*sevl@abv.bg
katsev.i@abv.bg*

OVERVIEW OF MODERN OPTICAL DEVICES FOR RECOGNITION USED BY ARTILLERY FORWARD OBSERVERS

**Sasho S. Evlogiev
Ivelin G. Katsev**

Abstract: *The armed forces of every nation rely on intelligence formations to obtain information about the enemy. A review of some of the state-of-the-art intelligence tools in the world gives us an insight into the development of technology and innovation in optical intelligence.*

Keywords: *Laser rangefinder, reconnaissance, surveillance, forward observer, intelligence formations, recognition.*

В основата на бойните действия е процеса на придобиване на разузнавателна информация за противника. Осигуряването с достоверна, навременна и непрекъснатата информация за действията на противника допринася за постигане на надмощие в операцията. Опитът от локалните конфликти, динамичността на съвременните бойни действия и различните видове учения са показали, че при провеждането на военни операции количеството на целите нараства чувствително, повишава се и дълбочината на разполагането и маневреността им, което води до увеличение на обемът на решаваните от разузнаването задачи, съкращава се рязко времето за организиране на разузнаване, за събиране и обработване на разузнавателна информация. Това изисква модернизирани технически средства, повишаване на уменията от личния състав на всички нива и подобряване на организацията на артилерийските формирования.

В артилерийските формирования разузнаването основно се води от предни наблюдатели (Forward observers). Основните задачи на артилерийските предни наблюдатели могат да бъдат: разузнаване и наблюдение на местността, разузнаване и слеждане на целите, възпиране на цели и обслужване на стрелбата на артилерията и авиацията.

Оптическото разузнаване като основен вид артилерийско разузнаване предоставя бързо и точно засичане на целите, бързо развързване в боен ред и готовност за изпълнение на задачи, осигуряват непрекъснато придобиване на разузнавателна

информация и осигурява достоверност при оценяване на резултатите от поразяването на артилерията. Точността зависи от техническите грешки в приборите, релефа на местността, разстоянието на засичане и други.

За да постигнат поставените им задачи артилерийските предни наблюдатели използват оптически прибори за разузнаване, GPS устройства за привързване и радиостанции за комуникация, както и топографни карти и други прибори.

Лазерните далекомири (Laser rangefinder) са в основата на придобиване на разузнавателна информация и се използват широко от разузнавателните формирования [3]. Най-модерните лазерни далекомири, предназначени за използване от артилерийските предни наблюдатели, са производство на две големи компании Northrop Grumman и Safran Vectronix AG. И двете компании са едни от лидерите на международния пазар по отношение на производството на лазерни прибори за военни цели.

Компанията Northrop Grumman е основана през 1994 г. от Джак Нортроп, работва и произвежда иновации в следните области – кибер среда, логистика, автоматизирани системи, C4ISR системи, ударни и разузнавателни системи и технологии [6],[8].

Lightweight Laser Designator Rangefinder - AN/PED-1, е модулна лазерен далекоммер състоящ се от два основни елемента – модул за локация на целта и модул за лазерно обозначение. Първоначално предназначен за употреба от тринога, в следствие на подобрения е подходящ и за монтиране на разузнавателни машини. Основно се използват от предните наблюдатели за разузнаване на и обслужване на стрелбата на артилерията, както и от предните авио насочвачи. Неговите възможности се свеждат до[4]:

- Работа по всяко време на денонощието и при всякакви условия;
- Възможност за прецизно разузнаване на цел;
- Подходящ е за разузнаване на стационарни или подвижни цели;
- Дигитална съвместимост.

Основни техническите характеристики :

- Тегло – 16кг;
- Температурен диапазон на работа от -37 до +49;
- GPS приемник с точност <16м;
- Разстояния на измерване от 100м до 20 км;
- Точност на измерване на вертикален ъгъл – 13 милса = 0.8° ;
- Точност на измерване на вертикален ъгъл – 8 милса = 0.4° ;
- Точност на измерване на разстоянията – 5 метра;
- Наличие на термална система за разузнаване през ноща.

Lightweight Laser Designator Rangefinder with High Accuracy LLDR-2H – модулния лазерен далекоммер предоставя висока точност при големи разстояния на измерванията, далекоммер може да



Фиг. 1. Lightweight Laser Designator Rangefinder

оформя зона за отговорност като разширява зоната за непосредствено съприкосновение. Чрез уникалната си интеграция на водещи технологии, далекомера осигурява сензори с висока разделителна способност за изпълнение на задачи по разузнаване, определяне координатите на целта и обслужване на стрелбата на артилериата. Неговите възможности се свеждат до[5]:

- Насочване с висока точност;
- Тактически поглед върху картната подложка;
- Скица на терена;
- Индикатор за точност на местоположението на целта, който се показва в окуляра и в мрежата;
- Работа по всяко време на денонощието и при всякакви условия;
- Подходящ е за разузнаване на стационарни или подвижни цели;
- Атермална помпено диодна технология.

Основни техническите характеристики :

- Тегло – 15кг;
- Температурен диапазон на работа от -37 до +49;
- GPS приемник с точност <16м;
- Разстояния на измерване от 100м до 20 км;
- Точност на измерване на хоризонтален ъгъл – 10 метра;
- Точност на измерване на вертикален ъгъл – 3 милса = 0.2°;
- Точност на измерване на разстоянията – 5 метра;
- Наличие на термална система за разузнаване през ноща.

Mark VII Handheld Eyesafe Laser Target Locator – портативния лазерен локатор е предназначен за използване от артилерийските предни наблюдатели, предните авио насочвачи и групите за дълбоко разузнаване. Далекомера може да се свързва с GPS устройства (модули), като Precision Light Weight GPS Receiver (PLGR) и да изчислява с висока точност координатите си. Възможностите на Mark VII са[2]:

- Наблюдение и разузнаване на местността;
- Разузнаване на цели;
- Измерване на азимут, ъгъл на възвишение и разстояние до цел;
- Два режима на работа – ден/нощ.
- Технически характеристики:
- Тегло – 2кг;
- Температурен диапазон на работа от -20 до +50;



Фиг. 2. Lightweight Laser Designator Rangefinder with High Accuracy LLDR-2H



Фиг. 3. Mark VII Handheld Eyesafe Laser Target Locator

- Разстояния на измерване от 20м до 20 км;
- Увеличение – 7.3X18;
- Електронен компас с точност – 9 милса = 0.6°;
- Точност на измервания вертикален ъгъл – 3 метра;
- Точност на измерване на разстоянията – 3 метра.
- Наличие на термална система за разузнаване през ноща.

Safran Vectronix AG е световен лидер в продажбите на най-модерните оптически системи, оборудване и сензори за военни и цивилни нужди. Компанията разработва основно оптически системи за наблюдение, портативни оптически прибори за разузнаване и наблюдение и оборудване, което се монтира върху екипировката, на машини и други.

STERNA (Non-Magnetic, Precision Target Location System (PTLS)) е система за разузнаване и наблюдение, предназначена за използване от артилерийските предни наблюдатели и предните авио насочвачи. Има три модула – STERNA-M, STERNA-V и STERNA-J, които се използват в зависимост от мисията на разузнавателните формирования. Модулите имат сходни характеристики. Възможности на STERNA [7]:

- Олекотена конструкция на системите;
- Висока точност на привързването;
- Работа по всяко време на денонощието и при всякакви условия;
- Изпълнява мисии с над 72 часа продължителност;
- Термален мултифункционален визьор.

Технически характеристики:

- Тегло – 4-6 кг;
- Разстояния на измерване от 5м до 10 км, при STERNA-V23 до 25км;
- Точност на измерване на хоризонтален ъгъл – 1 милс = 0.07°;
- Точност на измерване на вертикален ъгъл – 3 милса = 0.2°;
- Точност на измерване на разстоянията – 5 метра;
- Наличие на термална система за разузнаване през ноща;
- Време за ориентация на системата – 120сек.

MOSKITO – Compact day and night observation and location unit е портативен лазерен локатор предназначен за измерване на разстояние, хоризонтален и вертикален ъгъл с включен визьор за работа през ноща. Възможности[1]:

- Наблюдение и разузнаване на местността;
- Разузнаване на цели;



Фиг.4 STERNA (Non-Magnetic, Precision Target Location System (PTLS))



Фиг. 5. MOSKITO – Compact day and night observation and location unit

- Измерване на хоризонтален ъгъл, вертикален ъгъл и разстояние до цел;
- Възможност за работа през нощта.

Технически характеристики:

- Тегло – 2 кг;
- Разстояния на измерване от 5м до 10 км;
- Увеличение – 5х през деня, 3х през ноща;
- Точност на измерване на вертикален ъгъл – 3 милса = 0.2°;
- Точност на измерване на разстоянията – 5м.

PLRF25C - Pocket Laser Range Finder е най-компактния модел на Vectronix, т.н. “pocket edition”. Въпреки малките си размери, PLRF25C предоставя висока точност на измерванията на малки разстояния. Възможности[1]:

- Наблюдение и разузнаване на местността;
- Разузнаване на цели;
- Измерване на хоризонтален ъгъл, вертикален ъгъл и разстояние до цел;
- Възможност за работа през нощта.

Технически характеристики:

- Тегло – 590гр;
- Разстояния на измерване от 50м до 4км;
- Увеличение – 6х;
- Точност на измерване на хоризонтален ъгъл – 10 милса = 0.6°;
- Точност на измерване на вертикален ъгъл – 3 милса = 0.2°;

➤ Точност на измерване на разстоянията – 2 м при измервания от 50 м до 1500 м и 5 м при измерване на разстояния под 50 м и над 1500 м.

В динамичността на съвременната обстановка и новите схващания за водене на въоръжени и невъоръжени операции, провеждането на учения и опита от съвременните локални конфликти налага използването на съвременна техника за разузнаване. Добиването на разузнавателна информация трябва да има изпреварващо действие в реално време с висока точност, достоверност, непрекъснатост и скритост. Както се вижда от техническите характеристики, съвременните приборите за разузнаване предоставят огромни възможности за разузнаване и наблюдение, с висока точност, бърза подготовка за работа, висока надеждност и възможност за ефективна работа през ноща и други условия на ограничена видимост, също така много важна е и имплементацията на GPS модули в разузнавателните прибори, които осигуряват бързо и точно определяне на координатите на точки от местността. Приборите дават възможност на разузнавателните формирования в пълен обем и при всякакви условия да изпълняват поставените им задачи. Използването на съвременни разузнавателни прибори и качествена подготовка на разузнавателните формирования е добра основа за повишаване на качеството на осигуряването с разузнавателна информация в операциите.



Фиг. 6. Pocket Laser Range Finder

Литература:

1. Handheld equipment, Safran Vectronix AG, 28.07.2017г.
<http://www.safran-vectronix.com/mission/handheld-equipment/>
2. Handheld Eyesafe Laser Target Locator, Northrop Grumman, 27.07.2017г.
<http://www.northropgrumman.com/Capabilities/MarkVII/Pages/default.aspx>
3. Laser rangefinder, Wikipedia site, 26.07.2017г.
https://en.wikipedia.org/wiki/Laser_rangefinder
4. Lightweight Laser Designator Rangefinder (LLDR), Northrop Grumman, 27.07.2017г.
<http://www.northropgrumman.com/Capabilities/ANPED1LLDR/Pages/default.aspx>
5. Lightweight Laser Designator Rangefinder 2H (LLDR 2H), Northrop Grumman, 27.07.2017г.
<http://www.northropgrumman.com/Capabilities/LLDR2H/Pages/default.aspx>
6. List of reconnaissance units, Wikipedia site, 26.07.2017г.
https://en.wikipedia.org/wiki/List_of_reconnaissance_units
7. Northrop to Provide Lightweight Laser Rangefinders, Army technology site, 26.07.2017г.
<http://www.army-technology.com/news/news66231.html>
8. Observation Systems, Safran Vectronix AG, 28.07.2017г.
<http://www.safran-vectronix.com/mission/observation-systems/>
9. Vectronix - Electro-Optics, Rangefinders, Image Intensifiers and Orientation Equipment, Army technology site, 26.07.2017г.
<http://www.army-technology.com/contractors/surveillance/vectronix1/>

A METHOD FOR SOLVING THE TASK FOR MODERNIZATION OR PURCHASING OF LIGHTLY ARMORED COMBAT VEHICLES

Krasimir S. Davidov*, Tsonio G. Tsonev**

* University of Shumen "Bishop Konstantin Preslavski" Technical Sciences Faculty; Department Logistics; kras_i_dav@abv.bg

** National Military University "Vasil Levski", Artillery, AAD and CIS Faculty, con19@abv.bg

Abstract: The report scrutinizes possibilities for the using the systematic approach for solving the problems connected with the modernization of weapon complex of lightly armored combat vehicles.

Key words: logistics; modernization; combat vehicle.

The change of the nature of hostilities, associated with the reduction in operating density of troops and the transition from the area of destruction of objects to the method of selective destruction allows to be made conclusion that the main role in armed conflicts in the XXI century will belong to the highly precise weapon by using conventional means for destruction.

This requires a constant searching of new opportunities to create or purchase of armament complexes which provide greater efficiency of both the individual models of weapons and the weapon complexes. It is required a detailed analysis of the conditions of their operation and optimization of the composition and characteristics of all subsystems based on objectively chosen, physically measurable criterion which does not conflict to the factor „efficiency – value”.

Performing a detailed analysis of the weapons complex that are needed for completing the battle machine is only possible by using the systematic approach.

To solve these tasks it is required to be reported the features of the functioning of the complexes of weapons in a conflict environment, the internal and the external links. The justification of the structure of the weapons complex based on new technical solutions becomes especially important when this problem must be solved.

To understand regularity "system integrity", should primarily take into account its two sides:

- system properties (all) Q_s is not a simple sum of the properties of its components (parts) Q_i : $Q_s \neq \sum Q_i$;
- the properties of the system (all) depends on the properties of its components (parts): $Q_s = f(q_i)$.

Besides these two sides of the regularity "integrity" must be in mind that, as a rule, combined elements in the system lose some of its properties which they have if they are outside the system, or system seems to suppress some of the properties of the elements. But on the other hand, items within the system can acquire new properties.

Rational combination of the parameters of the complex also is very important. It provides joint fulfillment of three conditions: the sufficiency of the striking effect of munitions simplicity in the using of the complex and high efficiency.

In this sense, when it must be the modernized the weapons complex of lightly armoured combat vehicles an important task to solve is the choice of weapons, imposing major demands on it, the definition of rational form, the composition and the characteristics.

It should be noted that when modernization of weapons complexes of combat vehicles is made, due to the desire to be ensured high tactical and technical characteristics, normally obtained exceeded the limits on the sizes and the weight. This, in turn, may require revision and completion activities on the base machine. It must be emphasized that the modernization of weapons of lightly armoured combat vehicles reflects on the characteristics of the chassis.

The performing of an evaluation not only of indicators of combat effectiveness, but also of the main characteristics of the chassis will allow to be obtained a comprehensive assessment of the combat vehicle, i.e., it will be conducted an analysis of how increasing of the combat effectiveness will affect the characteristics of the chassis (it the selfsame together define the coverage of tactical and technical requirements of the machine as a whole).

By applying a systematic approach for solving the problem, the properties of the combat vehicle could be submitted in the form of a structural diagram. On the top level of the structure are four basic properties: firepower, safety, mobility and total operational and technical capabilities. In each of the above mentioned properties exist internal ones, which can also have their own structure. Depending on the objectives pursued, the decomposition of the structure of the properties can be on several levels (usually up to 6÷7). An exemplary structure of the properties of an armoured combat vehicle is shown on figure 1.

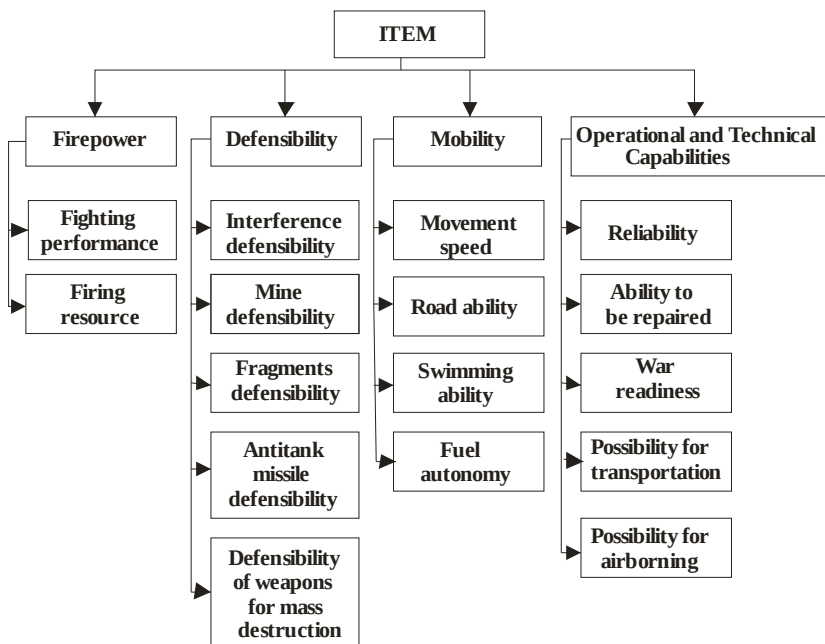


Fig. 1. Structure of the properties of the specimen.

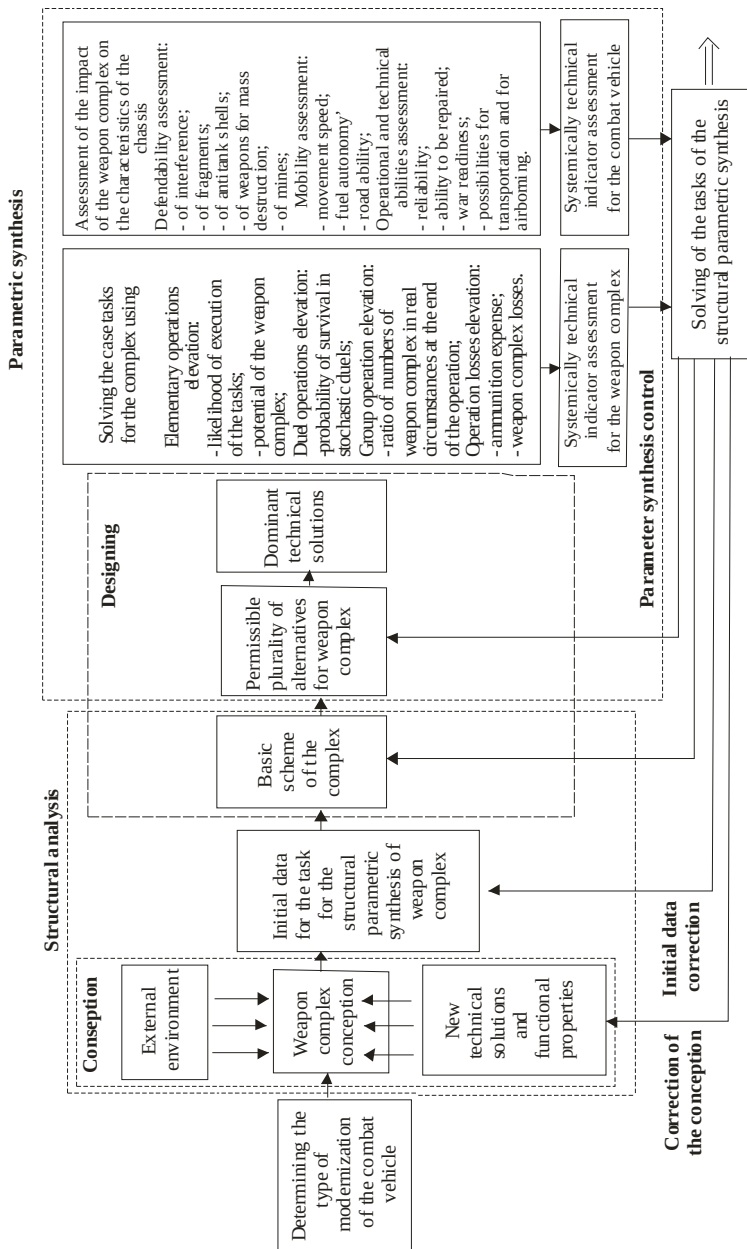


Fig. 2. Scheme of solving tasks of structural parameter optimization of modernization of complexes weapons for light armoured fighting vehicles.

To be performed a comprehensive assessment of the properties of the combat vehicle is necessary to be developed engineering methodology to justify the modernization of the machine and in particular the complex weapons. The methodology, based on the analysis of indicators of combat effectiveness, allows to be estimated the impact of the structural parameters of the modernized weapons complex on the main characteristics of the chassis. An exemplary structural diagram of such a methodology is shown in fig.2.

In the process of weapons creating it must be determined the rational combination of these two properties, occurring in all stages of the design of its subsystems and the model as a whole.

The reporting of the properties is not only principle approach to increasing the adequacy of the models of optimal design, but also a significant reserve for increasing the effectiveness of the weapons.

The need to be increased the combat and operational characteristics of weapons complex of combat vehicles when must be limited the dimensions, mass and value the indicators requires not only the optimization of its parameters, but also on its structure. This is related to the definition of a set of schemes and design parameters of the complex weapons, in other words it must be solved tasks connected with structural parameter optimization based on physically measurable criterion.

Solving such a task can be connected with familiar task for searching for the parameters of additional types of devices in the presence of line of fixed ones. This is a prerequisite for the presentation of the formulation of the task for structural and parametric synthesis.

In order to be shown the solving of the problem for structural-parametric justification is necessary to be created the assembly of elements of complex weapon M_{KB} and its conditions of operation by multitude:

$$M_{KB} = \{M_B, M_{0R}, M_{SUO}, M_{TS}, M_U\}_{0RT} \quad (1.1)$$

where: $M_B, M_{0R}, M_{SUO}, M_{TS}, M_U$ - respectively are subsets of ammunition, weapons systems, systems for fire control, targets and conditions of use.

In fact the logic of the performance of the operations for structural and parametric rationale is reduced to solving the problems for compliance of the elements of the complex armed with their groupings, which provides a maximum of the received criterion for effectiveness K in the form:

$$\begin{aligned} m_B &\in M_B, \\ m_{0R} &\in M_{0R}, \\ m_{SUO} &\in M_{SUO}, \\ m_{TS} &\in M_{TS}, \\ m_U &\in M_U \cup (m_B; m_{0R}; m_{SUO}; m_{TS}; m_U)_{\max} = \max K \end{aligned} \quad (1.2)$$

where: $m_B, m_{0R}, m_{SUO}, m_{TS}, m_U$ - are elements, respectively, of subsets $M_B, M_{0R}, M_{SUO}, M_{TS}, M_U$;

K - optimal solution for each M_{KB} .

The analysis of construction schemes of the considered complex weapon formed a subset of alternative technical solutions A^* which are capable to perform the set task,

$$A^* = \{m_B^*; m_{0R}^*; m_{SUO}^*\} \Rightarrow \left(\bar{K}_{DOP} - K_Z \right), \quad (1.3)$$

where: M_B^* ; m_{0R}^* ; m_{SUO}^* - are elements forming alternative technical solutions A^* , which provide a set level of criteria for efficacy K_Z ;

$\bar{K}_{DOP}$ - tolerance of the optimal solution or extreme of the objective function.

For reliable solving the task of selecting the features and design of modern complex weapon is necessary to have a consistent output data which include the conditions of combat use, a list of typical targets and laws for their destruction, the characteristics of armaments and their component parts (ammunition, weapons, units and systems for fire control). Let's say it in another way - to define the mutual relations of the main features of the complex weapon with criterion function with respect to the mass-dimensions restrictions.

Such characterizations, firstly, can be: ability to detect objects, precision, energy characterizations, related with the parameters of weapons complex and determining the power of the striking impact. This allows to be done systematically technical description of the complex weapon in mathematical form, i.e., to be displayed morphological, information and functional properties. Based on the general principles for the creation of information models, used in the theory of armaments, where any object, process or phenomenon is described by a set of characteristics forming R-dimensional space of properties, which depends on the probability distribution of written above characteristics can be done systematically technical description of the complex weapon.

The modeling in certain degree allows to be given an objective assessment of the technical level of the complex of weapons of armoured vehicles and simultaneously to reveal the process of their military functioning in the course of solving situation task.

Exactly this approach, typical for the implementation of systematically technical researches consists in the separation of the multitude features of the weapons complex of group of bases parameters and can be applied also to its component parts: arms, ammunition, system fire control, as each of them in turn can be divided into elements.

For disclosing the interrelationships between the components of the complex must be built its generalized scheme.

The results of the shaping the motion of the battle include: current numbers and losses of the opposing sides, expense of the ammunition, expense of the implementation of combat tasks and evaluation of the coefficient of technical level of the analyzed technique object toward to the regular model.

Thus, the starting point for systematically describing of the weapons complex is the establishment of the relationship between effectiveness indicators and conditions of its operation. After the finishing an evaluation of the effectiveness of the weapons complex and the cost of its development (including costs for reworking the chassis if it was necessary) it must analyzed the activities performed over the parameters of safety, mobility and exploitation - technical capabilities of the machine as a whole.

According to the results of the evaluations by the chief developer and agreed with the applicant it must be decided whether the solution for modernization is acceptable.

References:

1. Буренок В. М., Ляпунов В. М, Мудров В. И., “Теория вооружения”, 46 ЦНИИ, МО РФ, Москва, 2002.
2. Шипунов А. Г., Игнатов А. В., “Структурно-параметрический синтез пушечно-ракетных комплексов вооружения”, ГУП "КБП", Тула, 2000.
3. Давидов К., Панайотова Т., Дянков П., “Системният подход при проектирането на логистични системи”, Университетско издателство “Епископ Константин Преславски”, Шумен, 2017.

USE OF HEURISTIC ALGORITHMS IN LOGISTICS

Andrey I. Bogdanov

KONSTANTIN PRES LAVSKI UNIVERSITY OF SHUMEN,
SHUMEN 9712, 115 UNIVERSITETSKA STR.

anbog@abv.bg

Abstract: *The paper deals with algorithms for solving logistics problems. It describes types of heuristic algorithms focusing on their strengths and weaknesses. Incorporating the advantages and disadvantages of heuristic algorithms, it offers feasible solutions*

Keywords: *logistics, heuristic algorithms, traveling salesman problem.*

I. Introduction

Many logistic problems are combinatorial by nature. Combinatorial optimization problems could be solved by exact or by heuristic algorithms. The exact algorithms always find the optimal solutions. The wide usage of the exact algorithms is limited by the computer time needed to discover the optimal solutions. In some cases, this computer time is enormously large [1].

Heuristic algorithm could be described as a combination of science, invention, and problem solving skills. In essence, a heuristic algorithm represents procedure invented and used by the analysts in order to “travel” through the space of feasible solutions. Good heuristics algorithm should generate quality solutions in an acceptable computer time. Complex logistic problems of big dimensions are usually solved with the help of various heuristic algorithms [2]. Good heuristic algorithms are capable of discovering optimal solutions for some problem instances, but heuristic algorithms do not guarantee optimal solution discovery.

II. Exposition

An example of approximation is described by Jon Bentley [3] for solving the traveling salesman problem (TSP) so as to select the order to draw using a pen plotter. TSP is known to be NP-Complete (Nondeterministic Polynomial time) so an optimal solution for even a moderate size problem is intractable. Instead, the greedy algorithm can be used to give a good but not optimal solution (it is an approximation to the optimal answer) in a reasonably short amount of time.

The problem can be defined as follows: Find the shortest itinerary, which starts in a specific node, goes through all other nodes exactly once, and finishes in the starting node. In different traffic, transportation, and logistic problems, the traveling salesman can represent airplanes, boats, trucks, buses, crews, etc. Vehicles visiting nodes can deliver or pick up goods, or simultaneously perform pick-up and delivery.

“Greedy” heuristic algorithms build the solution of the studied problem in a step-by-step procedure [4]. In every step of the procedure the value is assigned to one of the variables in order to maximally improve the objective function value. In every step, the

greedy algorithm is looking for the best current solution with no look upon future cost or consequences. Greedy algorithms use local information available in every step. The fundamental concept of greedy algorithms is similar to the “Hill-climbing” technique.

In case of “Hill-climbing” technique the current solution is continuously replaced by the new solution until it is not possible to produce further improvements in the objective function value. “Greedy” algorithms and the “Hill-climbing” technique are similar to the hiker who is trying to come to the mountaintop by never going downwards (Fig. 1).

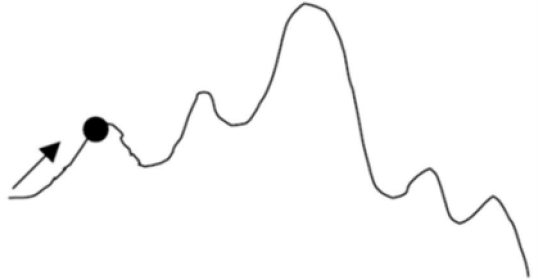


Fig. 1. Hiker who is trying to come to the mountaintop by going up exclusively

As it can be seen from Figure 1, hiker’s wish to never move down while climbing, can trap him or her at some of the local peaks (local maximums), and prevent him or her from reaching the mountaintop (global maximum). “Greedy” algorithms and the “Hill-climbing” technique consider only local improvements.

The Nearest Neighbor (NN) heuristic algorithm is a typical representative of “Greedy” algorithms. This algorithm, which is used to generate the traveling salesman tour, is composed of the following algorithmic steps:

Step 1: Arbitrarily (or randomly) choose a starting node in the traveling salesman tour.

Step 2: Find the nearest neighbor of the last node that was included in the tour. Include this nearest neighbor in the tour.

Step 3: Repeat Step 2 until all nodes are not included in the traveling salesman tour. Connect the first and the last node of the tour.

The NN algorithm finds better solutions than the algorithm based on random choice, as it uses the information related to the distances between nodes.

Let us find the traveling salesman tour starting and finishing in node 1, using NN heuristic algorithm (Figure 2). The distances between all pairs of nodes are given in the Table 1.

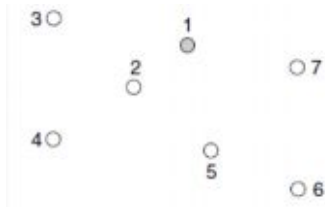


Fig. 2. Network in which a traveling salesman tour should be created using NN heuristic algorithm

	1	2	3	4	5	6	7
1	0	75	135	165	135	180	90
2	75	0	90	105	135	210	150
3	135	90	0	150	210	300	210
4	165	105	150	0	135	210	210
5	135	135	210	135	0	90	105
6	180	210	300	210	90	0	120
7	90	130	210	210	105	120	0

Table 1. The Distances between All Pairs of Nodes created using NN heuristic algorithm

The route must start in node 1. The node 2 is the NN of node 1. We include this NN in the tour. The current tour reads: (1, 2). Node 3 is the NN of node 2. We include this NN in the tour. The updated tour reads: (1, 2, 3). Continuing in this way, we obtain the final tour that reads: (1, 2, 3, 4, 5, 6, 7, 1). The final tour is shown in Figure 3.

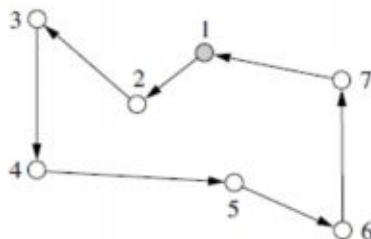


Figure 3. Traveling salesman tour obtained by the NN heuristic algorithm

When applying “greedy” approach, the analyst is forced, after a certain number of steps, to start to connect the nodes (in case of TSP) quite away from each other. Connecting the nodes distant from each other is forced by previous connections that significantly decrease the number of possible connections left.

Exchange heuristic algorithms are based on the idea of interchange and they are widely used. The idea of interchange is the idea to start with the existing solution and check if this solution could be improved.

Exchange heuristic algorithm first creates or selects an initial feasible solution in some arbitrary way (randomly or using any other heuristic algorithm), and then tries to improve the current solution by specific exchanges within the solution.

The good illustration of this concept is two-optimal tour (2-OPT) heuristic algorithms for the TSP [3-OPT and k-optimal tour (k-OPT) algorithms are based on the same idea]. Within the first step of the 2-OPT algorithm, an initial tour is created in some arbitrary way (randomly or using any other heuristic algorithm). The two links are then broken (Fig. 4).

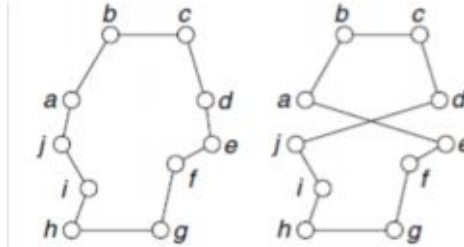


Fig. 4. Interchange of two links during 2-OPT algorithm

The paths that are left are joined so as to form a new tour. The length of the new tour is compared with the length of the old tour. If the new tour length is less than the old tour length, the new tour is retained. In a systematic way, two links are broken at a time, paths are joined, and comparison is made. Eventually, a tour is found whose total length cannot be decreased by the interchange of any two links. Such a tour is known as two-optimal tour (2-OPT).

By using the 2-OPT algorithm, we will try to create the traveling salesman tour for the network shown in Figure 2. The distances between nodes are given in Table 1. The traveling salesman should start his trip from node 1. The initial tour shown in Figure 3 is generated by the NN algorithm. It was not possible to decrease the total length of the initial tour by interchanging of any two links. Our initial tour is 2-OPT

In some cases it is desirable to decompose the problem considered into smaller problems (sub problems). In the following step every sub problem is solved separately. Final solution of the original problem is then obtained by “assembling” the sub problem solutions. We illustrate this solution approach in case of the standard vehicle routing problem (VRP).

The Sweep algorithm is one of the classical heuristic algorithms for the VRP [5]. This algorithm is applied to polar coordinates, and the depot is considered to be the origin of the coordinate system. Then the depot is joined with an arbitrarily chosen point that is called the seed point. All other points are joined to the depot and then aligned by increasing angles that are formed by the segments that connect the points to the depot and the segment that connects the depot to the seed point. The route starts with the seed point, and then the points aligned by increasing angles are included, respecting given constraints. When a point cannot be included in the route as this would violate a certain constraint, this point becomes the seed point of a new route, and so on. The process is completed when all points are included in the routes (Fig. 5).

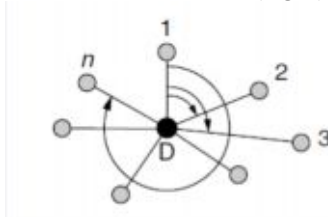


Fig. 5. Sweep algorithm

In case when a large number of nodes need to be served, the Sweep algorithm should be used within the “clustering-routing” approach. In this case, considering clockwise direction, the ratio of cumulative demand and vehicle capacity should be checked (including all other constraints).

The rotating calipers technique for designing geometric algorithms may also be interpreted as a form of plane sweep, in the projective dual of the input plane. A form of projective duality transforms the slope of a line in one plane into the x-coordinate of a point in the dual plane, so the progression through lines in sorted order by their slope as performed by a rotating calipers algorithm is dual to the progression through points sorted by their x-coordinates in a plane sweep algorithm.

III. Conclusion

The objective of a heuristic is to produce a solution in a reasonable time frame that is good enough for solving the problem at hand. This solution may not be the best of all the actual solutions to this problem, or it may simply approximate the exact solution. But it is still valuable because finding it does not require a prohibitively long time.

The final solution depends on a choice of the seed point. By changing locations of the seed point it is possible to generate various sets of vehicle routes. For the final solution the set of routes with minimal total length should be chosen.

IV. References:

1. Apter, Michael J. (1970). The Computer Simulation of Behaviour. London: Hutchinson & Co. p. 2003.
2. Gillett, B. and Miller, L., A Heuristic Algorithm for the Vehicle Dispatch Problem, *Oper. Res.*, 22, 340–352, 2004
3. Hillier, F.S. and Lieberman, G.J., Introduction to Operations Research, McGraw-Hill Science, Columbus, OH, 2002.
4. Bentley J., Writing Efficient Programs. Prentice Hall. 1984 p. 11.
5. Souvaine, D, Line Segment Intersection Using a Sweep Line Algorithm, Tufts University 2008
6. Taha, H., Operations Research: An Introduction (8th Edition), Pearson Prentice Hall, Upper Saddle River, NJ, 2006.

EXPERIMENTAL INVESTIGATION ON THE DEVIATION OF THE MIDPOINT OF THE HITS OF THE SHOTS AND THE GROUPING AT SHOOTING WITH SMALL ARMS WITH FITTED SILENCER

Yana D. Dimitrova*, Tsonio G. Tsonev**

** National Military University "Vasil Levski", "Artillery, AAD and CIS" Faculty dimi-
trovax2yana@gmail.com*

*** National Military University "Vasil Levski", Artillery, "AAD and CIS Faculty",
coni19@abv.bg;*

Abstract: *The report scrutinizes an experimental investigation on the deviation of the midpoint of the hits of the shots and the grouping at shooting with small arms with fitted silencer of the chamber type with rubber chopper wheel.*

Key words: *small arms, silencer, grouping, midpoint of the hits.*

Introduction

The increase in the economical, political and cultural ties between the countries set at the forefront new threats for international peace and security.

Currently terrorism is one of the biggest threats for the security on national and international level. The terrorist organizations decentralize their structures, diversify modes of operation and cleverly infiltrate in the democratic society, which hinders their neutralization.

The increase of the terrorist activities led to the expansion of tasks performed by the Armed Forces of the Republic of Bulgaria.

Part of the new tasks of the military formations are associated with the suppression of terrorist groups and paramilitaries. In a significant part of cases due to the specificity of the anti-terrorist activity the sound of the shots should be hidden. This can be achieved by using special devices called silencers.

On the other hand the growing influx of devices for individual ballistic protection put a tendency improving tactical and technical characteristics of small arms to guarantee the destruction of enemy personnel, equipped with such devices.

Part of the global trends related with the development of armaments are currently focused on creating new samples small arms which have increased combat effectiveness.

Two of the factors that have a significant impact on combat effectiveness are grouping and accuracy in shooting.

Studying of the available literature shows that installation of the silencer on small arms leads to a change of these factors, especially when must be shot at long distances. The reduced combat effectiveness of weapons equipped with silencers can lead to failure to set combat tasks and can increase the amount of losses of personnel.

In the military units of the Republic of Bulgaria main type of small arm is an automatic rifle AK-47, a silencer designed for it is PBS-1, which is on the type of chamber silencer with rubber chopper wheel.

Currently in Bulgaria there have been no systematic studies, related with determining of changing of grouping and the midpoint of the hits of firing of the small arms, fitted with a silencer of the chamber type with rubber chopper wheel when firing is on single or automatic fire.

The report is the first step in exploring the influence of rubber chopper wheel of a silencer of the chamber type on grouping and the changing of the midpoint of hits at single firing with small arms.

2. Experimental investigation

2.1. Purpose: to be investigated experimentally the change of the grouping and the midpoint of hits (MPH) of the small arm fitted with a silencer of the chamber type with rubber chopper wheel at a single shooting.

2.2. Tasks:

- to establish a mathematical law that describe the changing of the grouping of 7,62 mm automatic rifle "Kalashnikov" fitted with a silencer PBS-1, using 7,62x39 mm cartridges "US";
- to establish a mathematical law that describe the changing of the midpoint of the hits of 7,62 mm automatic rifle "Kalashnikov" fitted with silencer with 7,62x39 mm cartridges "US";

The experimental investigation was conducted on the educational shooting ground "Divdyadovo".

In the investigation to ensure the immobility of the firing system, the automatic rifle 7,62 mm "Kalashnikov" was fastened on the mount (frame) "Samozhenkov" with additional clamps - according to fig 1. In order to ensure the immobility of the mount, its legs were attached to the soil of the range polygon by using metal spacers and weights - 15 kg on each leg.

The conditions under which the test was conducted are:

- ambient temperature $19^{\circ} \pm 10^{\circ} \text{C}$; relative humidity $65 \pm 5\%$;
- ammunition are the main for the armament model, new, undamaged, from one party and year of manufacture, in order to be reduced the influence of the reasons that caused differences in the initial take-off speed of bullets;
- ammunition tempering was made in a room (room for storing weapons in cadet battery) at a constant temperature for 24 hours before the shooting, as ammunitions are not removed from their standard package;
- the test was performed by firing with one number of 7,62 mm automatic rifle AK-47 "Kalashnikov" and one number of silencer PBS-1;
- distance of the shooting - 100 m (measured from the muzzle of the barrel to shield with the target);
- barrel angle - 0° toward to the horizontal plane;
- barrel cooling was made each 60 shots.



Fig. 1. Automatic rifle AK-47 fixed to the mount "Samozhenkov".

2.3. Procedure for conducting experimental investigation

A. Preparation of weapons and ammunition

Sequence:

- the barrel channel must be cleaned from grease, soot and other contaminants before shooting starts;
- dismantle the standard measurement plate from the automatic rifle and replaced with measurement plate for shooting with silencer PBS-1;
- dismantle the safety lever and install 7,62 mm automatic rifle AK-47 to the mount (frame) "Samozhenkov";
- secure the mount (frame) "Samozhenkov" to the soil of the range polygon by metal spacers and weight - 15 kg for each leg;
- place a shield having attached on it a white cardboard with dimensions of 1 m high and 1 m width, on distance of 100 m away from muzzle of the barrel;
- aim the weapon in the setpoint of the shield, then mechanisms for directing on the mount must be locked;
- performe a warm-up shot.

B. Performance of experimental shooting

Experimental shooting is performed in the following sequence:

a) *Determine the grouping and midpoint of hits (MPH) of 7,62 mm automatic rifle AK-47 without silencer with 7,62x39 mm cartridges model '43:*

- produce 2 series of 20 shots of a single fire;
- determine grouping and midpoint of hits for each series individually;
- calculate the average of the two series.

b) *Determine the grouping and midpoint of hits of 7,62 mm automatic rifle AK-47 with mounted on the barrel silencer without rubber chopper wheel with 7,62x39 mm cartridges "US".*

Due to the specific structure of the silencer PBS-1, the rubber chopper wheel can not be removed because it serves as a spacer sleeve. To determine the grouping and the midpoint of hits when firing, excluding the influence of the tribological characteristics of the chopper wheel is made of the hole on the chopper wheel with a diameter of 15 mm - fig. 2.

- dismantle the silencer PBS-1, placed fitted (with hole 15 mm) rubber chopper wheel and assemble the silencer;
- attach silencer PBS-1 to 7,62 mm automatic rifle AK-47;
- produce 2 series of 20 shots on single fire;
- determine the grouping and the midpoint of hits for each series individually.

c) *Determine the grouping and the midpoint of hits of 7,62 mm automatic rifle AK-47 fitted with silencer with 7,62x39 mm cartridges "US":*

- separate the silencer and set a new chopper wheel;
- attach silencer PBS-1 to 7,62 mm automatic rifle AK-47;
- produce 10 series of 20 shots on single fire;
- determine the grouping and the midpoint of hits for each series individually.



Fig. 2. The chopper wheel with hole with diameter of 15

d) Determine the grouping and the midpoint of hits of 7,62 mm automatic rifle AK-47 without silencer with 7,62x39 mm cartridges "US":

- separate the silencer from the automatic rifle;
- produce 2 series of 20 shots on single fire;
- determine the grouping and the midpoint of hits for each series individually.

2.4. Logistics

For making the experimental shootings the following logistics support is used:

- cartridge 7,62x39 model 1943 - 40 (forty) numbers;
- cartridge 7,62x39 model "US" - 280 (two hundred and eighty) numbers;
- shield attached to a target with a setpoint with sizes 1 m high and 1 m wide - 20 (twenty) numbers.

3. Experimental investigation results

The results of the experimental investigation of the grouping and the midpoint of hits of 7,62 mm automatic rifle AK-47 fitted with silencer with 7,62x39 mm cartridges "US" are presented in table 1.

Table 1

Results obtained from the experimental investigation of grouping and the middle point of hit of 7,62 mm automatic rifle "Kalashnikov" fitted with silencer with 7,62x39 mm cartridges „US”.

№ of series	Distance between the two outermost hits		Deviation of the middle point of hits from the setpoint	
	In the horizontal plane [cm]	In the vertical plane [cm]	In the horizontal plane [cm]	In the vertical plane [cm]
1	30	21,5	15,2	15,2
2	19,2	17,7	18	30,8
3	16,2	19,9	26,8	14
4	23	14,3	29	7,4
5	19,4	27,7	27,5	6,2
6	22,8	8,5	24,2	5
7	28	19,4	3,3	0,3
8	23,3	29	22,5	8,5
9	17,2	18,8	15	3,5
10	22	22	40,8	27,5

The average data of the firing 7,62 mm automatic rifle AK-47 without silencer with 7,62x39 mm cartridges model 1943 are:

- the deflections on the midpoint of hits from the setpoint are: in the horizontal plane $X = 4$ cm and in the vertical plane $Y = 3$ cm;

- the distances between the two outermost hits are: in the horizontal plane $X = 15$ cm and in the vertical plane $Y = 22$ cm.

The average data of the firing 7,62 mm automatic rifle AK-47 without silencer with 7,62x39 mm cartridges model “US” are:

- the deflections on the midpoint of hits from the setpoint are: in the horizontal plane $X = 8.4$ cm and in the vertical plane $Y = 25.8$ cm;

- the distances between the two outermost hits are: in the horizontal plane $X = 17.6$ cm and in the vertical plane $Y = 18$ cm.

The average data of the firing 7,62 mm automatic rifle AK-47 with a silencer without chopper wheel with 7,62x39 mm cartridges model “US” are:

- the deflections on the midpoint of hits from the setpoint are: in the horizontal plane $X = 20.5$ cm and in the vertical plane $Y = 4$ cm

- the distances between the two outermost hits are: in the horizontal plane $X = 15$ cm and in the vertical plane $Y = 17$ cm.

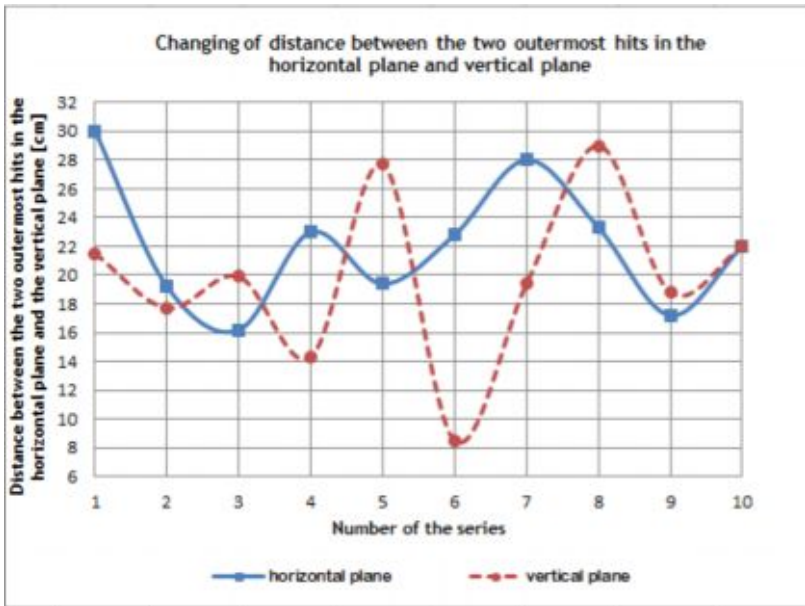


Fig. 3. Graphics of the change of the distance between two outermost hits in the horizontal and vertical plane.

The approximate mathematical law that modifies the values of the deviation of the midpoint of the hits in the horizontal plane is:

$$y = a + b.x + c.x^2 + d.x^3 + e.x^4 + f.x^5 \quad (1)$$

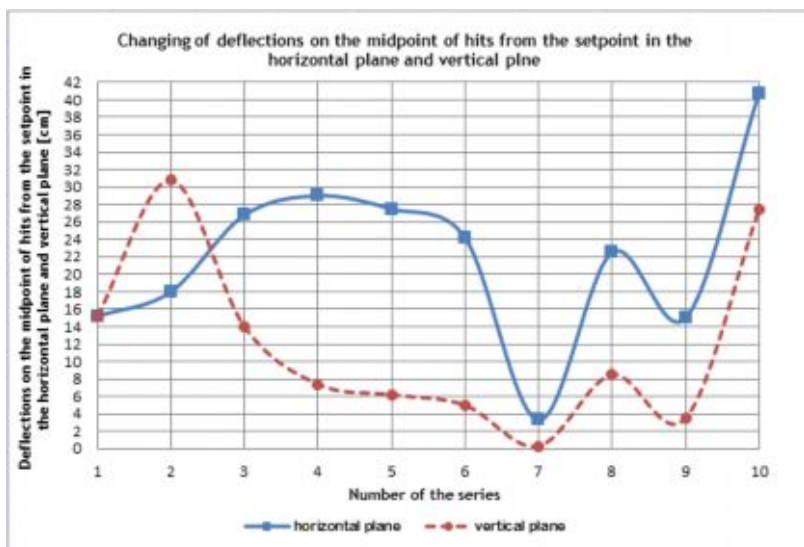


Fig. 4. Graph of change of deviation of the middle point of the hits (MPH) of the setpoint in the horizontal and vertical plane.

The approximate mathematical law that modifies the values of the deviation of the midpoint of the hits in the vertical plane is:

$$y = a + b.x + c.x^2 . \ln x + d.x^{2.5} + e.x^3 \quad (2)$$

The approximate mathematical law, that modifies the values of the grouping in the horizontal plane is:

$$y = a + b.x + c.x^2 + d.x^3 + e.e^x \quad (3)$$

The approximate mathematical that modifies the values of the grouping in the vertical plane is:

$$y = a + b.\sin^2\left(\frac{2\pi.x}{d} + c\right) \quad (4)$$

4. Conclusions:

1. From the data presented in table 1 it can be concluded that the grouping and the deviation of the middle point of the hits from the setpoint of the silencer of the chamber type, with a rubber chopper wheel change with the amount of the made shots, respectively, with the wear of the rubber chopper wheel of silencer.

2. The deviations of the midpoint of the hit from the setpoint in horizontal and vertical plane when it is shoot with small arms with mounted silencer with rubber chopper wheel don't have the same character and amended on complex mathematical law. The same goes for change of the grouping. Therefore the shooter can not make

accurate predictions on the place of the bullet hit, because this place will depend on the wear of the chopper wheel.

3. It is necessary to make a investigation of the variation in the midpoint of the hits and the grouping when it is shoot with small arms with silencer without rubber chopper wheel in order to increase the efficiency of firing a weapon fitted with a silencer.

References:

1. ЦОНЕВ Ц. Г., ДАВИДОВ К. С., Основи за устройството на стрелковото оръжие – част I, ШУМЕН., 2013.
2. ВЕНТЦЕЛЬ Е.С., Теория вероятностей., МОСКВА, 1969.
3. ВЪЛКОВ Н. В., ДАВИДОВ К. С., ЦОНЕВ Ц. Г., ГАНЕВ В. В. Основи и правила за стрелба с огнестрелни оръжия. Материална част на стрелковото оръжие., ВАРНА: СТЕНО, 2008. ISBN 978-954-449-411-7.
4. МОНТГОМЕРИ Д.К., Планирование эксперимента и анализ данных., ЛЕНИНГРАД: СУДОСТРОЕНИЕ, 1980.
5. КИРИЛОВ В. М., Основи за устройството и проектирането на стрелковото оръжие. СОФИЯ: ДВИ, 1975.

С. И. Антонов, И. С. Христозов,

МОДЕЛИ НА СЪЩЕСТВУВАЩАТА СИСТЕМА ЗА ТЕХНИЧЕСКО ОБСЛУЖВАНЕ И РЕМОНТ НА ВЪОРЪЖЕНИЕТО

Стамен И. Антонов*, Иван С. Христозов**

*НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, stamantonov@abv.bg

** Институт за перспективни изследвания за отбраната, ihristoz@yahoo.com

MODELS OF THE EXISTING SYSTEM FOR MAINTENANCE AND REPAIR OF THE ARRANGEMENT

Stamen I. Antonov*, Ivan S. Hristozov**

*National Military University “Vasil Levski”, Artillery, AAD and CIS Faculty, stamantonov@abv.bg

**Defense Advanced Research Institute, ihristoz@yahoo.com

Abstract: The weapons repair process models are considered in the form of a process chart and network schedules. With their use, the "bottlenecks" of the maintenance system, which reduce the effectiveness of performance of the activities and keep the implementation of the overall process, are analyzed. The duration of each activity in the armaments repair process is determined by statistical and probabilistic methods.

Keywords: Map diagram, network model, maintenance and repair system, command and executive logistics at the tactical level

Осигуряването на постоянна техническа готовност на въоръжението е главна задача в системата на експлоатацията му, която се организира основно от логистичните органи, особено на тактическо ниво.

За да се осигури поддръжката на въоръжението следва да се познава методиката, правилата и образците планиращи документи, свързани с режимите на експлоатация на въоръжението.

Членството на Република България в НАТО, както и продължаващата трансформация на въоръжените ни сили изискват внедряването на интегрирани информационни системи за управление на логистичното осигуряване, в това число и за мониторинг, управление и контрол над експлоатационните параметри на въоръжението във тактическите формирования от Българската армия, както и съвместяване на тези информационни системи с на останалите армии от НАТО.

Еднозначното и точно определяне на решения по експлоатацията на въоръжението е сложен процес, свързан със събиране, обработка и анализ на разнородна и голяма по обем информация, относно основните му експлоатационни параметри.

Във военните формирования на тактическо ниво се прилага утвърден модел на система за техническо обслужване и ремонт на въоръжението. Действащата процедура за документоформание и документооборот при текущия ремонт на

въоръжението обаче е доста трудоемка и тромава. Това налага необходимостта да се анализира съществуващата практика и да се предложи нов, ефективен модел за дейностите по документооборота, съпътстващ текущия ремонт на въоръжението.

Модели на съществуващата система за техническо обслужване и ремонт на въоръжението

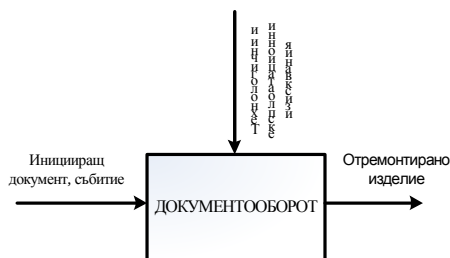
Моделът трябва да отговаря на следните основни въпроси:

- Кои са “входът” и “изходът” на системата?
- От какви дейности се състои процесът в системата?
- Кой изпълнява всяка процедура?
- Какво се получава в резултат на изпълнение на процедурата?
- Кой получава резултата и как той използва този резултат?

Анализ на процеса на документодвижението през отделните изпълнители и подизпълнители при регистриране и оформяне заявките и останалите документи по техническото обслужване и ремонта на въоръжението

Едно от определения за процес гласи [5]: „Процес е съвкупност от взаимосвързани и взаимодействащи си видове дейности“. При анализа като начало е необходимо да се определи процесът като цяло, т.е. да се определят целта и границите му. Процеса по документооборота ще бъде разгледан от гледната точка на извършването на текущи ремонти на въоръжението със собствени сили и средства на тактически формирования с ранг на батальон.

Входовете и изходите на процеса са представени на фиг. 1 като видовете дейности са обозначени като „черна кутия“. Това е контекстната диаграма на процеса.

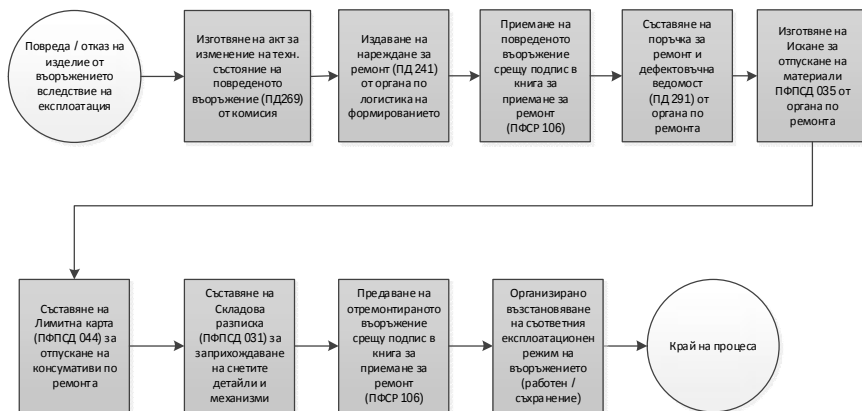


Фиг. 1. Контекстна диаграма на процеса

В черната кутия има действия, които се извършват в определена последователност. Кои са те за разглеждания процес? В таблица 1 е представена матрица на етапите от документооборота при ремонта на въоръжението, която дава последователността от необходимите действия. По-долу се предлага модел на процеса чрез прилагане на един от най-разпространените методи в областта на управлението, а именно диаграма на последователността на дейностите (flow chart).

Съставяне на карта диаграма на последователността на дейностите (flow chart)

Същността на този метод се състои в графичното изобразяване на последователността от действия на разглеждания процес чрез използване на различни символи (елипса, правоъгълник и стрелки). Диаграмата на процеса на съпътстващия документооборот при текущия ремонт на въоръжението от ремонтните органи на тактическото ниво е дадена на фигура 2.



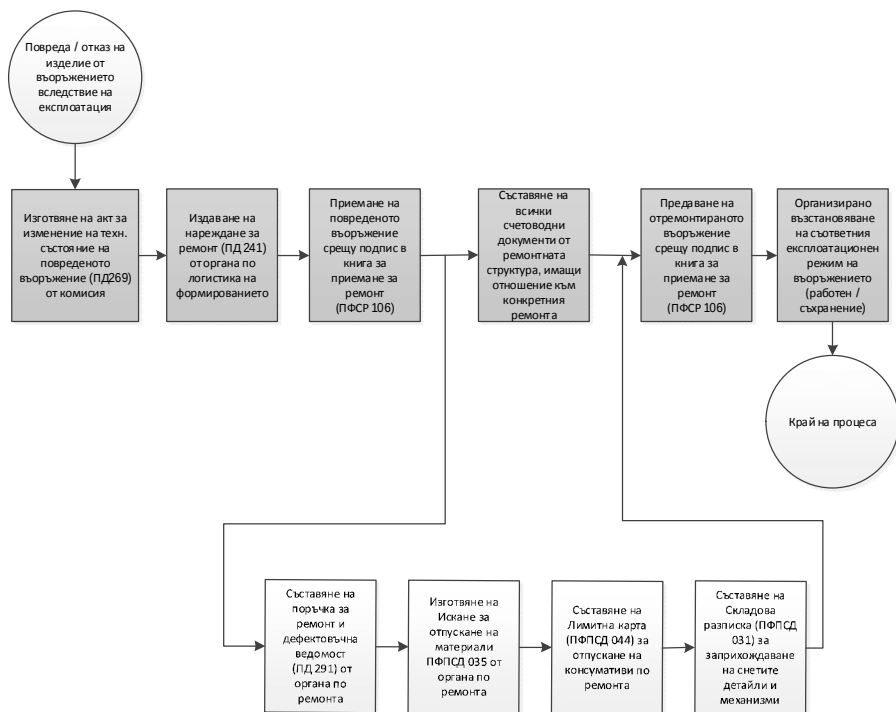
Фиг. 2. Диаграма на последователностите

В диаграмата последователността на действията се разглежда изключително във времето, като стрелка показва кое действие след кое следва (с оглед на това, че в следващите диаграми процесът ще бъде развит детайлно, диаграмата от фиг. 2 е доста опростена).

Анализът на процеса по диаграмата на последователностите показва следното:

- не всички дейности се изпълняват с една и съща скорост;
- за усъвършенстване на технологията и икономия на време някои от видовете дейности могат да се извършват паралелно.

Усъвършенстван процес е даден на диаграмата на последователностите от фиг. 3.



Фиг. 3. Диаграма на последователностите (усъвършенстван вариант)

Независимо че диаграмата от последователности се е променила, описанието на процеса от гледна точка „вход- изход” или „черна кутия” не се е променил. Изводът, който може да се направи е, че когато се говори за оптимизиране на процес е важно как технологично ще се построи този процес, а това засяга организацията и управлението на процеса. За описание на процеса в такъв случай може да се приложи методът “карта на процеса” (process map).

При оптимизиране на процеса също трябва да се отчита и времето за неговото изпълнение. За тази цел са необходими: първо - времето за извършване на всяка дейност от процеса и второ - времето изразходвано за целия процес. В този случай може да се приложи методът на мрежовия график.

Съставяне на карта на процеса (Process Map)

С цел анализиране на организацията и управлението на процеса “документооборот при текущ ремонт на въоръжението” се построява карта на процеса. Методът се използва с цел двумерно изобразяване на дейности, което е най – благоприятно за възприемане от човека. Също така изборът на параметри на процеса (оси на картата) може да бъде насочен за целта на анализа, а именно изобразяване в две координатни оси, например изпълнители и време, местоположение и участници и т.н.

Например първата ос да бъде дейностите в процеса-построяване на алгоритъм от последователността на дейностите в процеса, или това е оста на времето. Втората ос - кои изпълнители какви дейности извършват.

Алгоритъмът трябва да отразява ситуацията „как е“.

В настоящия доклад, картата на процеса е дадена в табличен вид (таблица 1), в която процесът е декомпозиран функционално и са посочени кои длъжностни лица какви функции изпълняват.

Матрица на функциите в дейността “текущ ремонт на въоръжение” – изпълняващ орган – отделение за ремонт на АМЧ и СО

Таблица 1

	Функции (О – организира, У – участва, И – изпълнява; К – контролира)	Командир на военното формирование	Зам.-командир по логистика	Секция „Логистика“ S-4	Командир на логистична рога	Непосредствен ремонтчик	МОЛ на въоръжението
1.	Документооборот при текущ ремонт на въоръжението на МБ						
1.1	Подготвителен етап						
	Регистрация на повредено въоръжение		О,К	У			И
	Инициране на комисия за първоначална дефектация и съставяне на акт за изменение на техническото състояние (ПД 269)	О	К	У		И	
	Издаване на нареждане за ремонт (ПД 241)		О,К	И			
1.1.4.	Вписване в съответното сведение за неизправно въоръжение и техника		О,К	И			
1.2	Етап на извършване на текущия ремонт						
1.2.1.	Проверка окомплектоването на въоръжението преди приемането му за ремонт				О,К	И	У
1.2.2.	Приемане на повреденото въоръжение срещу подпис в книга за приемане за ремонт (ПФСР 106)		О,К		И		У
1.2.3.	Подробна дефектация с проверка в слобен и разглобен вид				О,К	И	

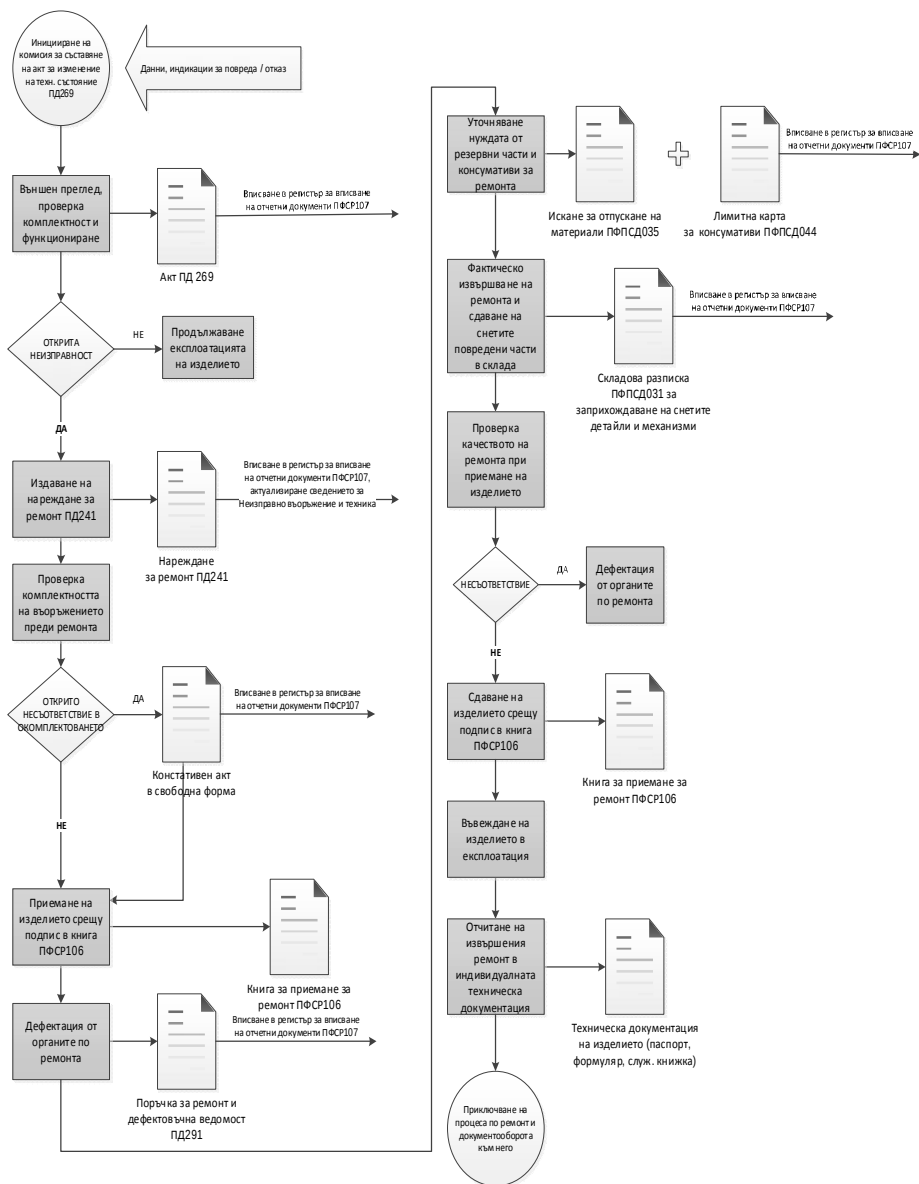
	Функции (О – организира, У – участва, И – изпълнява; К – контролира)	Командир на военното формирование	Зам.-командир по логистика	Секция „Логистика“ S-4	Командир на логистична рота	Непосредствен ремонтчик	МОЛ на въоръжението
1.2.4.	Съставяне на поръчка за ремонт и дефектовъчна ведомост (ПД 291)			О	К	И	
1.2.5.	Изготвяне на Искане за отпускане на материали (ПФПСД 035)		О,К	И	У		
1.2.6.	Получаване на резервни части за влагане при ремонта			О,К	У	И	
1.2.7.	Съставяне на Лимитна карта (ПФПСД 044) за отпускане на консумативи по ремонта		О,К		И	У	
1.2.8	Получаване на консумативи и общоразходни материали за ремонта			О,К	У	И	
1.3	Приключване на текущия ремонт						
1.3.1.	Съставяне на Складова разписка (ПФПСД 031) за заприхождаване на сметите детайли и механизми		О,К	И	У		
1.3.2.	Връщане в склада на сметите негодни детайли, механизми и агрегати				О,К	И	
1.3.3.	Предаване на отремнтираното въоръжение срещу подпис в книга за приемане за ремонт (ПФСР 106)		О,К		И		У
1.3.4.	Проверка действителното извършване на ремонта и окомплектоването, както и работата на механизмите на въоръжението				О,К	У	И
1.3.5.	Организирано възстановяване на съответния експлоатационен режим на въоръжението (работен / съхранение)	О	К				И

	Функции (О – организира, У – участва, И – изпълнява; К – контролира)	Командир на военното формирование	Зам.-командир по логистика	Секция „Логистика“ S-4	Командир на логистична рота	Непосредствен ремонтник	МОЛ на въоръжението
1.3.6.	Отписване от съответното сведение за неизправно въоръжение и техника		О,К	И			
1.3.7.	Нанасяне на данни по извършения ремонт на въоръжението в индивидуалната му техническа документация		О,К				И

На фиг. 4 се посочват алгоритъмът на процеса и изискванията за съответния нормативен документ на всяка дейност.

Картата на процеса помага в работата на различни етапи от технологичната оптимизация [4]:

- на етап изясняване на проблема картата е документ, който показва ситуацията „как е“;
- на етапа търсене на решение картата отразява какъв трябва да бъде изследвания процес; окончателния вариант на картата може да бъде съгласуван с всички заинтересувани страни;
- на етапа измерване на резултата уточненият вариант на картата се използва за проверка (одит) на процеса и оценка на резултатност;
- на етапа стандартизация на процеса окончателният вариант на картата може да бъде използван в качеството си на документирана процедура за обучение на персонала, за осигуряване на процеса откъм ресурси, разпространение на получения опит върху другите процеси, свързани със документалното обработване на логистичната поддръжка.



Фиг. 4. Алгоритъм на процеса „текущ ремонт на възгоржение“

Съставяне на мрежови модел на процеса

Този метод е известен като ПЕРТ метод или Activity Network Diagram. Произлиза от абривиатурата **P**rogram **E**valuation and-**R**eview **T**echnique (PERT)

Мрежовият модел е схема на управлението. В основата му стоят линейни графици. Най-характерните предимства на мрежовия график се състоят в следното:

1. Прилагането на мрежовия метод се изразява в мрежови модел, който отразява взаимната връзка между дейностите и тяхната логическа и технологическа последователност. Поради това не може да се пропуснат някои или пък да се включат други, несвързани с дадената дейност.

2. Точно се определя продължителността на дадената дейност, а оттам и на целия процес.

3. Дава възможност да се определят основните дейности и най-чувствителните места (т.нар. „тесни места“), които могат да задържат изпълнението на целия процес.

4. Спомага за намиране на най-ранния срок за започване на всяка от дейностите на сложна организация.

5. Определя необходимостта от навременно въвеждане на необходимите сили и средства за изпълнение на съответните работи;

6. Предлага ефикасен контрол за изпълнение на съответните работи и техните срокове.

7. Осигурява целесъобразно използване на силите и средствата при наличие на резерв от свободно време за някой от изпълнителите.

Не на последно място предимство на мрежовия метод е неговата универсалност.

С помощта на този метод може да бъдат изследвани всякакви дейности.

Мрежовият метод позволява получаването на научно обосновани отговори на най-важните въпроси, които възникват в работата и координацията на много взаимосвързани процеси.

Елементите на мрежовия график са три: *работа, събитие и път*.

Работа е всеки трудов процес, съпроводен с разход на време и ресурси. Работите в един мрежови график могат да бъдат *действителни*, изискващи разход на време и ресурси, *изчаквания*, изискващи само разход на време и *фиктивни*, неизискващи разход на труд, материални ресурси и време. Продължителността на работата може да бъде измерена количествено в единица време.

Събитие се нарича моментът от време, когато завършва една работа и започва друга. Събитието е резултат от проведените работи и за разлика от тях няма времетраене.

Път е всяка непрекъсната логическа (технологична) последователност от работи от изходното до завършващото събитие. Дължината на пътя се определя от сбора от продължителността на включените в него работи. От изходното до завършващото събитие може да има много пътища, но в резултат на съставяне на мрежовия график и анализирането му се отделя този път, в който сумата от продължителността на работите му е максимален. Този път се нарича *критичен*. Той определя необходимото време за извършване на всички работи, включени в мрежовия график.

Работата обикновено се кодира с номерата на събитията, между които е заключена, т.е. (i,j) , където i е номерът на предшестващото събитие, а j е номер на последващо събитие $i < j$.

Основни свойства на мрежовия модел:

- събитието се случва тогава, когато всички входящи в него работи са завършили;
- изходящите от събитията работи могат да започнат само след тяхното завършване;
- следваща работа може да започне само след завършване на предшестващата.

Построението на мрежовия график започва с определяне на последователността от събитията, които след това се нанасят в таблица със съответния ранг. Рангът на събитието се определя от реда на номериране в общата последователност от събития. След това на графичен модел работите се нанасят в линия, съединяваща изходните и последващите събития.

Ако процесът Pr се състои от работи $Pr_1, Pr_2, \dots, Pr_n$, то за построяване на мрежовия график е необходимо за всяка работа Pr_k ($k=1, 2, \dots, n$) да е известно или да може достатъчно точно да се оцени времето за изпълнението ѝ $t(Pr_k)$. Продължителността на работа реално е дължината на дъгата. Дължината на пътя T е сбор от дължините на всички дъги, образуващи дадения път, т.е. $T = \sum t_{i,j}$, където $t_{i,j} \in T$, се означава дъгата, съединяваща i и j събитие и е насочена от връх i към връх j .

Построен по такъв начин мрежовият график според термините на теорията на графите е насочен граф. Графът не съдържа цикли. Такъв граф е разновидност на ориентирания граф, включващ в позиции и преходи.

Формиране на показателите по времетраене за всяка дейност

В настоящето изследване се разглеждат мрежови графици, съставени по времеви параметър. Трябва да се отбележи, че правилността на поставените времеви параметри има първостепенно значение за качеството на модела и оперативността на ръководството на процеса по дадения график. Определянето на продължителността на работите е трудно. Съществуват няколко способа.

За често повтарящи се работи, за които има нормативи, продължителността се взема от тях. Такива за процеса по текущия ремонт на въоръжението няма.

За работи, по които има достатъчно натрупан опит, оценките могат да се получат вследствие обработването на достатъчен обем статистически данни. Например за продължителността на работите може да се използва значението на средната продължителност

$$(1) \quad t_{i,j} = \frac{1}{n} \sum_{k=1}^n t_{i,j,k} ,$$

където $t_{i,j,k}$ е продължителността на i,j работа в k опит.

За работи, за които няма временни оценки, с помощта на метода на *експертни оценки* от специалисти се определят три оценки минимална, максимална и най-вероятна стойност на продължителностите на работите:

- $t_{min\ i,j}$ – най-благоприятно време или оптимистична оценка;

- $t_{\max ij}$ – най-неблагоприятно време или песимистична оценка;
- $t_{н.в. ij}$ – най-вероятна

Имаме [1, 2]:

$$(2) t_{ij} = \frac{1}{6}(t_{\min ij} + 4t_{н.в. ij} + t_{\max ij})$$

Полученото по формула (2) очаквано време за изпълнение на работите е случайна величина и е необходимо да се знае каква грешка е допусната в оценката, т.е. отклонението от очакваното значение. Погрешността в този случай се оценява по получената дисперсия, изчислена по формулата:

$$(3) \sigma^2 = \frac{(t_{\max ij} - t_{\min ij})^2}{6},$$

където σ е дисперсията;

$t_{\max ij}$ - максималната оценка;

$t_{\min ij}$ – минималната оценка.

Тази формула показва, че колкото е по-широк диапазонът между максималната и минималната оценка, т.е. колкото е по-широк размаха на разпределението, толкова по-голяма е неопределеността, свързана с разглежданата операция и обратно, колкото по-малка е дисперсията толкова са по-точни оценките за продължителността на дейностите и максималната и минималната оценка са близко една до друга.

На практика използването на формула (2) предизвиква затруднения при определянето на $t_{н.в. ij}$.

Използван е следният алгоритъм [6] за определяне на времето t_{ij} на работата (i,j) :

1. Чрез анкета от n експерти са събрани статистически данни за $t_{\max ij}$ и $t_{\min ij}$ за всяка работа
2. Определени са средните минимални $t_{\text{средно } \min ij}$ и максимални $t_{\text{средно } \max ij}$ стойности за всяка работа по формула (1).
3. За време за извършване на работа (i,j) е прието времето t_{ij} , изчислено по формула (4), със средно квадратично отклонение, изчислено по формула (5) [1].

$$(4) t_{ij} = \frac{1}{5}(3t_{\text{средно } \min ij} + 2t_{\text{средно } \max ij})$$

$$(5) \sigma_t^2 = 0,04(t_{\max ij} - t_{\min ij})^2$$

В такъв случай вероятността работата наистина да бъде извършена за време $t_{\text{реално}} = t_{ij}$ е $P(n)=0,5$, където $P(n)$ се определя по формула (6) [3].

$$(6) P(n) = \Phi\left(\frac{t_{\text{реално}} - t_{i,j}}{\sqrt{\sigma^2(i,j)}}\right),$$

където

$P(n)$ е вероятността за извършване на работа (i,j) в разчетния срок;

$t_{реално}$ - реален срок за извършване на работа (i, j);
 $t_{i,j}$ - разчетно време;

$\sigma^2(i, j)$ - дисперсията на времето за извършване на работа (i, j);

$\Phi(n)$ –функцията на нормалното разпределение

$$(7) \quad \Phi(x) = \frac{1}{\sqrt{2\pi}} \int e^{-\frac{t^2}{2}} dt$$

Известна е като функцията на Лаплас за определяне на вероятността за свършване на събитие в директивен срок. При $0,35 < P(n) < 0,65$ се счита, че е дадена оптимална оценка.

При направеното допускане за $t_{реално} = t_{i,j}$, то $P(n)=0,5$.

В таблица 2 е дадена матрица на процедурите със съответното времетраене на всяка работа, включена в последователностите от работи за изследвания процес. За всяка работа са направени описаните по-горе изчисления.

Матрица на дейностите (операциите) “Текущ ремонт на въоръжение” от управленските и изпълнителни логистични органи на тактическо ниво

Таблица 2

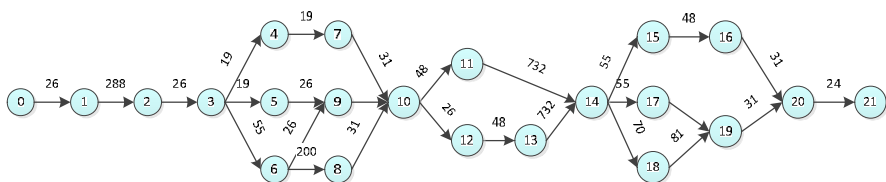
№	Наименование на събитие	Предшестващ процес	Времетраене на процеса		Дисперсия	$t_{i,j}$
			min	max		
1.	Старт на процеса (фиктивна работа)	-	0	0	0	0
2.	Регистрация на повредено въоръжение	1	20	35	3	26
3.	Инициране на комисия за първоначална дефектация и съставяне на акт за изменение на техническото състояние (ПД 269)	2	240	360	24	288
4.	Издаване на нареждане за ремонт (ПД 241)	3	20	35	3	26
5.	Вписване в съответното сведение за неизправно въоръжение и техника	3	15	25	2	19

№	Наименование на събитие	Предшестващ процес	Времетраене на процеса		Дисперсия	ti,j
			min	max		
6.	Проверка окомплектоването на въоръжението преди приемането му за ремонт	3	45	70	6	55
7.	Приемане на повреденото въоръжение срещу подпис в книга за приемане за ремонт (ПФСР 106)	4	15	25	2	19
8.	Подробна дефектация с проверка в сглобен и разглобен вид	6	170	245	15	200
9.	Съставяне на поръчка за ремонт и дефектовъчна ведомост (ПД 291)	5,6	20	35	3	26
10.	Изготвяне на Искане за отпускане на материали (ПФПСД 035)	7,8,9	25	40	3	31
11.	Получаване на резервни части за влагане при ремонта	10	40	60	4	48
12.	Съставяне на Лимитна карта (ПФПСД 044) за отпускане на консумативи по ремонта	10	20	35	3	26
13.	Получаване на консумативи и общоразходни материали за ремонта	12	40	60	4	48
14.	Фактическо извършване на текущия ремонт	11,13	660	840	36	732
15.	Съставяне на Складова разписка (ПФПСД 031) за заприхождаване на сметите детайли и механизми	14	45	70	6	55
16.	Връщане в склада на сметите негодни детайли, механизми и агрегати	15	40	60	4	48
17.	Предаване на отремантираното въоръжение	14	45	70	6	55

№	Наименование на събитие	Предшестващ процес	Времетраене на процеса		Дисперсия	$t_{i,j}$
			min	max		
	срещу подпис в книга за приемане за ремонт (ПФСР 106)					
18.	Проверка действителното извършване на ремонта и окомплектоването, както и работата на механизмите на въоръжението	14	60	85	5	70
19.	Организирано възстановяване на съответния експлоатационен режим на въоръжението (работен / съхранение)	17,18	75	90	3	81
20.	Отписване от съответното сведение за неизправно въоръжение и техника	16,19	25	40	3	31
21.	Нанасяне на данни по извършения ремонт на въоръжението в индивидуалната му техническа документация	20	20	30	2	24

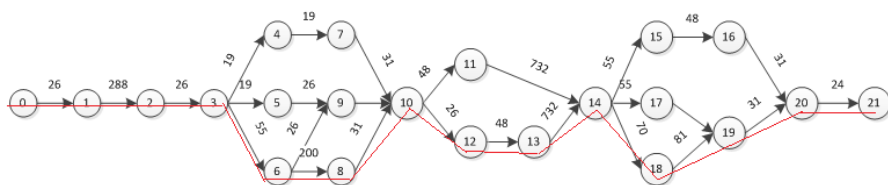
Като се знае продължителността на изпълнение на всяка работа поотделно, лесно може да се определи продължителността на изпълнение на всяка последователност по пътя на простото събиране на показателите за време на съответните работи. Може да се обобщи, че минимално необходимият интервал между началното и крайното събитие е времето, съответстващо на движението на процеса по път с най-голяма дължина на пътищата, съединяваща началното и изходното събитие. Това време се измерва със сбора $t(i,j)$ на работите, включени в пътя. Взаимовръзката между работите е такава, че всяка последователност непременно трябва да бъде спазена.

Мрежовият график на процеса „текущ ремонт на въоръжение“ има вида, показан на фиг. 5:



Фиг. 5 Мрежов график на процеса „текущ ремонт на въоръжение“

На фиг. 6 е посочен критичен път за процеса „текущ ремонт на въоръжение“ като максимален път между всички останали.



Фиг. 6. Мрежов график на процеса с посочен на него критичен път.

Пътят минава през работа (3, 6), (6, 8), защото се взема $\max\{(3, 4) + (4, 7), (3, 5) + (5, 9), (3, 6) + (6, 8), (3, 6) + (6, 9)\}$.

Критичният път е образуван от сумата от работите:

$(0, 1) + (1, 2) + (2, 3) + (3, 6) + (6, 8) + (8, 10) + (10, 12) + (12, 13) + (13, 14) + (14, 18) + (18, 19) + (19, 20) + (20, 21) = 26 + 288 + 26 + 55 + 200 + 31 + 26 + 48 + 732 + 70 + 81 + 31 + 24 = 1638$

Най-ранното време за свършване на работата е 1638 мин. (27,3 часа).

Анализът на резултата показва, че за процеса „текущ ремонт на въоръжение“ тесните места са между работа (4, 7), (5, 9), (6, 9), (6, 8), (15, 16), (17, 19), (18, 19).

Съгласно таблица 1, видовете дейности, които отговарят на тези работи са свързани със писмените разпореждания от управленските до изпълнителните логистични грани за приемане и стартиране на ремонтно-възстановителни дейности, оформянето на дефектовъчната ведомост, която от своя страна е основание пред счетоводните звена за получаване на резервни части и материали, фактическата дефектация на въоръжението, оформянето на счетоводните документи по заприхождаване на сметите след ремонта части и фактическото им предаване в склада, предаване на отремонтираното въоръжение на преките му ползватели след проверка на качеството на извършения ремонт и окомплектоването му. В настоящото изследване не се предлага оптимизиране на дейности, които са извън разглежданата система. Може само да се препоръча анализ на дейността на отговорните длъжностни лица, свързана със документооформянето и документооборота, който трябва да се осъществи, и от там намаляване на общото време за изпълнение.

Заклучение

Описаните, чрез използване на методите диаграма на последователностите и карта на процеса, модели на процеса „текущ ремонт на въоръжение“ и определянето на времетраенето на всяка от дейностите с използване на статистически и вероятностни методи дават възможност да се видят “тесните места” в системата по техническо обслужване и ремонт. Събраният чрез представителна анкета от военнослужещи, пряко отговорни за правилното водене на документите при осъществяването на текущ ремонт на въоръжението съгласно „Счетоводен документооборот в Министерството на отбраната, Българската армия и структурите на пряко подчинение на министъра на отбраната“ и анализиран емпиричен материал за продължителността на дейностите потвърждава извода, че действащият модел е бавен, много трудоемък и налага търсене на нова технология за решаване на проблема.

Литература:

1. Асанов М. О., Дискретная оптимизация, Урал НАУКА, Екатеринбург 1998.
2. Хоботов. Л. Б., Использование оптимизационно-имитационного подхода для решения задач планирования и выбора маршрута обработки. // Автоматика и телемеханика. 1/1996
3. С.Д.Кузнецов Направления исследований в области управления базами данных: краткий обзор. СУБД N 1, 1995
4. Дегтерев А.С., Ерыгин Ю.В., Лобков К.Ю. Оптимизация портфеля инновационных проектов на машиностроительном предприятии ОПК в условиях конверсии // Конверсия в машиностроении, 3/2004
5. Quality Management System – fundamental and vocabulary ISO 9000:2015
6. Христозова Латинка, Модели на процеса по проучване за надеждност на физически лица, Годишник на ИПИО, София, 2006

COMMUNICATION AND COMPUTING TECHNOLOGIES

Г. Л. Димитров,

КОМУНИКАЦИОННИ РЕШЕНИЯ ЗА БЪРЗО РАЗВРЪЩАНЕ ПО ВРЕМЕ НА БЕДСТВЕНИ СИТУАЦИИ

Георги Л. Димитров

*Висше военноморско училище "Н. Й. Вапцаров" катедра "Електроника"
Варна 9026, ул. "Васил Друмев" 73*

RAPID DEPLOYABLE POST-DISASTER COMMUNICATION SOLUTIONS

Georgi L.Dimitrov

*Nikola Vaptzarov Naval Academy, Department of Electronics
Varna 9026, 73 Vasil Drumev street*

Abstract. *In cases of disasters and accidents, rapid deployable communication solutions are necessary to recover the lost infrastructure and restore connectivity to provide assistance to sufferers and the first responders in the incident area. Designing such a network should allow fast, scalable and flexible deployment without apriori knowledge about the environment. The communication solutions should be resilient and with minimal human intervention.*

Keywords. *Rapid deployable networks, disasters, accidents, LTE 4G, RDN, cognitive radio systems*

1. Въведение

През септември 2014 ураганът Одил удря Мексико в бреговете на Калифорния. Ураганият вятър, категоризиран в четвърта степен, опустошава няколко града, където дърветата и електрическите стълбове са изтръгнати, срутени и натрошени и това предизвиква тотален срив в комуникациите. Повечето от градовете ударени от такива бури изгубват начините си за връзка и всякакви услуги с останалия свят. В резултат на такова бедствие комуникационната инфраструктура може много често да бъде напълно или частично унищожена, превръщайки засегнатата зона в остров изолиран за всякаква информация [1]. След бедствие осигуряването на връзка между спасителните екипи, например пожарна служ-

ба, полиция или парамедици, спешна неотложна помощ, става основна задача, която да позволи на първите участници да докладват своите констатации и да координират своите спасителни тактики. Ето защо, от гледна точка на комуникационните мрежи, целта е да се възстанови поне временно свързаността, за да се осигурят такъв обмен на информация. Един от начините да се преодолеят тези проблеми е да се организира и изпълни разпространена мрежа с компоненти като маршрутизатори, точки за достъп и транспондери, рипитри и приемопредаватели, които да заменят унищожените и да създадат мрежа при поискване [2].

Разполагането на мрежа в критични условия представлява важен набор от предизвикателства. Първо, предложената мрежа трябва да бъде разгръната без предварително познаване на ситуацията. Поради това, разгръщането му трябва да се изпълнява леко и възможно най-бързо, което означава, че мрежата трябва да бъде създадена бързо, почти в реално време, да замени повредената част от инфраструктурата и да облекчи претоварването. Второ, мрежата трябва да бъде адаптивна, самоконфигурируема, гъвкава, мащабируема и енергийно ефективна, за да се справи с неизвестна динамична среда на безжичните устройства, захранвани от батерии, което означава, че мрежата трябва да бъде настроена при поискване в съответствие с местонахождението и нуждите от скорост на предаването на данни. Проблеми от този тип са мотивирали дългосрочни изследователски усилия за подхода към разгръщането на мрежови компоненти, наречен RDN (rapidly deployable network - бързо разгръщащи се мрежи). Бързо развиващата се мрежа е известна също като "импровизирана мрежа" или спонтанна мрежа, е адаптивна мобилна комуникационна система, която може лесно да бъде разширена и допълвана [3]. Целта на RDN е временно да замени инфраструктурата, повредена след бедствие, за да се гарантира спешна комуникация между спасителния команден център, първите реагиращи и ако е възможно пострадалите в зоната на бедствие. Възстановяването на постоянните комуникации за засегнатото население е извън обхвата на този материал. Успоредно с това се полагат значителни усилия за подобряване на възможностите на различните технологии за професионално мобилно радио (PMR), като например подобрената и разширена услуга за данни на ETSI TETRA (TEDS), която все още има значителни ограничения по отношение на изискванията на новите аварийни приложения. Технологията Long Term Evolution (LTE 4G) се счита за технология, която да бъде използвана за нетърговски дейности в областта на обществената безопасност в бъдеще, като тази тенденция се радва на световен консенсус. Въпреки това, ключовите характеристики трябва да продължат да се прилагат в LTE, преди да може да отговаря на изискванията на системите за обществена безопасност. Тази статия обобщава основните изисквания за бързо внедряване на мрежови решения при сценарии за бедствия и представя класификация на съществуващите предложения. Описват се основните характеристики на такива приложения и се дава анализ на предимствата и слабостите на няколко подхода.

2. Изисквания към мрежите с бързо развързване

„Спонтанните“ мрежи използват безжична технология, която позволява гъвкаво, мащабируемо и мобилно внедряване с малко или никакво предварително планиране. Дори ако тези мрежи са временно решение, техният дизайн трябва да отговаря на определени минимални изисквания за осигуряване и поддържане на устойчива комуникация за първите участници. Изобщо, най-характерните изисквания за дизайна, цитирани в литературата, са както следва.[1],[4]

а. **Устойчивост:** Устойчивостта е способността да се осигури и поддържа приемливо ниво на обслужване в условията на грешки и предизвикателства пред нормалната работа. Следователно, мрежата трябва да осигурява и поддържа основни услуги при неблагоприятни условия, както и да позволява бързо и пълно възстановяване на комуникационната услуга.

б. **Основен набор от услуги:** Осъществяването на гласова комуникация традиционно е основната задача. Първите участници може да се наложи да обменят актуална информация за позицията, карти, изображения и други локално наблюдавани данни, за да се координират операциите. Освен това, в зависимост от възможностите на разгърнатата мрежа, може да е желателно поддържане на видео стрийминг, ограничен до конкретни случаи свързани със спасителни цели.

с. **Автономност и самостоятелност на мрежата:** самоуправлението, самооптимизацията и самовъзстановяването помагат да се намали нуждата от човешка намеса в доставянето и контрола на услугите, помагат да се подобри автоматизирането на процесите и да се подобри надеждността на мрежата.

д. **Мобилност:** Мобилните възли улесняват разгръщането и пренасочването на услугите, което позволява да се приспособи топологията на мрежата към условията на зоната на инцидента. Освен това позициите на възлите могат да бъдат модифицирани, с цел подобряване на работата на мрежата.

е. **Оперативна съвместимост:** В най-голяма степен разполагаемата мрежа трябва да може да работи съвместимо с други хетерогенни и невредими мрежови системи, за да разшири обхвата на предлаганите услуги. Това изискване е много желана характеристика, въпреки че нейното постигане зависи от условията на импровизация, при които мрежата е разположена.

Следващата секция въвежда основните безжични технологии, които отговарят на точно описаните изисквания.

3. Бързо развързващи се мобилни мрежи

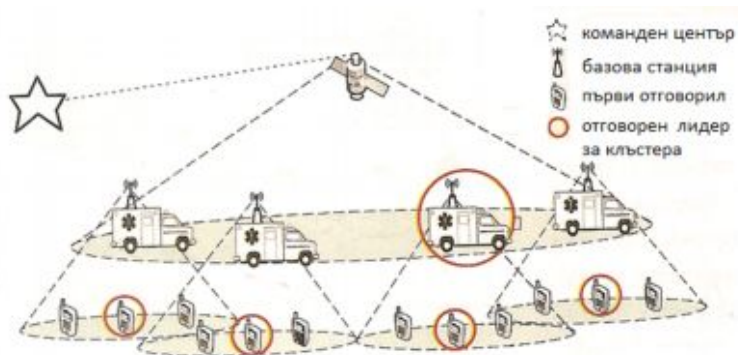
Благодарение на технологии като Bluetooth, ZigBee, HyperLAN и IEEE 802.11x, мобилните мрежи са лесни за изпълнение. Evans et al. въвежда концепцията за бързо развързващите се мрежи през 1998 г., за да поддържа връзката между военните корпуси, непрекъснато движещи се през неизвестни територии [3]. Основната идея е да се разгърне мрежовата инфраструктура в импровизиран манипулатор за предоставяне на комуникационни услуги за военни приложения, базирани на технологията за асинхронно предаване (ATM). След тази първоначална разработка се разглеждат няколко схеми за разгръщане, като изследванията са съсредоточени върху комуникациите при спешни случаи. Целта е при първа реакция командирите да се свързват с командните центрове за инциденти и по възможност с пострадали. Могат да се идентифицират две основни категории на такива схе-

ми: а) Подход при големи населени места – метрополитен и б) подходи на местно ниво. Първата цел е да се обхване една широка област и в повечето случаи мрежата е част от по-голяма аварийна система. Топологията на мрежата трябва да се приспособи към всеки отделен сценарий и всички евентуални промени в околната среда [4], [5].

3.1. Подход при големи населени места – метрополитен. Подходът на градската зона е ориентиран към разполагането на мрежови възли и устройства за покриване на голяма област вследствие на инцидента. Този подход възприема слоеста структура, в която първите отговорили са свързани с базови станции или точки за достъп, пренасяни предимно от превозни средства като линейки, полицейски автомобили или противопожарни камиони. Всяка от тези базови станции е свързана към въздушен или аерокосмически възел, например самолет или сателит, който на свой ред свързва зоната на инцидента с командния център [6], [7]. Тази архитектура е показана на фиг.1, която илюстрира полицейските автомобили, снабдени с точка за достъп, така че всяка точка покрива определена област за комуникация. Тъй като средствата на спасителните сили се използват директно, решенията от този тип често се прилагат в по-мощни случаи, като системата може да включва:

- Инструмент за наблюдение за наблюдение на зони преди, по време и след бедствие.
- Публична алармена система, която да предупреди населението за възможни природни бедствия.
- Комуникационна инфраструктура за сценарии за възстановяване след бедствие, като RDNs.
- Комуникационна инфраструктура за разпространение и обмен на информация между бедствената зона и другаде.
- Система за обработка и анализ на информация за бедствието.

Примери за такива системи са проектът за комуникация и системата за защита на гражданите (CHO-RIST) [8], проектът Wireless Deployable Net-Work System (WIDENS) [9] и схемата за виртуални клъстери (VCL) [10]. От тях последният е предложен за военни комуникационни приложения. Такива системи се основават на клъстерна организация и слоеста архитектура, в която има клъстерен лидер отговорен за всяка група от лица, сигнализиращи за първи път. Всеки клъстерен лидер действа като мост между първите които отговарят и точките за достъп, носени от превозните средства (фиг.1). По подобен начин, на ниво точка за достъп има поне един лидер, свързващ останалата част от възлите към горния слой. Един такъв слой е например спътник, действащ като портал.



Фиг. 1. Бързо развърщаща се мрежа чрез кълъстерен подход в градски условия

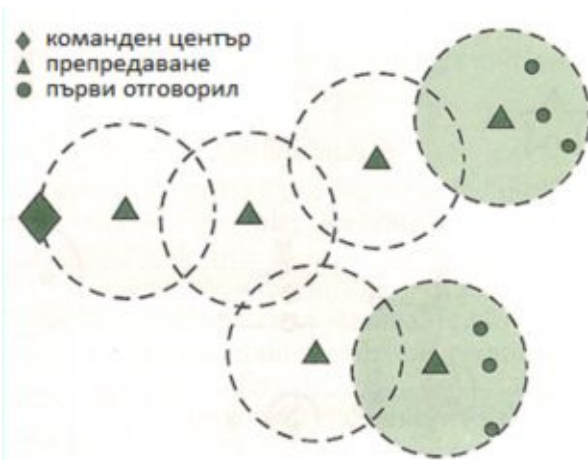
CHORIST представлява мобилна мрежа, използваща безжични маршрутизатори рутери, носени от аварийните автомобили [8]. Автомобилите се свързват автоматично по модел „пиър-към-пиър“ и образуват самостоятелен конфигуриращ се вътрешен пръстен - ядро. В покрайнините на зоната на покритие, мобилните приемопредаватели, носени от първите отговорили, са свързани с най-близкия рутер през WiFi. Така се получават локалните клетки. Отдалечената връзка с командния център се установява чрез IP “гърбнак”. По подобен начин WIDENS предлага подход при който комуникацията между словите е кръстосана. Това се съчетава с архитектура, основана на кълъстер, предоставящ висококачествена услуга, използваща ad hoc точки за достъп. Този подход включва свързване на физическо ниво и на ниво MAC адрес. Физическият слой използва реконфигурируем множествен достъп с ортогонално честотно разделяне (OFDMA) и множество антени (многооизлизат, многоизлизат - MIMO) за предоставяне на услугата пренос на данни. В допълнение, този подход включва и организиране по MAC адрес. Това става в кълъстери, където в даден набор възли, кълъстерният лидер е най-добре разположеният възел (вж.Фиг.1). Релейните възли се използват за осигуряване на взаимовръзка между кълъстерите, а свързването на създадената мрежа с други мрежи се осъществява през шлюзове-възли. Концепцията е наречена **terminode** – краен възел. Това означава, че всеки възел в мрежата може да изпълнява функциите на кълъстерен лидер, релейна станция, маршрутизатор или шлюз, в зависимост от местоположението и изискванията за осигуряване на комуникациите. Така възлите могат динамично да променят ролята си и да използват технология на кръстосана комуникация между словите. Това води до висока производителност на мрежата. Схемата за виртуално разпределение на клетките за тактически комуникации разделя определена област на покритие на фиксирани виртуални клетки, подобно на разпределянето при клетъчните мрежи (3G). Точките за достъп използват ресурсите на виртуалните клетки (VCL), за да създадат клетка, която се движи над останалите. Радиостанциите които са в отделните хора ползват малки клетки, като всяка клетка има възел, играещ ролята на лидер. Тези клетки се групират в по-голяма клетка чрез точките за радиовръзка. И накрая, всички клетки се обединяват чрез спътникова връзка или безпилотен авиационна платформа(UAV). Подходът се фокусира върху адаптирането на 3G технологиите към тактическите системи. Про-

ектът [11] на SALICE (Сателитна помощна локализация и комуникационна система за спешни услуги) се фокусира върху интегрирана навигационна (NAV) / комуникационна (COM) система за аварийни сценарии. В тази архитектура, спасителните екипи в мрежата на инцидента са организирани в подобни групи или клъстери. Основните изследователски теми на гореспоменатия проект са техниките за локализация, софтуерно дефинирана радиовръзка (SDR) и когнитивни радиоапарати NAV/COM, интегрирането на спътници и платформи опериращи на висока надморска височина (HAPs) в работата на спасителните служби и приемането на хетерогенни решения в зоната за намеса.

Като обобщение, подходът при големите населени места – метрополитен, осигурява широколентова свързаност за спасителните екипи основно за мащабни сценарии. Този подход предлага ограничени възможности за пренасочване или подобряване на търсенето, тъй като превозните средства, носещи възлите, имат ограничена мобилност. Поради това тяхното местоположение може да се окаже не оптимално за обслужване на всички мобилни устройства, работещи в зоната на инцидента.

3.2. Подход чрез изграждане на локална свързаност. За разлика от подхода при големите населени градски области, при работа на местно ниво се предоставят услуги на място. Необходимо е да се създаде мрежа в целевата зона чрез разпределени, евтини, адаптивни решения, които да се развърнат на ход. Следователно, алгоритмите за внедряване трябва да могат да работят без никаква предварителна информация за околната среда. Функционалността на местните подходи зависи от следните фактори особено силно – изисквания за размер, тегло и мощност. По този начин, ниските характеристики са желателни при внедряването на бързо развързващи се мрежи – малък размер, малко тегло. Съществуват два типа механизми, класифицирани въз основа на стратегии за внедряване: „трохи“ и мобилна „гръбначна“ структура.

Терминът "трохи" е позоваване на добре известната приказка "Хензел и Гретел", в която Хензел изпуска трохи за проследяване на пътя до дома. В контекста на мрежите за бързо развързване, „трохите“ представляват малки и евтини предаватели. Тяхната единствена цел е да предават пакети информации между крайните възли. По този начин, в дадена спешна ситуация, първите отговорили са снабдени с няколко устройства за предаване през мобилно радио. Мобилните потребители трябва да пускат тези устройства на редовни интервали, докато се придвижват в аварийната зона, за да поддържат връзка с командния център. Предаването на информацията прекъсва по заявка, за да се създаде статичен ad hoc гръбнак, адаптиран към околната среда.



Фиг. 2. Концептуална схема на принципа на „трохи“

На фигура 2 е показан пример за мрежа, основаваща се на тази концепция. Команден център поддържа комуникация с мобилните потребители чрез предаватели, пуснати от първите отговорили, като по този начин постепенно се разширява обхвата. Като предимства на подхода "трохи", могат да бъдат изтъкнати следните:

- Активира създаването на мулти-хоп мрежа при поискване.
- Позволява комуникация между първите отговорили, веднага щом се включат предавателите.
- Позволява комуникация с изолирани предаватели.
- Гарантира надеждна комуникация.
- Предлага разширена зона на покритие.
- Намалва вероятността за разделяне на мрежата.

Основният проблем, който трябва да бъде разгледан, е кога и/или къде да се поставят предавателите за установяване и поддържане на свързаност за първите отговорили. Да се установят прости, статични правила за отпадане на предаватели – само на определено разстояние, един предавател на етаж или на всеки три врати се възприема като наивен подход. Предавателите трябва да бъдат винаги в комуникационните обхвати на другата страна и следва да се съобразяват явления като интерференция, затихване на канала, фонов шум или скрит проблем [12, 13]. По този начин целта е да се разработи алгоритъм за вземане на решение за внедряване, който да подобрява максимално ефективността на мрежата.

Проведени са обширни проучвания, за да се отговори на проблема с разполагането на предавателите. Алгоритмите наблюдават качеството на връзката чрез измервания на индикатора за силата на получения сигнал (RSSI), съотношението сигнал към шум (SNR) [12] или широчина на честотната лента. Такива измервания могат да бъдат получени чрез сонди, изкуствено поставени в мрежата или въз основа на контролни съобщения, получени директно по протокола за маршрутизация. Съществува праг за задействане на събитие за разполагане. След като качеството на връзката падне под този праг, потребителят трябва да пусне нов предава-

тел. Например алгоритмите, представени в [12], използват предварително определен праг за всички приложения, докато този в [13] определя прага, базиран на честотната лента, необходима за всяко приложение. Разгръщането се извършва ръчно от първия отговорил. По този начин, за да се уведоми потребителя се изпълнява и предупредителен сигнал - светлинен или звуков. Ето защо ефикасният алгоритъм за внедряване трябва да е в състояние да следи промените в мрежата, за да задоволи потребностите на предавателите. Например, контролни съобщения се добавят към заглавната част на контролния пакет от протокола за рутинане. По този начин, внедряването на предавателя се задейства или защото мобилният потребител открива деградиране на качеството на връзката, или защото получава заявка за разгръщане от своите съседи. Последният случай възниква, когато мобилен потребител изгуби покритие. Следователно мобилният потребител трябва да изпраща на своите съседи съобщение за искане друг потребител да пусне предавател. След като бъде взето решение за внедряване, кандидатите, които ще бъдат разгрънати, излъчват съобщения за ново включване. Souryal et al. предлагат алгоритъм въз основа на бърза оценка на физическия слой, осъществен от мобилния предавател [12]. Предавателят непрекъснато излъчва пакети към предварително преместените приемници. Когато приемникът е в обхвата на комуникацията, той отговаря с потвърждаваща поредица. След това се прави измерване на съотношението сигнал шум SNR. Ако максималната стойност падне под праговото ниво, трябва да се намери друг предавател. Подходът „трохи“ е подходящ за разширяване на комуникационното покритие за първите участници в сценария.

4. Дискутирани въпроси и заключения

В тази статия е направен общ преглед на решения за бързо внедряване на комуникационни мрежи при настъпили аварии и бедствени ситуации. Това представлява ключова задача, тъй като комуникацията между спасителните екипи и пострадалите зависи от това заместване на съществувалата инфраструктура. Предложена е класификация на подходите. Основните различия между тези решения се крият в наличните ресурси и способностите на екипа, който ще разгръне спонтанната мрежа.

През последните години, поради широкото разпространение на мобилни смарт устройства като смартфони, лаптопи и таблети, възникват нови възможности за използването им при сценарии за бедствия. Такива устройства обикновено са снабдени с WiFi, Bluetooth, 3G или 4G радио интерфейси и са оборудвани с GPS приемници за самостоятелно позициониране. Всички тези характеристики могат да се ползват за активиране на комуникации от устройство към устройство. А вградените сензори, като видеокамери и фотоапарати, могат потенциално да предоставят на екипите за спешна помощ точна представа на случващото се в зоната на бедствие.

Литература

- 1.Y. Ran, "Considerations and Suggestions on Improvement of Communication Network Disaster Countermeasures after the Wenchuan Earthquake," *IEEE Commun. Mag.*, VOL 49, no. 1, Jan. 2011, pp. 44-47.
- 2.K. Mase, "How to Deliver Your Message from/to a Disaster Area," *IEEE Commun. Mag.*, vol. 49, no. 1, Jan. 2011, pp. 52-57.

- 3.J. Evans, *et al.*, "The Rapidly Deployable Radio Network," *IEEE JSAC*, VOL 17, no. 4, Apr. 1999, pp. 689-703.
- 4.F. Legendre *et al.*, "30 Years of Wireless Ad Hoc Networking Research: What about Humanitarian and Disaster Relief Solutions? What are We Still Missing?" *Proc 1st Intl Conf. Wireless Technologies for Humanitarian Relief (ACWR)*, Amritapuri, Kollam, Kerala, India, Dec. 2011, p. 217.
- 5.R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 43, no. 3, Mar. 2005, pp. 123-31.
- 6.S. Ghafoor *et al.*, "Cognitive Radio for Disaster Response Networks: Survey, Potential, and Challenges," *IEEE Wireless Commun.*, vol. 21, no. 5, Oct. 2014, pp. 70-80.
- 7.M. Berioli *et al.*, "Aerospace Communications for Emergency Applications," *Proc. IEEE*, vol. 99, no. 11, Nov. 2011, pp. 1922-38.
- 8.H. Aiache *et al.*, "Increasing Public Safety Communications Interoperability: The CHORIST Broadband and Wideband Rapidly Deployable Systems," *Proc Next Generation Public Safety Communication Networks and Technologies (NGenSafe)*, Dresden, Germany, Jun. 2009.
- 9.H. Aiache *et at*, "WIDENS: Advanced Wireless Ad-Hoc Networks for Public Safety," *Proc 1ST Mobile & Wireless Communications Summit*, Dresden, Germany, Jun. 2005.
10. E. Cayirci and C. Ersoy, "Application of 3G PCS Technologies to Rapidly Deployable Mobile Networks," *IEEE Network*, vol. 16, 2002, pp. 20-27.
11. E. Del Re *et at*, "SALICE Project: Satellite-Assisted Localization and Communication Systems for Emergency Services," *IEEE Aerospace and Electronic Systems Mag.*, vol. 28, no. 9, Sep. 2013, pp. 14-15.
12. M. R. Souryal *et at*, "Real-Time Deployment of Multihop Relays for Range Extension," *Proc 5th Intl. Conf. Mobile Systems, Applications, and Services (MobiSys)*, San Juan, Puerto Rico, Jun. 2007, pp. 85-98.

Г. Л. Димитров,

МОБИЛНА РОБОТИЗИРАНА КОМУНИКАЦИОННА МРЕЖА ЗА БЪРЗО РАЗВРЪЩАНЕ В СЛУЧАИ НА АВАРИИ И БЕДСТВИЯ

*Висше военноморско училище “Н. Й. Вапцаров” катедра “Електроника”
Варна 9026, ул. “Васил Друмев” 73*

RAPID DEPLOYABLE ROBOTIC COMMUNICATION NETWORKS FOR CRITICAL SITUATIONS

Georgi L.Dimitrov

*Nikola Vaptzarov Naval Academy, Department of Electronics
Varna 9026, 73 Vasil Drumev street*

Abstract *In critical post-disaster situations, rapid deployable communication solutions are sorely needed. In this paper has been considered a robotic backbone approach which allows for easy recovery of connectivity, featuring at the same time autonomous mobility and self-development. Robotics reduces the need for human intervention. The ubiquity of modern mobile devices has risen usage in disaster scenarios.*

Keywords. *Rapid deployable communication networks, robotic backbone approach, intelligent automation, disaster, accidents*

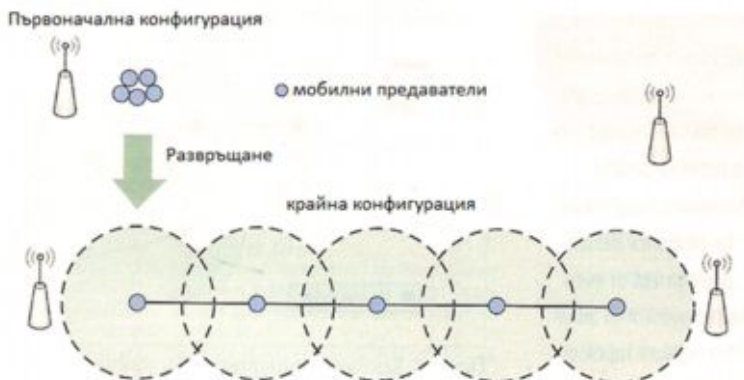
1. Въведение

Възможността за комуникация на първите, отзовали се в случаите на бедствие, представлява най-критичният компонент на ефективното реагиране при извънредни ситуации. Деветдесет и два процента от анкетираните потърпевши в такива моменти отговарят че достъпът до гласовите комуникации и не само разговорите, а и изпращането на снимки и друг вид информация, дефинитивно ще подобри реакцията на съответните органи. Ако при инцидент липсват комуникации, координаторът не може да управлява. Способността да се възстанови веднага комуникацията, ако съществуваща мрежа не работи или да се установи връзка, където няма инфраструктура, е изключително полезно за обществената безопасност. Бързо развърщане на комуникации се налага в ситуации, като например: пожари, големи местопрестъпления, природни бедствия, заложници прекъсване на електро-захранването, терористични актове при големи спортни събития или концерти. В допълнение към унищожаването на инфраструктурата, останалите комуникационни мрежи, например мобилните мрежи може да са недостатъчни поради големия брой хора, които се опитват да се обадят на службите за спешна помощ или да комуникират с близките си. Разполагането на мрежа в критични условия представлява важен набор от предизвикателства. Предложената мрежа трябва да бъде разгърната без познаване на околната среда. Поради

това, разгръщането му трябва да се изпълнява леко и възможно най-бързо, което означава, че мрежата трябва да бъде създадена бързо, почти в реално време, за да замени повредената част от инфраструктурата и да облекчи задръстванията. Мрежата трябва да бъде адаптивна, самоконфигурируема, гъвкава, мащабируема и енергийно ефективна, за да се справи с неизвестна динамична среда на безжичните устройства, захранвани от батерии, което означава, че мрежата трябва да бъде настроена при поискване в съответствие с местонахождението и нуждите от скорост на предаването на данни.

2. Изграждане на Мобилна роботизирана структура

Решенията за бързо внедряване на мрежа в отговор на спешни обстоятелства имат за цел да възстановят връзката, когато съществуващата мрежова инфраструктура е била унищожена или никога не е съществувала. Тези предложения се основават най-вече на безжичните мобилни мрежи, ad hoc и клетъчните технологии и приемат различни подходи за определяне как, къде и кога трябва да бъдат разположени устройствата, съставляващи бързо разгръщащите се мрежи. С подхода на каскадно свързващи се приемопредаватели [1] се постига сериозен успех благодарение на гъвкавостта и ефективността на разходите. Въпреки това, приемопредавателите остават статични, след като бъдат развърнати, което е основният недостатък на тази стратегия. Ако в крайна сметка се променят условията на околната среда, структурата на мрежата е възможно да не се адаптира към новите условия. През последните години се наблюдава разработване на механизми, подобни на подхода описан в [2]. При такава конфигурация приемопредавателите са снабдени с автономна мобилност и саморазвиване. Тази възможност позволява на мобилните предаватели да приспособяват собствените си места при заявка. Този подвижен роботизиран подход се улеснява от напредъка през последните десетилетия в роботиката и автоматизацията. Целта на роботизираната мрежа е да осигури комуникационна свързаност на мобилните потребители с минимална човешка намеса по време на разгръщането. Групата мобилни приемопредаватели трябва да може да се самоорганизира и да се използва самостоятелно и ако е възможно, да оптимизира работата на мрежата. „Гръбнакът“ на мрежата представлява безжична релейна мрежа на базата на работи. На фиг. 1 е показана концепцията за такава мобилна мрежа. Мобилните релейни устройства се поставят в първоначална конфигурация, наведнъж заедно или поотделно. Следвайки алгоритъм за внедряване, те ще се разпространят самостоятелно в целевата зона, като създават безжичната структурна мрежа – „гръбнак“. Могат да се идентифицират два вида схеми в тази категория. Схемите от първия тип се основават на стратегии, свързани с образуването на верига, т.е. роботите следват една верига (фигура 1). Сред тях Pezeshkian et al. предлага първоначален режим на следване на лидер, образувайки линия [2]. Когато деградацията на сигнала (RSSI) достигне определен праг, най-отдалеченият приемопредавател по линията ще спре и ще се отдели като стане статичен. Този процес се повтаря, докато всички предаватели станат статични възли.



Фиг. 1. Верижно развързване на мобилна роботизирана комуникационна мрежа

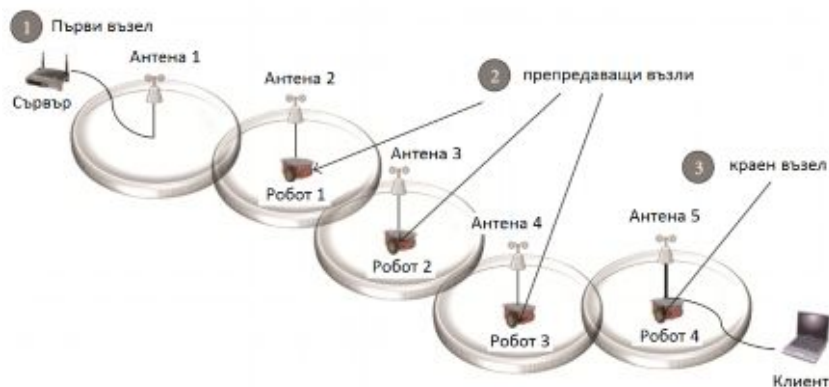
Сред тях Pezeshkian et al. предлага първоначален режим на следване на лидер, образувайки линия [2]. Когато деградацията на сигнала (RSSI) достигне определен праг, най-отдалеченият приемопредавател по линията ще спре и ще се отдели като стане статичен. Този процес се повтаря, докато всички предаватели станат статични възли.

По същия начин Nguyen et al. разглежда случая на две точки за достъп, всяка от които е извън обсега на другата [3]. Изградена е верига от предаватели за възстановяване на връзката между тези две точки за достъп. Предложеният от авторите алгоритъм разглежда три типа приемопредаватели - водещ, последовател и опашка, като всеки се движи, както е посочено, в зависимост от типа му. Всички предаватели се намират първоначално близо до първата точка за достъп. След това лидерът се придвижва напред, докато не намери следваща точка за достъп. Всеки път, когато стойността на сигнала падне под определен праг, приемопредавателят - последовател ще се премести, за да поддържа връзката между първата точка за достъп и лидера. Този последовател ще преследва възела преди него, за да създаде верига. След като лидерът достигне подходяща точка за достъп, той „спира“, поради добра стойност на сигнала (RSSI). Останалите приемопредаватели ще спрат итеративно въз основа на същото правило. В двата гореспоменати алгоритъма [3, 4] се приема, че има разлика между мобилните предаватели-роботи, т.е. има водещи роботи и роботи - последователи. Такава диференциация може да се разглежда като слабост, защото движението на последователите зависи от движението на лидера. Ако лидерът не успее по някаква причина, това ще доведе до провал в останалата част на комуникационната верига.

3. Концепция на верижно развързваща се мрежа

Алгоритъмът който бе споменат по-горе притежава два етапа: линейно разрастване и оптимизиране на „гръбначната“ свързаност. Роботизираните единици могат да развърнат автоматично мобилна широколентова мрежа, като има възможност пропускателната способност да нараства, намалявайки броя на участъците с препредаване. Безжичният сигнал се препредава от сървър към клиента. Всеки робот пренася една точка за достъп, като се формира линейно разрастваща се мрежа покриваща мащабни разстояния. Ако се добавят допълнителни антени и радио

оборудване стават възможни и допълнителни многопътни комуникации. Броят на мобилните роботизирани устройства зависи от изискванията на мрежата. Броят на възлите, които формират линията на комуникация и броят на мобилните устройства е еднакъв. За да се формира връзка, минималният необходим брой е три – един лидер, втори последовател и един последен – на опашката за връзка със сървъра.



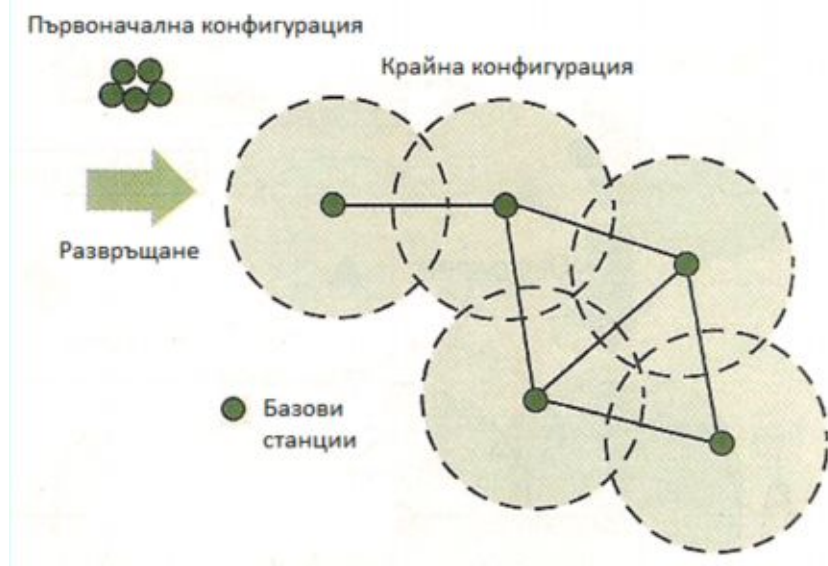
Фиг. 2. Самоконфигурируема безжична мрежа, използваща мобилни роботи, носещи приемопредаватели и антени

Алгоритъмът е настроен така, че роботите винаги да наблюдават силата на радио сигнала, за да определят кога да се задействат. В този алгоритъм всеки робот е отговорен за определянето на качеството на сигнала от преходния робот, като този който е на опашката следи сигнала на стационарната точка за достъп на шлюза – гейтуей. С такава идея ако една точка за достъп се придвижи, цялата система се придвижва, като създава последователни „вълни“ на задействане на покритието. Всяко роботизирано устройство има назначен приоритет и определно ниво на радиосигнала който проследява. Възлите имат възможност да се преразпределят [3]. Използват се индикатори като сила на сигнала, фактор на препредаването и праг на роуминга. Според логиката на алгоритъма се намаляват препредаванията на трафика. (вж Фиг.2). Втората част е свързана с оптимизиране на „гръбначната свързаност“. При тази задача съществува водещо роботизирано мобилно устройство. Тази мобилна единица се придвижва напред според зададената топология на мрежата до момента в който открие краен възел. Така при това действие се преценява какъв брой участъци на препредаване да се ползват и каква дистанция „ще пропътува“ трафика. Алгоритъмът за оптимизиране зависи от способността на мрежата да преразпределя трафика през точките за достъп.

4.Подвижна автономна рутерна система (MARS - mobile autonomous router system)

По подобен начин позволява на мобилните приемопредаватели да се разположат самостоятелно в линия. Основната разлика обаче е, че при този вариант всички възли са равнопоставени [4]. Всеки мобилен приемопредавател се настройва в зависимост от характеристиката на качеството на връзката в опит да постигне

възможно най-доброто приемане по отношение на честотна лента. Схемите от втория тип се основават на стратегии, които се стремят да разпространят възлите, за да покрият дадена област колкото се може по-добре (Фигура 3). Например, в [5] Тимотеу и Лука докладват роботизиран алгоритъм за разгръщане на гръбнак, базиран на местата на блокирани пострадали. Целта е да се увеличи броят на свързаните пострадали, за да се улесни създаването на комуникация между тях и спасителния команден център. Роботите търсят пострадали и си сътрудничат, за да поддържат връзката на гръбнака. За тази цел всеки робот с приемопредавател контролира собствените си движения, като изпълнява три основни стъпки: проучване, свързване и установяване. По време на първата стъпка роботът изследва зоната, търсеща пострадали. Роботът ще спре да се движи, ако неговото движение наруши връзката на мрежата или ако роботът осъществи връзка с пострадалите.



Фиг. 3. Концепция за разпределна мобилна роботизирана мрежа

Във втория случай роботът ще се превърне в клъстерен лидер и ще възложи задачата за изследване на следващите роботи. Един недостатък на тази технология е, че се предполага роботите да имат априори информация за зоната на бедствие. Тази информация обаче не винаги е налице предварително. Работата, представена от Reich et al. [6] е от същия тип. Тези автори разглеждат мобилна мрежа, която автоматично поддържа собствена свързаност, като непрекъснато премества своите възли. Авторите предлагат алгоритъм за саморазпространение на мобилните възли в дадена област. Всеки възел, който се движи самостоятелно, използва знания за радиуса в две стъпки, за да определи кога да прекрати своето движение въз основа на критерия за вземане на решение. Този критерий представлява риск от разделяне или прекъсване на мрежата. По този начин всеки възел изпълнява алгоритъма, по такъв начин, че да се поддържа свързаност. Алгоритъмът работи, както следва: ако

даден възел все още има поне един предварително определен брой свързвания на връзката със своите съседи, той продължава да се премества. Той може да увеличава разстоянието от съседите си. В противен случай възелът трябва да спре движението, защото всяко движение ще доведе до прекъсване. Мобилният роботизиран подход значително намалява необходимостта от човешка намеса в разгръщането на мрежата. Освен това мобилността на възела позволява гъвкаво разполагане или дори пренасочване, за да се адаптира топологията на системата към различни вътрешни и външни сценарии. По-специално, възлите в схемата от втория тип могат да бъдат конфигурирани да се раздалечат, като същевременно поддържат многопътна комуникация. Въпреки че размерът и теглото на всеки възел може да са много ниски, консумацията на енергия остава ключов фактор за производителността. По този начин човек, който изпълнява импровизираната „спонтанна“ мрежа, трябва да има способността да решава какъв вид комуникации да се ползват в реално време, защото такива решения са жизненоважни за успеха на разгръщането.

5. Дискутирани въпроси и изводи

Бъдещите разработки ще включват също внедряването на системи, които да ползват външни антени, както за всички посоки, така и насочени. Освен това могат да бъдат разработени механизми за увеличаване на височината на антените, с цел увеличаване на покритието и мрежовата ефективност. С проведенния експеримент на екипа на Nguyen *et al* [3] [7] се доказва възможността за изграждане на мрежи за мобилни широколентови комуникации, използващи роботи. Възможно е още повече да се подобри работата на мрежата, като се намали броя на препредаването на мрежовия трафик (хоп участъците) спрямо най-отдалечения възел. Тази операция се извършва автономно. Ако мобилно устройство се придвижва по-близо до възела на опашката, цялата система се адаптира автоматично, за да възприеме промяната. Чрез използването на проста концепция за радио сенсификация, идеята за мрежа с мобилни роботи може да бъде доразвита, за да бъде приложима към автоматизирани платформи, проправящи път към нова ера на безжична комуникация и услуги почти навсякъде и по всяко време по света.

Разработването на наистина ефективна комуникационна мрежа след бедствие или авария все още изисква значителни усилия. Бъдещите предложения трябва да позволяват гъвкаво внедряване или преразпределение на ресурсите, с цел приспособяване към условията на всеки сценарий. Решенията следва да функционират с минимална човешка намеса в района на инцидента и трябва да бъдат съвместими с настоящите технологии. При осигуряване на комуникационни решения за бързо разгръщане не трябва да се пренебрегва въпросът за енергоснабдяването, което е изключително критично при безжичните устройства, захранвани с батерии.

Литература

1. R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 43, no. 3, Mar. 2005, pp. 123-31.
2. N. Pezeshkian, H. G. Nguyen, and A. Burmeister, "Unmanned Ground Vehicle Radio Relay Deployment System for Non-Line-of-Sight Operations," *Proc 13th LATED Intl. Conf. Robotics and Applications, WUrzburg, Germany, 2007*, pp. 501-06.
3. Nguyen C. *et al.*, "Using Mobile Robots to Establish Mobile Wireless Mesh Networks and Increase Network Throughput," *Intl. J. Distributed Sensor Networks (1.1DSN)*, vol. 2012, 2012, pp. 1-13.

4. K.-H. Kim, K. G. Shin, and D. Niculescu, "Mobile Autonomous Router System for Dynamic (Re)formation of Wireless Relay Networks," *IEEE Trans. Mobile Computing*, vol. 12, no. 9, 2013, pp. 1828-41.
5. S. Timotheou and G. Loukas, "Autonomous Networked Robots for the Establishment of Wireless Communication In Uncertain Emergency Response Scenarios," *Proc. 2009 ACM Symposium on Applied Computing (SAC)*, Honolulu, Hawaii, USA, Mar. 2009, pp. 1171-75.
6. J. Reich, V. Misra, D. Rubenstein, and G. Zussman, "Connectivity Maintenance in Mobile Wireless Networks via Constrained Mobility," *IEEE JSAC*, vol. 30, no. 5, Jun. 2012, pp. 935-50 ...lera *et al.*, "Making a Mesh Router/Gateway from a Smartphone: Is that a Practical Solution?" *Ad Hoc Networks*, vol. 9, no. 8, Nov. 2011, pp. 1414-29.
7. G. Aloï *et al.*, "STEM-Net: An Evolutionary Network Architecture for Smart and Sustainable Cities," *Trans. Emerging Telecommunications*

М. Х. Ламбева

СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ. ВЪЗМОЖНОСТИ ЗА ОЦЕНЯВАНЕ

Милена Х. Ламбева

*гр. Шумен, ул. "Карел Шкорпил" 1, Национален военен университет "Васил Левски",
Факултет "Артилерия, противовъздушна отбрана и комуникационни
и информационни системи"*

INTEROPERABILITY OF INFORMATION SYSTEMS FOR MANAGEMENT. POSSIBILITIES FOR ASSESSMENT

Milena H. Lambeva

Abstract: Every area of human activity that is assisted by information systems is affected by the problem of "incompatibility". Finding effective methods for measuring, assessing, and analyzing compatibility is an important step towards resolving it. This work analyzes existing compatibility assessment methodologies and formulates general recommendations for future research.

Keywords: interoperability assessment, compatibility

Проблемът със съвместимостта между информационните системи не е нов. Департаментът по Отбрана на САЩ официално обявява неговото съществуване преди повече от петдесет години. В следствие изследванията надхвърлят рамките на военните организации, и той е припознат във всички области на човешката дейност, която се подпомага от информационни системи – на практика навсякъде.

В резултат в момента са известни десетки определения на понятието „съвместимост“, а в литературата са идентифицирани повече от шестдесет вида [3] несъвместимост.

Несъвместимостта между информационните системи, се изразява в невъзможността те, или отделни техни компоненти да обменят своевременно и ефективно данни, информация или знание, и да използват обменените данни, информация или знание.

Основните предпоставки за несъвместимостта са:

- различия между апаратните средства и протоколите за комуникация;
- неспособността на входно-изходните приложения да обменят данни по между си, определя се от различията между:
 - алгоритмите в приложния софтуер, които обработват и представят информация на потребителя;
 - използваните форми на документирано ръководство на разработване, внедряване и оперативен контрол на всяка от системите;

- стандартите за техническа и системна архитектура (хардуер, системен софтуер, комуникации, данни, приложения и др.);
- несъвместимостта на данните, обуславяща се от семантични, синтактични и лексикографични различия.

Проблемът „несъвместимост“ на информационните системи се характеризира с устойчивост и комплексност.

Устойчивостта се определя от:

- непрекъснато изменение на гореизброените причини за неговото съществуване.

Те от своя страна са резултат от динамичното развитие на информационните и комуникационните технологии. Системните архитекти разполагат с богат избор от продукти за разработка със сходни функционални възможности, използват различни стандарти или техни версии, а често официалното утвърждаване на стандартите се изпреварва значително от тяхното „де факто“ признаване. Съвременните технологии за обработване и използване на информацията дават възможност да се решават все по-голям кръг от задачи, в следствие от което информационните системи стават все по-разнородни по множество показатели.

- динамично изменение на условията за взаимодействие между системите, която се изразява в промяна:

- на състава на взаимодействащите си системи.

Съвместната работа на военните информационни системи в рамките на коалиция, например е краткосрочна. Коалициите се формират в отговор на криза, или назряващ конфликт и съществуват до решаването на конфликтната ситуация. При възникване на друг конфликт, новосформираната коалиция може да бъде с променен състав от информационни системи.

- в характеристиките на системите, което е резултат от тяхната еволюция (тяхното развитие).
- в изискванията относно обменяната информация (предметна област, семантика, синтаксис);
- в изискванията относно характеристиките на обмен на информация (време, степен на участие на човека и др.)

Ето защо постигането на състояние на взаимодействие между системите, при което информация и услуги могат да бъдат обменяни пряко и задоволително между тях и/или техни потребители, е въпрос, който трябва да се поставя на разглеждане през целия им жизнен цикъл.

Другата страна на проблема е, че описанието на съвместимостта между системите чрез двете полярни състояния – несъвместимост и съвместимост, изкуствено би довело до неточност в оценката, тъй като между състоянието на пълна липса на съвместимост, която се изразява в тотална невъзможност на системите да обменят данни, до пълна съвместимост има широка гама от състояния, които се характеризират с различна степен в която системите са готови да обменят данни, информация или знание, в условията на различни ограничения. Поради тази причина всички известни модели на съвместимостта да разграничават степени на градация на свързаност и способност за обмен на данни, които наричат „нива на съвместимост“.

В тази връзка на постигането на определено ниво на съвместимост трябва да се разглежда не като еднократен акт, а като процес на многократно преход към по-високо ниво.

Ето защо определянето (измерването) и оценяването на текущото състояние на съвместимостта е условие (е необходимо) за да бъде възможно да се формулират конкретни цели за нейното усъвършенстване.

Съществуват в практиката три различни подхода ~~за измерване на~~, всеки от които притежава предимства и недостатъци:

- емпиричен;
- симулационен;
- теоретичен.

Емпиричният подход се състои в провеждане на експеримент в специализирана тестова среда или в реална обстановка и дава оценка най-близка до реалната оценка. Негов недостатък е голмият разход на ресурси (време и човешки усилия).

Симулационният подход изисква създаване на модели на изследваните системи. Неговата точност се доближава до тази на експерименталния.

Теоретичният подход е аналитичен подход, който оценява съвместимостта между модели на системите. При него, в сравнение с другите два, е по-трудно да се даде оценка най-близка до реалната, но негови предимства са краткото време, за което се формира оценката и ниския разход на ресурси. Друго негово съществено предимството е възможността, способностите на системите за колаборация да се оценяват, на всеки етап от жизнения цикъл, включително и по време на проектиране. Своевременно получената оценка на съвместимостта подпомага вземането на решение от системния архитект или системния интегратор.

Към момента са известни повече от петнадесет методологии за теоретично определяне на съвместимостта. Значителна част от тях, предимно тези публикувани преди 2007 година, са разработени от, или с подкрепата на НАТО или на министерството на отбраната на страна член на НАТО.

Най-рано, през 1980 е публикувана методологията на Агенцията за отбранителни информационни системи (DISA) на Министерството на отбраната на САЩ – „Спектър на оперативна съвместимост“ (Spectrum of Interoperability - SoIM). Тя има важна роля в областта на оценяването на съвместимостта, защото макар да няма широко приложение, служи за прототип на всички по-късно разработени методологии. Публикуваната девет години по-късно „Методология за Количествено определяне на оперативната съвместимост“ (Quantification of Interoperability Methodology (QoIM), под ръководството на Корпорация MITRE) и моделът Оперативна съвместимост на военни комуникации и информационни системи (Mil Comm. & Info Systems Interoperability (MCISI), 1996 г.), също не успяват да получат широка известност.

Като най-успешна, през последните двадесет години се утвърждава методологията предложена от работна група към Министерството на отбраната на САЩ (DoD C4ISR Architecture Working Group) през 1998 г. – „Нива на съвместимост на информационните системи“ (Levels of Information System Interoperability (LISI) [1].

Тя представява комплекс от средства за: определяне, оценка, измерване и повишаване на съвместимостта през целия жизнен цикъл на информационната система. LISI предоставя инструменти за теоретично решаване на следните задачи:

- оценка степента на съвместимост на една информационна система, в смисъла на нейно качество, което изразява способността ѝ да се интегрира с други такива при определени условия;
- оценка на степента на съвместимост между няколко системи, в смисъла на способността им да обменят пряко и задоволително информация и услуги по между си;
- оценка на възможността за повишаване на нивото на съвместимост между системите, т.е. на определяне на потенциалната съвместимост;
- управление на процеса на повишаване на степента на съвместимост между системите;
- определяне на изисквания по отношение на съвместимостта при проектиране на нови системи.

Тези оценки, по подобие на SoIM, се формират на базата на съответствието на възможностите на системите за комуникация, на различни степени на зрялост на съвместимостта.

Моделът на зрялост на LISI дефинира пет основни нива (всяко от които с различен брой поднива) на съвместимост, характеризиращи се с нарастване на сложността и прецизността на взаимодействието между информационните системи:

Ниво 0 – Изолирани системи. Информационната среда се характеризира с липса на възможност за електронен обмен на данни.

Ниво 1 – Свързани системи. Свързаността е от тип „Peer-to-Peer”. Съществува възможност за обмен между работни станции на ограничен капацитет от данни – тактови или графични файлове, електронни писма.

Ниво 2 – Функционална съвместимост. Характеризира се с разпределена изчислителна среда, в която се осъществява обмен на информация на базата на унифициран логически модел на данните.

Ниво 3 – Домейни. Информационното пространство е структурирано в отделни функционални области – домейни. Макар системите от състава на домейна да са хетерогенни и да запазват възможността си да функционират самостоятелно, те споделят общи хранилища за данни и споделят информация, която подпомага вземането на решение в рамките на домейна.

Ниво 4 – Оперативна съвместимост в универсална изчислителна среда. Това е най-високата степен на съвместимост. Системите от това ниво работят в глобално информационно пространство, разпределено в множество домейни. Множество от потребители могат едновременно да осъществяват достъп до, и да взаимодействат със сложни данни. Данните са напълно споделени и имат обща интерпретация.

Авторите на методологията систематизират множеството от характеристики, които трябва да бъдат оценени с оглед да се определи нивото на зрялост на съвместимостта в четири основни групи, които те наричат „атрибути”: процедури, приложения, инфраструктура и данни.

За оценка на степента на съвместимост между системите за командване и управление в НАТО се използват сходни на методологии: Директивата по съвместимостта на Алианса [6], която дефинира пет нива на съвместимост и STANAG 5048 [7], който дефинира шест.

През последните няколко години са разработени и се използват модели за оценка на съвместимостта на информационни системи, обслужващи области извън сигурността и отбраната. Такъв е моделът на зрялост на оперативната съвместимост

мост (Interoperability Maturity Model – IMM). Той е разработен в рамките на ръководената от Европейската комисия програма „Решение за съвместимост за публичните администрации, бизнеса и гражданите” (Interoperability solutions for public administrations, businesses and citizen) и е предназначен за оценка и повишаване на оперативната съвместимост на европейските обществени услуги.

Подобно на описаните горе методологии, IMM оценява съвместимостта в няколко степени (таблица 1) чрез измерване и оценка на няколко компоненти: доставка на услуги, потребление на услуги, посредничество за доставка на услуги и управление на услугите.

Да се направи описание на съществуващите методологии за оценка на съвместимостта е трудно, и със съмнителна практическа полезност. На част от тези, за които беше намерена детайлна информация в интернет-източниците, без претенции за изчерпателност, беше направен анализ с акцент върху: броя на степените на съвместимост, броя и вида на оценяваните параметри, вида на оценката (количествена или качествена) и възможността за използване на математически методи за анализ на получената оценка. Характеристиките на някои от тях са поместени в табл. 1.

Таблица 1. Методологии за измерване и оценка на съвместимостта

Методология за измерване и оценка	Нива на съвместимост	Атрибути на съвместимостта
Спектър на оперативна съвместимост [5]	1,2,3,4,5,6,7	техническа съвместимост, възможност за управление и контрол
Оперативна съвместимост на военни комуникационни и информационни системи [1]	1,2,3	оперативни изисквания, данни стандарти, интерфейси, средства за моделиране
Нива на оперативна съвместимост на информационните системи [2]	0,1,2,3,4	процедури, приложения, инфраструктура, данни
Нива на концептуалната оперативна съвместимост [9]	0,1,2,3,4,6	комуникационни протоколи, синтаксис на данните, семантика на данните, методи и процедури за обмен на данните
Референтен модел за оперативна съвместимост на Техническата архитектура на НАТО [4]	1,2,3,4	подготвеност, разбиране, командване и координация, социално-културни фактори
Модел на зрялост на оперативната съвместимост [10]	1,2,3,4,5	доставка на услуги, потребление на услуги, посредничество за доставка на услуги, управление на услугите
Директива по съвместимостта на Алианса [6]	0,1,2,3,4	комуникационни протоколи, хардуер, данни
STANAG 5048 [7]	1,2,3,4, 5, 6	комуникационни протоколи, хардуер, данни
Модел на зрялост на информационните системи [8]	1,2,3,4,5	Данни, софтуер, комуникационни протоколи, хардуер

Анализът показва:

1. Наличие на голям брой методологии за оценяване, прилагани по едно и също време, в една и съща област (например в отбраната).

2. Много силно сходство в подхода за оценяване, който прилагат различните методологии, въпреки че са разработвани независимо една от друга:

2.1 Измерването на съвместимостта се състои в съпоставка и измерване на степента на сходство между характеристиките на множество от атрибути на съвместимостта с предварително дефинирани в еталонен модел стойности.

2.2. Степента на съответствие (респективно възможността за обмен на данни и информация) се оценяват според дискретна скала, чийто брой варирира за изследваните методологии между 3 и 7.

2.3. Използването на дискретната скала за оценка на съвместимостта, която се изменя плавно от абсолютна несъвместимост до абсолютна съвместимост намалява точността на оценката.

2.4. Оценката на съвместимостта е количествена, в повечето случаи е изразена чрез цяло положително число, което отговаря на номера, с който се идентифицира степента на зрялост на съвместимостта (таблица 1).

2.5. Обща слабост на изследваните методологии е липсата на сериозна възможност за задълбочен, основан на математически методи анализ на оценката.

2.6. Нито една от разгледаните методологии не отчита фактора „време“, при обмен на данните, въпреки че валидността на информацията често е функция на времето.

3. Определяне на броя и вида на оценяваните параметри, при определяне на степените на скалата за оценка, както и съвкупността от свойства (способности), които характеризират всяко ниво, се основават на експертна оценка на специалисти от областта, от което следват и установените различия между тях.

В резултат от анализа могат да се направят няколко препоръки в които биха довели до повишаване на ефективността на оценяването:

1. Времето за достъп до данните да се включи в списъка на оценяваните атрибути.
2. Алтернатива на дискретната скала за оценка да се потърси в средствата на размитите множества.
3. Да се потърси възможност за прилагане на математически средства при анализ на оценката.

Литература

1. Amanowicz, M. and Gajewski, P., “Military Communications and Information Systems Interoperability,” in Proceedings of the Military Communications Conference, 1996, pp. 280-283.

2. C4ISR Architecture Working Group, Levels of Information Systems Interoperability Reference Model, 30 March 1998

3. Ford T. C., Colombi J. M., Graham S. R., Jacques D. R., *A Survey on Interoperability Measurement*

4. Kasunic, M. and Anderson, W., "Measuring Systems Interoperability: Challenges and Opportunities," Carnegie-Mellon University—Software Engineering Institute, Pittsburgh, PA, Tech. Note CMU/SEI-2004-TN-003, Apr. 2004.
5. LaVean, G., "Interoperability in Defense Communications," *IEEE Transactions on Communications*, vol. COM-28, no. 9, Sep. 1980
6. NATO Policy for C3 Interoperability, AC/322-WP/72, 2000
7. STANAG 5048 - The Minimum Scale of Connectivity for Communications and Information Systems for NATO Land Forces, 2004
8. STEFANUS Van Staden, JAMESON Mbale, *The Information Systems Interoperability Maturity Model (ISIMM): Towards Standardizing Technical Interoperability and Assessment within Government Information Engineering and Electronic Business*, 2012, 5, 36-41 Published Online October 2012 in MECS (<http://www.mecs-press.org/>) DOI: 10.5815/ijieeb.2012.05.05
9. Tolk, A. and Muguira, J., "The Levels of Conceptual Interoperability Model," Proceedings of the 2003 Fall Simulation Interoperability Workshop, Orlando, FL, September 2003.
10. Interoperability Maturity Model, Guideline, публикуван на 8 февруари 2016, достъпно на адрес: <https://joinup.ec.europa.eu/elibrary/document/interoperability-maturity-model>, посетен на 12.07.2017 г.

М. Х. Ламбева,

МОДЕЛ НА СЪВМЕСТИМОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ

Милена Х. Ламбева

*гр. Шумен, ул. "Карел Шкорпил" 1, Национален военен университет "Васил Левски",
Факултет "Артилерия, противовъздушна отбрана и комуникационни
и информационни системи"*

INFORMATION SYSTEMS COMPATIBILITY MODEL

Milena H. Lambeva

Abstract: Information systems incompatibility problem is still up to date. Measuring, evaluating and analyzing the degree of compatibility is step forward. This report proposes a formal model of the compatibility assessment process.

Keywords: interoperability assessment, semantic compatibility, data model

Липсата на съвместимост между информационните системи отдавна е проблем във всяка област на човешката дейност, която е автоматизирана. Оценяването на нивото на съвместимост е задължителна стъпка в процеса на интеграция на системите. В този доклад е предложено формално описание на съвместимостта, посочени са недостатъците на съществуващите методологии за оценка и подход за преодоляването им.

ДЕФИНИЦИЯ ЗА СЪВМЕСТИМОСТ. НЕОБХОДИМОСТ И ПОДХОДИ ЗА ОЦЕНЯВАНЕ

За да работят съвместно две или повече информационни системи в името на обща цел, е необходимо да обменят информация и да използват обменената информация. Тази способност се нарича оперативна съвместимост. Пълната съвместимост е по-скоро цел, отколкото реално състояние на взаимодействащите системи. Постигането на задоволително състояние на свързаност е многоетапен процес на подобряване на способностите, много важна част от който е измерването и оценяването на текущото състояние.

Съществуват три подхода за оценяване на способността на системите за съвместна работа: експериментален, който е основан на резултатите от тестове върху реални системи, симулационен и теоретичен.

Теоретичният подход се основава на съпоставка и измерване на степента на сходство между модели на системите, отразяващи способностите им за съвместна работа. Той дава възможност да се оцени:

- способността на една система да се интегрира с други такива при определени условия, на всеки етап от жизнения ѝ цикъл.
- възможността на няколко системи да обменят пряко и задоволително информация и услуги по между си;
- възможността за повишаване на нивото на съвместимост между системите.

Оценяването на потенциалните способности за интеграция на система на етапа на проектиране оказва влияние на процеса на нейното изграждане. Теоретичната оценка на съвместимостта на съществуващи системи, подпомага вземането на решение за интеграцията им.

ТЕОРЕТИЧНО ОЦЕНЯВАНЕ НА СЪВМЕСТИМОСТТА

Оценката на съвместимостта е формален израз на способността на взаимодействията системи:

1. да обменят данни;
2. да интерпретират еднозначно обменените данни.

Тя е резултат от измерване и оценяване на определени характеристики на системите, съгласно утвърдена методология. За построяване на модел за теоретично оценяване на съвместимостта се решават следните задачи:

- избор на множество от системни параметри за оценка;
- назначаване на коефициент на относителна тежест на всеки параметър;
- формулиране на скала и критерии за оценка на степента на сходство;
- определяне на вида на оценката и формулата за нейното формиране;

Избор на параметри за оценка

Изборът на множеството от параметри за оценка се състои в това да се посочат параметрите, определящи възможността на системата да взаимодейства с други системи.

Факторите, които определят способността на системата да обменя данни и информация са много, и могат да бъдат класифицирани в следните групи:

- **хардуерна съвместимост:** определя се от съвместимостта между апаратните средства и протоколите за комуникация;

- **съвместимост на приложенията:** изразява се в способността на входно-изходните приложения да обменят данни по между си. Те зависят от съвместимостта между:

- алгоритмите в приложния софтуер, които обработват и представят информация на потребителя;

- използваните форми на документирано ръководство на разработване, внедряване и оперативен контрол на всяка от системите; стандартите за техническа и системна архитектура (хардуер, системен софтуер, комуникации, данни, приложения и др.)

- **съвместимост на данните в два аспекта:**

- семантичен – изразява се във възможността за еднозначна интерпретация на значението на данните;

- синтактичен – изразява се в сходството в размера и формата на данните.

Съвместимостта на една, или между две и повече системи е комплексна величина, която се определя от параметрите: техническа съвместимост, съвместимостта между входно-изходните модули и съвместимост данните.

Състоянието на съвместимост I^n между n на брой взаимодействащи си системи $S_1, S_2, \dots, S_n$ формално може да се опише:

$$(1) \quad I^n = \{ T^n_h, A^n_p, D^n \}, \text{ където}$$

T^n_h - техническа съвместимост между $S_1, S_2, \dots, S_n$;

A^n_p - съвместимостта на входно – изходните приложения, принадлежащи на $S_1, S_2, \dots, S_n$;

D^n - съвместимостта на данните, които обработват, съхраняват и предават $S_1, S_2, \dots, S_n$,

Следователно оценката на съвместимостта се определя от оценката на T^n_h, A^n_p и D^n .

Всяко от подмножествата на I^n съдържа различен брой елементи, следователно за оценяване на степените на съвместимост T^n_h, A^n_p и D^n се налага определяне на степента на сходство между голям брой параметри които ги определят.

Например за да се оцени съвместимостта по отношение на данните D^n между n информационни системи трябва да се сравнят моделите им на данни и да се определи сходството в:

- семантиката на данните – D_s ;
- формата на данните – D_f ;
- размера на данните – D_v .

$$(2) \quad D^n = \{ D_s, D_f, D_v \},$$

За формиране на комплексната оценка I^n се налага оценяване на много голям брой параметри, които се определят експертно в зависимост от особеностите на функционалната област, която обслужват информационните системи Това се потвърждава от анализ на част от съществуващите методологии за измерване и оценяване на съвместимостта, направен за целите на настоящата работа. По отношение на подхода им за теоретично определяне на степента на съвместимост бяха изследвани следните методологии, изброени в азбучен ред:

- Директива по съвместимостта на Алианса (NATO Policy for C3 Interoperability)[6] – дефинира три групи параметри за оценка: комуникационни протоколи, хардуер, данни;

- Модел на зрялост на информационните системи (Interoperability Maturity Model)[8] – категоризира оценяваните параметри в четири групи: данни, софтуер, комуникационни протоколи, хардуер;

- Модел на зрялост на оперативната съвместимост (Information Systems Interoperability Maturity Model)[10] – оценява четири групи параметри, касаещи съвместимостта на европейските обществени услуги: доставка на услуги, потребление на услуги, посредничество за доставка на услуги, управление на услугите;

- Нива на концептуалната оперативна съвместимост (Levels of Conceptual Interoperability Model)[9] – оценява комуникационните протоколи, и още четири атрибута, свързани с данните: синтаксис на данните, семантика на данните и процедури за обмен;

- Нива на оперативна съвместимост на информационните системи (Levels of Information Systems Interoperability Reference Model)[2] – определя четири атрибута на оперативната съвместимост - процедури, приложения, инфраструктура, данни ;

- Оперативна съвместимост на военни комуникации и информационни системи (Mil Comm. & Info Systems Interoperability)[1] – класифицира оценяваните параметри също в четири групи: оперативни изисквания, данни, стандарти, интерфейси, средства за моделиране;

- Референтен модел за оперативна съвместимост на Техническата архитектура на НАТО (NATO C3 Technical Architecture Reference Model for Interoperability (NMI))[3] – оценява: подготвеност, разбиране, командване и координация, социално-културни фактори;

- Стандартизационни споразумения на НАТО 5048 (STANAG 5048)[7] – оценява комуникационни протоколи, хардуер, данни;

Всеки от моделите дефинира собствен списък с параметри за оценка, разпределени в относително малък брой (три или четири) категории.

Избор на скала и критерии за оценка

Не по-малко сложен е въпросът с определяне на скала за оценка. Нейният вид също зависи от преценката на един или повече експерти.

Комплексната съвместимост, както и съвместимостта по отношение на отделните атрибути може приема много състояния. Освен двете крайни състояния - пълна липса на свързаност и пълна съвместимост съществуват и множество други характеризиращи се с различни способности на системите за обмен на данни, информация и знание.

Авторите на съществуващите методологии за теоретична оценка [1, 2, 3, 6, 7, 8, 9, 10] различават различен брой състояния (между три и седем), които подреждат в съответствие с нарастване на способностите за обмен и споделяне на информация и наричат „нива на съвместимост“. Някои методологии използват мярката за съвместимост – „степен“. Краен брой определени състояния, означени с цяло положително число формират скалата за оценка. Правилата за присъждане на ниво на съвместимост на една или няколко системи, в зависимост от нейните способности за свързване се определят експертно и се задават описателно в модела за оценка.

Задачата за ***създаване на модел за теоретично оценяване*** на съвместимостта на една система, или между група системи се отличава с голяма степен на субективизъм при:

- определяне на множеството на оценяваните атрибути;
- съставяне на скалата за оценка и критериите за принадлежност;
- определяне на относителни тегла на параметрите;
- формулиране на вида на комплексната оценка и формулата за формирането на комплексната оценка;

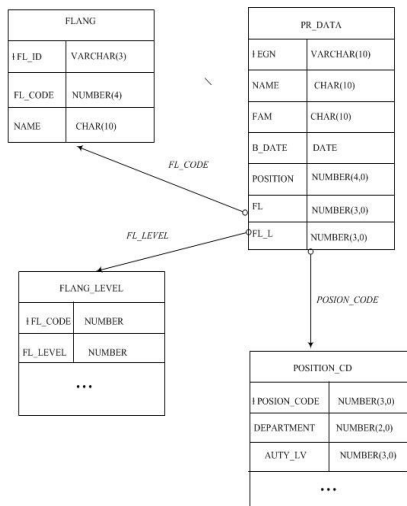
Качествата на модела (адекватност, пълнота и непротиворечивост) в значителна степен зависят от преценката на експерта, вземащ решение.

Задачата за ***теоретично оценяване*** на съвместимостта също значително зависи от мнението на експерта, както при тълкуване на критериите, така и при определянето на степента на сходство по всеки от показателите. Тя се характеризира и с

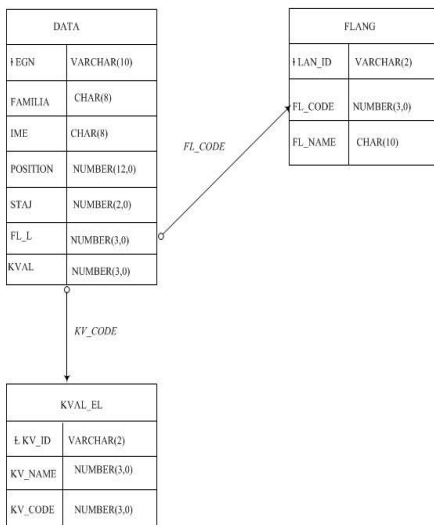
голямо количество входни данни, определящо се от броя на оценяваните параметри и броя на взаимодействащите системи.

Например за оценяване на две информационни системи по показателя „сходство на данните“ е необходимо да се извърши съпоставка на техните модели на данни, като се оценява сходството между полетата с данни и връзките между тях. Разбира се степен на сходство има смисъл да се търси между моделите на данните на системи, обслужващи една и функционална област.

На фигури 1 и 2 са показани извадки от физическите модели на данните на две информационни системи, в частта им касаеща администрирането на лични данни.



Фиг. 1. Физически модел на данни 1



Фиг. 2 Физически модел на данни 2

Таблица PR_DATA е основна таблица в Модел 1. Полетата в нея са следните:

- EGN – дава единния граждански код на лицето;
- NAME – име;
- FAM – фамилия;
- B_DATE – дата на раждане;
- POSITION – длъжност;
- FL – код на чуждия език, който владее лицето;
- FL_L – ниво на владееие на чужд език;

По кода на чуждия език от таблица FLANG се извлича чуждия език, а нивото на владееие се извлича от таблица FLANG_LEVEL.

Данните за заеманата от лицето позиция се извличат от таблица POSITION_CD по кода на позицията.

Основната таблица в Модел 2 е DATA. Тя съдържа основните данни за служителите:

- EGN – дава единния граждански код на лицето;

- FAMILIA – фамилията на служителя;
- IME – име;
- POSITION – заемана длъжност;
- STAJ – брой години стаж във фирмата;
- FL_L – ниво на владеење на чужд език;
- KVAL – квалификация.

Данните за квалификацията се извличат от таблицата KVAL_EL, а данните за нивото на владеење на чужд език от таблицата FLANG.

Таблица 1. Семантично съответствие на полетата в основните таблици на физическите модели

Значение	Наименование на поле в таблица PR_DATA	Наименование на поле в таблица DATA
EGH	EGN(VARCHAR 10)	EGN(VARCHAR 10)
Име	NAME(CHAR 10)	IME(CHAR 8)
Фамилия	FAM(CHAR 10)	FAMILIA(CHAR 8)
Дата на раждане	B_DATE	-----
Заемана длъжност	POSITION(NUMBER4,0)	POSITION(NUMBER12,0)
Чужд език	FL	-----
Ниво на владеење	FL_L(NUMBER 3,0)	FL_L(NUMBER 3,0)
Стаж	-----	STAJ
квалификация	-----	KVAL

Съпоставката на моделите се изразява в следното:

1. Сравняват се наименованията на полетата в двете основни таблици и се търси семантично съответствие между тях. Както показва таблица 1 съществуват четири двойки полета, чиито наименования имат едно и също значение и четири полета, които нямат аналог. Определя се D2s.

2. Извършва се структурна съпоставка на двойките полета с еднакво семантично значение и се оценява степента на съответствие на типа на данните – D2t.

3. Сравнява се размера на данните на онези двойки полета, които имат еднакво значение и сходна структура. Оценява се сходството в размера им - Dv.

4. Определя набор от допускания и правила за преобразуване на типа и размера на данните с еднакво семантично значение, с оглед структурата им да се сведе до една и съща, без да се губи информация. Формира се комплексна оценка Dn.

Всички дейности за изпълнение на стъпките от 1 до 4 се изпълняват от експерт или група експерти (по метода на експертната оценка). Решенията в голяма степен зависят от нивото на познаване на предметната област и моделите на данните на оценяваните системи и професионалните умения на експерта за работа с бази от данни.

Недостатъци на съществуващите методологии за оценка на съвместимостта могат да се обобщят:

1. Допускат висока степен на субективност при оценяване на отделните показатели.

2. Дават количествена оценка на съвместимостта, която по своята природа е качество.

3. Използват дискретна скала за оценка, която не съответства на реалната възможност съвместимостта на една информационна система (или между информационни системи) да се изменя плавно от абсолютна несъвместимост до абсолютна съвместимост.

Възможност за тяхното преодоляване може да се намери в използването на средствата на размитата логика за моделиране на съвместимостта на информационните системи, и построяване на модел на приближени разсъждения (каквито са разсъжденията на експерта), който да се използва в компютърна система.

Литература:

1. Amanowicz, M. and Gajewski, P., "Military Communications and Information Systems Interoperability," in Proceedings of the Military Communications Conference, 1996, pp. 280-283.

2. C4ISR Architecture Working Group, Levels of Information Systems Interoperability Reference Model, 30 March 1998

3. Kasunic, M. and Anderson, W., "Measuring Systems Interoperability: Challenges and Opportunities," Carnegie-Mellon University—Software Engineering Institute, Pittsburgh, PA, Tech. Note CMU/SEI-2004-TN-003, Apr. 2004.

4. NATO Policy for C3 Interoperability, AC/322-WP/72, 2000

5. STANAG 5048 - The Minimum Scale of Connectivity for Communications and Information Systems for NATO Land Forces, 2004

6. STEFANUS Van Staden, JAMESON Mbale, The Information Systems Interoperability Maturity Model (ISIMM): Towards Standardizing Technical Interoperability and Assessment within Government Information Engineering and Electronic Business, 2012, 5, 36-41 Published Online October 2012 in MECS (<http://www.mecs-press.org/>) DOI: 10.5815/ijieeb.2012.05.05

7. Tolk, A. and Muguira, J., "The Levels of Conceptual Interoperability Model," Proceedings of the 2003 Fall Simulation Interoperability Workshop, Orlando, FL, September 2003.

8. Interoperability Maturity Model, Guideline, публикуван на 8 февруари 2016, достъпно на адрес: <https://joinup.ec.europa.eu/elibrary/document/interoperability-maturity-model>, посетен на 12.07.2017 г.

М. Х. Ламбева,

РАЗМИТ МОДЕЛ ЗА ОЦЕНЯВАНЕ НА ОПЕРАТИВНАТА СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

Милена Х. Ламбева

*гр. Шумен, ул. "Карел Шкорпил" 1, Национален военен университет "Васил Левски",
Факултет "Артилерия, противовъздушна отбрана и комуникационни
и информационни системи"*

FUZZY MODEL OF INFORMATION SYSTEMS INTEROPERABILITY ASSESSMENT

Milena H. Lambeva

Abstract: *Measuring and evaluating compatibility between information systems is an important step in improving it. This report offers an algorithmic approach and automated implementation of the evaluation process through fuzzy logic capabilities.*

Keywords: *information systems, interoperability assessment, fuzzy logic, linguistic variable*

Проблемът с липсата на съвместимост между системите не е нов, и остава актуален в отговор на съвременните тенденции към повсеместна свързаност. Причините за неговото съществуване непрекъснато еволюират: бързо се увеличава числеността и разнородността на информационните системи, нараства необходимостта от споделяне на данни и услуги. Усилената цифровизация и интензивно развитие на информационните технологии водят до задълбочаване на различията между информационните системи по отношение на технологичните принципи за тяхното изграждане.

Известни са редица теоретични изследвания, целящи разрешаването на проблема с несъвместимостта. Съществуват и множество практически реализации, базирани на разнообразни подходи, методи и инструменти. Общото между тях е, че изтъкват необходимостта от ясна представа за реалната, необходимата и възможната степен на съвместимост. За да бъде подобрена, съвместимостта първо трябва да бъде измерена.

Най-многобройни са изследванията на възможностите за измерване, оценяване и анализ на съвместимостта, провеждане за нуждите на отбраната, предимно в рамките на Алианса. Голяма част от усилията са насочени към експерименталното измерване и симулацията. Разработени са много тестове за измерване на реалната способност. Най-малко са проучени възможностите за теоретично оценяване.

Теоретичната оценка на съвместимостта на една, или между няколко информационни системи, е не по-малко ценна от получената посредством симулация или провеждане на тестове в реална работна среда. Нейно предимство е възможността да се оценят потенциалните способности на една система за свързване с други системи, и възможността за обмен на данни между две и повече системи, единствено

вено на базата на техни описания – *модели на съвместимостта*, без да се налага те да са реално развърнати и да функционират.

СЪЩНОСТ НА ТЕОРЕТИЧНОТО ОЦЕНЯВАНЕ НА СЪВМЕСТИ- МОСТТА МЕЖДУ ИНФОРМАЦИОННИТЕ СИСТЕМИ

Оценката на съвместимостта е формален израз на способността две или повече информационни системи да обменят данни и информация и да използват обменените данни и информация. Теоретичната оценка е резултат от съпоставка и измерване на сходството между избрани техни характеристики.

Преди да се реализира съпоставката е необходимо създаване на модел за теоретично оценяване. Задачата за построяване на модел за теоретична оценка се решава експертно, с отчитане на особеностите на функционалната област, която обслужват информационните системи. Съществува висока степен на субективност при вземане на решение, обусловено от компетентността и познаването на експертната област от страна на експерта при:

- избор на множество от системни параметри за оценка;
- назначаване на коефициент на относителна тежест на всеки параметър;
- формулиране на скала и критерии за оценка на степента на сходство;
- определяне на вида на оценката и формулата за нейното формиране;
- определяне на стъпките на процеса на измерване и оценяване.

За създаване на списък от параметри за оценка, от всички параметри на системите се избират само онези, които определят способността им да приемат и предават данни от и към други системи, и да ги интерпретират по един и същ начин.

Съвместимостта между системите се определя от: съвместимостта между апаратните средства, протоколите за комуникация, стандартите за техническа и системна архитектура, способността на входно - изходните приложения да обменят данни по между си, сходството в семантиката, размера и формата на данните. Факторите са много и могат да бъдат класифицирани в три основни групи: техническа съвместимост, съвместимост на входно–изходните приложения, съвместимост на данните.

Следователно оценката на състоянието на съвместимост (фигура 1) I между n на брой взаимодействащи си системи $S_1, S_2, \dots, S_n$ се определя от множеството:

(1) $R(I) = \{R(T), R(A), R(D)\}$, където:

$R(T)$ – оценка на техническата съвместимост между $S_1, S_2, \dots, S_n$;

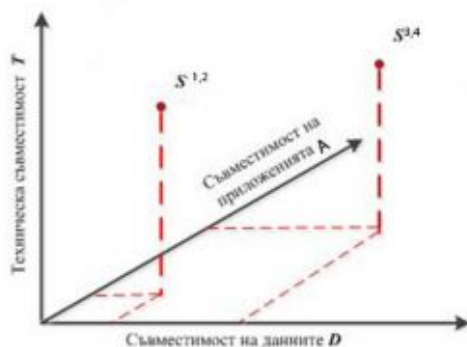
$R(A)$ – оценка на съвместимостта на входно – изходните приложения, принадлежащи на $S_1, S_2, \dots, S_n$;

$R(D)$ – оценка на съвместимостта на данните, които обработват, съхраняват и предават $S_1, S_2, \dots, S_n$.

Избор на скала и критерии за оценка

Трябва да се въведе единна мярка за оценките $R(T)$, $R(A)$ и $R(D)$, която да отразява степента на близост между оценяваните параметри. Повечето познати методологии използват мярката „степен“ или „ниво“ на съвместимост. Скалата за оценка подрежда степените на съвместимост в съответствие с нарастване на способностите за обмен и споделяне на информация. Съществуващите методоло-

гии използват дискретни скали от краен брой нива, които са числови или лингвистични.



Фиг. 1. Графично представяне на съвместимостта между системи

Процес на измерване и оценяване

Всяка от оценките $R(T)$, $R(A)$ и $R(D)$ е комплексна и се формира от оценките на множество параметри. Например степента на съвместимост на данните D^n се определя от:

- D_s – степен на семантично съответствие;
- D_t – степен на съответствие във формата на данните;
- D_v – степен на съответствие в размера на данните.

(2) $D = \{ D_s, D_t, D_v \},$

Оценката (2) е резултат от специфичен познавателен процес, имащ за задача посредством сравняване на моделите на данните, да се оцени възможността на полета от модела на данни на една система, и връзките между тях, да бъдат съпоставени полета от модел на данни на друга система. Изпълнението на всеки етап от този процес е свързан с вземане на решение относно съществуването и степента на съответствие между:

1. значението на наименованията на полетата на данните, касаещи една и съща функционална област. Оценката D_s^n е израз на отношението между броя семантично еднакви полета, към всички полета от данни.
2. структурата на данните с еднакво семантично значение. Оценката на съответствие на типа на данните – D_t^n може да варира от „напълно еднаква структура“ до „несъпоставими типове данни“.
3. размера на данните с еднакво значение и структура, която може да се сведе до еднаква – D_v^n .

На всеки етап оценката се формира експертно, и в голяма степен зависи от квалификацията и познаването на предметната област от експерта. В пълна сила това е валидно и за формирането на оценките T^n и A^n .

Може да се направи заключението, че задачата за теоретично измерване и оценяване на съвместимостта между информационни системи се характеризира с:

- многоразмерност, определена от голямото количество данни, които трябва да бъдат анализирани;
- нееднозначност на решението като следствие от субективността, както при тълкуване на критериите за оценка, така и при вземане на решение за (при определяне на степента на сходство по определени показатели)

Според изследване, направено от Томас Форт и др.[2], значителна част от съществуващите методологии не почиват на математически методи за измерване и анализ на оценката. Формулираната оценка е качествена и няма числен израз. Повишаване на ефективността на процеса на оценяване е възможно посредством автоматизираното му компютърно изпълнение и математически анализ на резултатите от измерването.

Възможни са два подхода:

- следване на количествен подход при оценяване. Използване на възможностите на класическата математика (теория на вероятностите, математическа оптимизация, теория на изчислителната сложност, линейно програмиране, нелинейна оптимизация, теория на графите, теория на сложността);
- формиране на качествена оценка, каквато е практиката. Използване на методите на размитата логика за формализация на задачата за оценяване на степента на съвместимост между две и повече системи, с оглед последваща компютърна реализация.

РАЗМИТ МОДЕЛ НА СЪВМЕСТИМОСТТА НА ДВЕ ИНФОРМАЦИОННИ СИСТЕМИ

Теорията на размитите множества[1,3] дава възможност да се формализира процеса на вземане на решение относно степента на сходство в характеристиките на оценяваните модели на системите, който в голяма степен се основава на субективната оценка на експерта.

Моделиране на входните данни

Оценяваните системи се представят с крайно, непразно, дискретно множество $S = \{S^1, S^2, \dots, S^n\}$.

Входни данни са данните за архитектурата на оценяваните системи, получени от техни описания. За всяка система S , те се дефинират от наредената тройка $S = \langle T, A, D \rangle$, където:

$T = \{t_1, t_2, \dots, t_m\}$ - крайно, непразно, дискретно множество от експертно избрани технически параметри, свързани със способността за свързване с други системи;

$D = \{d_s, d_a, d_v\}$ - множество от експертно избрани параметри, характеризиращи съвместимостта на данните;

$A = \{a_1, a_2, \dots, a_p\}$ - крайно, непразно, дискретно множество от експертно избрани параметри, характеризиращи способността на входно-изходните приложения да обменят данни.

Елементите $e_i, e \in \{t, a, d\}$ могат да са от различен тип. Могат да са лингвистични или числови данни от различен тип: целочислен, реален или булев (например: елементът t_m , описващ „системата притежава възможност за свързване пос-

редством WI-FI“ може да приема стойност „0“ – „не притежава“, или „1“ – „притежава“).

С цел да се опрости задачата за целите на примера се въвежда ограничението $n=2$.

Моделиране на оценката

Оценката (1) на съвместимостта между две системи S^i и S^j , $i, j \leq n$, $i \neq j$ се определя от:

$$R(T^n) = \min \{ r(t_1^{ij}), r(t_2^{ij}), r(t_3^{ij}), \dots, r(t_k^{ij}), \dots, r(t_m^{ij}) \}$$

$$(3) \quad R(A^n) = \min \{ r(a_1^{ij}), r(a_2^{ij}), \dots, r(a_L^{ij}), \dots, r(a_p^{ij}) \}$$

$$R(D^n) = \min \{ r(d_s^{ij}), r(d_t^{ij}), r(d_v^{ij}) \}$$

Всяко $r(t_k^{ij})$, $k = [1, m]$, $r(a_L^{ij})$, $L = [1, p]$, и $r(d_s^{ij})$, $r(d_t^{ij})$, $r(d_v^{ij})$ е качествена оценка на степента на сходство между съответните показатели: например $r(t_k^{ij})$ е оценката на съвместимостта на системите S^i и S^j по k – тия технически показател, и може да приема някоя от стойностите: много ниска степен, ниска степен, средна степен, висока степен, много висока степен, дефинирани в размита лингвистична скала за оценка. Скалата за оценка е една и съща за всички $r(t_k^{ij})$ и R , и се формулира експертно.

Моделиране на процеса на оценяване:

1. За всяка от системите S^i и S^j се определят множествата:

$$T^i = \{ t_1^i, t_2^i, t_3^i, \dots, t_k^i, \dots, t_m^i \}$$

$$A^i = \{ a_1^i, a_2^i, \dots, a_L^i, \dots, a_p^i \}$$

$$D^i = \{ d_s^i, d_t^i, d_v^i \}$$

$$T^j = \{ t_1^j, t_2^j, t_3^j, \dots, t_k^j, \dots, t_m^j \}$$

$$A^j = \{ a_1^j, a_2^j, \dots, a_L^j, \dots, a_p^j \}$$

$$D^j = \{ d_s^j, d_t^j, d_v^j \}$$

2. По предварително дефинирани правила се извършва се съпоставка на всяка двойка от елементи e_k^i и e_k^j . Формира се дискретна числена оценка на степента на сходство $o(e_k^{ij})$, $o(e_k^{ij}) = [0\%, 100\%]$, в затворения интервал между 0% (пълна несъвместимост) и 100% (пълна съвместимост). Изборът на правила за съпоставка и критерии за определяне на оценката е експертен и зависи от естеството на съпоставяните параметри.

3. На всяка числена оценка $o(e_k^{ij})$ се съпоставя лингвистична променлива [4], зададена по следния начин:

$$\beta = \langle \text{степен на } r(e_k^{ij}) \rangle;$$

$$T = \langle \text{много ниска, ниска, средна, висока, много висока} \rangle$$

$$X = \langle 0\%, 100\% \rangle;$$

$$G = \{ \text{„или“} \};$$

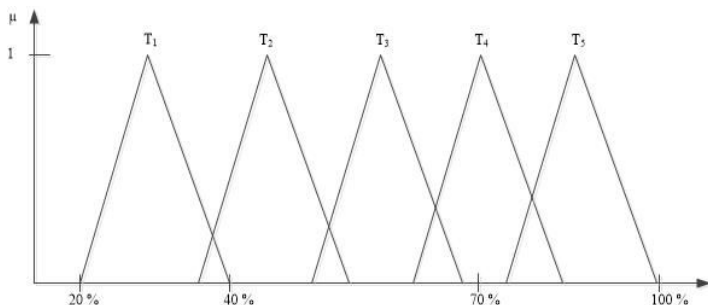
$$M = \{ \min \}.$$

Съгласно множеството G , допустими са терми от вида „много ниска или ниска“, „висока или много висока“ и др., получени от елементите на терм - множеството с помощта на логическата връзка „или“. Съгласно M , преобразуването на

терми от вида „висока или много висока” в размита променлива става с помощта на операцията $\min$ на Заде.

Графичният вид на примерна функция на принадлежност към термите е показана на фигура 2.

4. Определят се оценките (3).
5. Формира се комплексната оценка (1).



Фиг. 2. Функция на принадлежност към термите: $T_1 = \{\text{много ниска}\}$, $T_2 = \{\text{ниска}\}$, $T_3 = \{\text{средна}\}$, $T_4 = \{\text{висока}\}$, $T_5 = \{\text{много висока}\}$

Изводи:

1. Предложеният метод за определяне на степента на съвместимост между две и повече информационни системи е удобен за алгоритмизация и програмна реализация.
2. Съществено за адекватността на модела е определянето на: списък на оценяваните параметри, правила за съпоставка, критерии за формиране на оценка и вида на ФП, което се извършва чрез обработка на експертно мнение.

Литература:

1. Василева М., Размити множества. Теория и практика, Шумен, 2008 г.
2. Ford T. C., Colombi J. M., Graham S. R., Jacques D. R., A Survey on Interoperability Measurement, Twelfth International Command and Control Research and Technology Symposium (12th ICCRTS), 19-21 June 2007, Newport, RI
3. Zadeh L. A. Outline of a New Approach to the Analysis of Complex Systems and Decision Processes. IEEE Transactoin on System, Man and Cybernetics, 1973
4. Zadeh L .A. The concept of a Linguistic Variable and its Applications to Approximate Reasoning. Information Sciences, 8, 9,1975

D. I. Dimitrov, D. A. Atanasov,

IMPLEMENTATION OF THE HOUGH TRANSFORM IN DETECTION OF TARGET TRAJECTORY

**Dilyan Ivanov Dimitrov
Deyan Atanasov Atanasov**

NATIONAL MILITARY UNIVERSITY "VASIL LEVSKI"
"ARTILLERY, AIR DEFENSE AND CIS" FACULTY
SHUMEN, 1 KAREL SHKORPIL STR

Abstract: *The article considers target detection method for radar signals on the basis of target trajectory detection using the Hough transform (HT). It is explained the principals of the transform, its advantages and an example of detection algorithm.*

Keywords: *Hough transform, radar signals, detection algorithm*

1. Introduction

It is typical for radars that target detection is realized consecutively with the help of predefined threshold for every element of resolution capability. In that method there are two basic problems with detection of weak signals. For the first one, after making decision of a target presence the information from the element is not used and the task for detection is solved for the next element. Moreover, the wrong taken decision of a target absence in the element of resolution capability leads to losses of information. For the second problem, if it is used a power accumulation of reflected signal of the target, it is supposed that the target does not leave the element of resolution capability during the whole time of accumulation which does not always execute for high speed targets and it takes to decreasing the probability of detection.

Hough transform allows overcoming both of the problems. For the first time it was used for solving the detection problems described in the work of Carlson, Evans and Wilson [1]. The feature of this method is along with detecting targets to estimate their trajectory parameters. That it's realized between coverage information accumulation where can be hold signals from weak undetectable targets. Then to the accumulated information is used HT which is forming peaks in parameter space. Analyzing these peaks, we can take decision of a target presence or absence.

2. Hough transform

The Hough transform was first introduced by Paul Hough in 1961 as a method of detecting complex patterns in binary image processing. It achieves this by determining specific values of parameters which characterize these patterns. The HT converts a difficult global detection problem in image space into a more easily solved local peak detection problem in a parameter space. The key idea behind the HT can be illustrated by considering sets of collinear points in an image. A set of image points (x, y) , which lie on a straight line, can be defined by a relation f , such that

$$f((a, b), (x, y)) = y - ax - b = 0 \quad (1)$$

Where a and b are two parameters, the slope and intercept, which characterize the line. It can be drawn infinite number of straight lines through (x_i, y_i) point which satisfy the equation $y_i = ax_i + b$ in different values of a and b [3]. Now let's look at plane (a, b) , called parameter space and rewrite the equation of the straight line as $b = -x_i a + y_i$. It appeared that in this plane a particular pair (x_i, y_i) corresponds to some kind of straight line. Another point (x_j, y_j) corresponds to another straight line and both of them intersect in a point (a', b') , where a' is a slope and b' - intercept point where y-axis and the straight line crosses both points (x_i, y_i) and (x_j, y_j) . In general, every point of this line in parameter space corresponds to a straight line where every each of them intersects in the point (a', b') (figure 1).

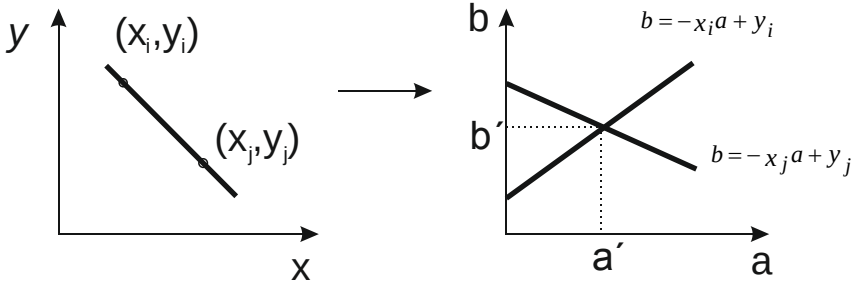


Figure 1. Explanations for the Hough Transform

It is suggested that straight lines might be usefully parameterized by the length ρ , and the orientation θ , of the normal vector to the line from the image origin given as

$$\rho = x \cos(\theta) + y \sin(\theta). \quad (2)$$

This has distinct advantage over the (b, a) parameterization which has a singularity for lines with large slopes, i.e. $a \rightarrow \infty$. Using the (ρ, θ) parameters means that image points map into sinusoidal curves in a two parameter space. Assigning values for θ , it can obtain ρ values.

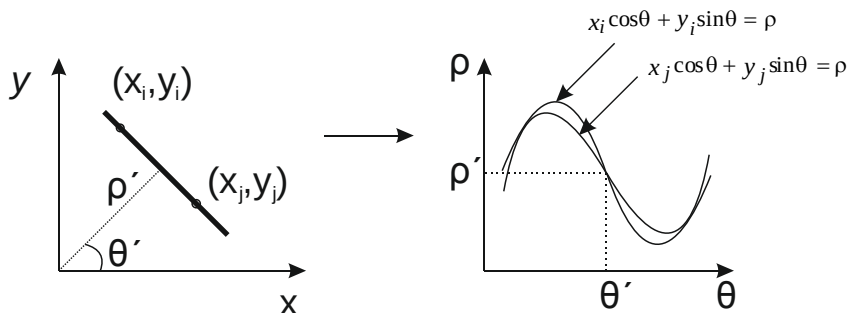


Figure 2. Hough transformation in option $(\rho-\theta)$ of the parameterization

As in the case with (a,b) parameters through every point can pass multiple lines with different ρ and θ . Furthermore, for each point (x,y) of the image corresponds multitude plane points (ρ, θ) .

After transforming (2) it can be set as:

$$\rho = \sqrt{x^2 + y^2} \sin\left(\theta + \arctg \frac{x}{y}\right) \quad (3)$$

where the conclusion can be made that a curve in (ρ, θ) space is sinusoid and its amplitude and phase depends on the values of x and y .

The Hough transform implements like this. A sampling is realized in the parameter space (ρ, θ) as a result of this a regular grid of cells $\Delta\rho \times \Delta\theta$ is made. Each cell is assigned a counter. The number of all counters is called accumulator. After that a body forms with values of parameter θ : $\theta_n = n\pi/\Delta\theta, n=1, \dots, N_\theta$. For each i -point of the space a sinusoid is made $\rho_{i,n} = x_i \cos \theta_n + y_i \sin \theta_n$.

Separation of the lines is based on this, each cell of the parameter space (ρ_0, θ_0) corresponds to number of points of the measuring space lying on line $\rho_0 = x \cos(\theta_0) + y \sin(\theta_0)$. Each point belonging to this line gets to its cell and increases the value of the counter with a unit of measurement. Points corresponding to the noises of the images are even distributed in the (ρ, θ) space. After the end of the transform the values of the counter of each cell correspond to number of points lying on relevant line. As a result it can be chosen a predetermined number of maximum long curves or separate all which exceed a particular threshold.

So, the classical HT algorithm is consisting of the following steps:

- choice of sampling cells;
- filling up the accumulator;
- searching of maximums;
- separating lines corresponding of the maximums; as parameters of the line are taken the coordinates of the center of the cell.

The main problem in implementation of Hough transform is the choice of sampling parameters. Here the following problems are possible. If the grid is chosen very small

and at the exit number of points there is a noise, then a point of a curve can get into different cells of the grid. This means that the potential maximum of the accumulator corresponding on that curve would be eroded – it would be very difficult or impossible to locate. Besides, the smaller the sampling step, the higher is volume of calculations. On the contrary, if the grid is chosen too large, the probability that one point will contain points lying on different curves, as well as noise points will increase. With any sample grid, if the points form a straight line with a parameter lying on the cell boundary, because of the observation noise, the points of this curve will fall into neighboring cells, which will lead to a blur of the peak in the accumulator.

Practical application of the classical Hough transform is hampered by the high complexity of the algorithm both in time and in memory, since in each cycle it is necessary to process the results of not only current but also non-maximal previous reviews (HT – block algorithm). Therefore it is not surprising that most of the improvements in the method are aimed at its acceleration, while the other part realizes the expansion of its functionality. Among the most common modifications noted:

- *Generalized HT* - Intended for the allocation of shapes of any shape;
- *Combinatorial HT* - Used to highlight straight lines, it calculates the parameters of two-point line segments (possible preliminary division of the image into small areas);
- *Probabilistic HT* - Where HT is carried out only for a part of the so-called control points of the original image ($0 \leq \alpha \leq 100\%$), chosen randomly with uniform probability.
- *Hierarchical HT* - Where the original image is divided into regular segments, for each of which HT are executed, the lines of each four neighboring squares are combined, etc. Until it is out of stock;
- *Adaptive HT* - Using an accumulator of initially small size, which is then iteratively pre-engineered to achieve a specified accuracy in that part of the parameter space where the maximum is detected (i.e., the desired curve);
- *Randomized HT* - Where the pair of points of the original image through which the line is drawn is randomly iteratively selected; the counter corresponding to this straight line increases.

3. Use of the Hough transform in search radar

The uncertainty of the origin of the mark, the presence of noise and possible observation of several moving objects are characteristic for the problem of trajectory detection. The properties of the Hough transform allow using it as a robust and effective algorithm for detecting a trajectory that implements the selection from a set of binary two-dimensional points of parametrically specified lines corresponding to the trajectory of the radar target. Theoretically, it is possible to find a line of random shape, however, in practice, trajectory tracking of the trajectory in the detection interval is usually considered as a straight line. The algorithm for finding a trajectory with the help of HT refers to the block class, because in it the observations of several recent surveys are processed together.

The use of HT to isolate the trajectory was proposed in Smith and Winter article [2], and a full-scale synthesis and analysis of the trajectory of the radar target on its basis was carried out in a series of three papers by Carlson, Evans and Wilson [1]. Here, the trajectory detection statistics were obtained for the use of the HT method, and it was also

shown that the selection of the HT grid to be too small leads to the separation of the trajectory points into several cells, while it is too large - to the addition of noise points to the cells with the points of the trajectory.

The algorithm for detecting trajectories based on Hough transform is realized as follows [4]:

- 1) The sample θ is sampled to N_θ cells, the cell center is defined as

$$\theta_n = \left(n - \frac{1}{2} \right) \Delta\theta, n = 1, \dots, N_\theta \quad (4)$$

- 2) Accumulated marks obtained on the last N review:

$$Z_1^N = \left\{ z_i^k \right\}_{i=1, m_k}^{k=1, N} \quad (5)$$

- 3) For each i -th mark and the value of parameter θ_n , the values of parameter $\rho_i(\theta_n)$ are calculated according to the formula:

$$\rho_i(\theta_n) = x_i \cos \theta_n + y_i \sin \theta_n \quad (6)$$

- 4) A division of the definition domain of parameter ρ into N_ρ cells is made, the cell center is defined as

$$\rho_n = \left(n - \frac{1}{2} \right) \Delta\rho, n = 1, \dots, N_\rho \quad (7)$$

where $\Delta\rho = (\rho_{\max} - \rho_{\min}) / N_\rho$.

- 5) It checks the hit of each received value $\rho_i(\theta_n)$ in one or another cell in the parameter space, after which the value of the corresponding cell of the accumulator is increased by one.

- 6) The maximum value in the accumulator is looked for, it is compared with the threshold, according to the comparison results a decision is made to detect or not to detect the trajectory.

- 7) To the determined trajectories, an estimation of the parameters $\rho_t(\theta_t)$ corresponding to the center of the cell is carried out.

- 8) The sliding window moves one clock forward (marks from the first view are discarded; markings from the new scan are added instead).

The algorithm for detecting a trajectory based on HT has a number of significant advantages:

- It can be used for parallel detection of several new trajectories simultaneously, which allows it to be matched directly with identifying algorithms, for example, Joint Probabilistic Data Association (JPDA) and Multiple Hypothesis Tracking (MHT).
- It is stable in relation to both the change in the distribution of false marks, and the omission of marks from the target.

- The resulting estimate of the trajectory is also a good approximation of the original trajectory, i.e. in addition to detecting the trajectory, filtration problems are also solved.
- There is the possibility of specifying the nomenclature of the laws of motion of the target, which makes it possible to detect the trajectory of objects that not only move along a straight line, but also make a known maneuver.

Due to these advantages, the method of detecting trajectories based on HT finds application in the presence of a large number of targets and a complicated interference background.

However, along with obvious advantages, this algorithm has no less significant drawbacks. As already noted, due to the presence of measurement errors, it is possible to bring the converted measurement to the neighboring cells of the accumulator. For a large cell of the parameter space, a large number of false measurements can enter it.

Fig. 3 illustrates the problems that arise when a trajectory is detected using the Hough transform. Figure 3, *a* shows the situation in which there are no errors in radar measurements, as well as false marks (but there are omissions). The intersection point of the sinusoids in the parameter space is easily identifiable. In the presence of measurement errors and false marks (Fig. 3, *b*), the results of the transformation will be scattered between the accumulators. As a result, estimating the cell of the parameter space with the maximum value of the counter can turn out to be wrong, which reduces the accuracy of the estimation of its parameters and the probability of a correct detection of the trajectory until it is illegally dropped and increases the probability of detecting a false trajectory. If the accumulator size is too small, the maximum will spread over several cells and the trajectory will not be detected.

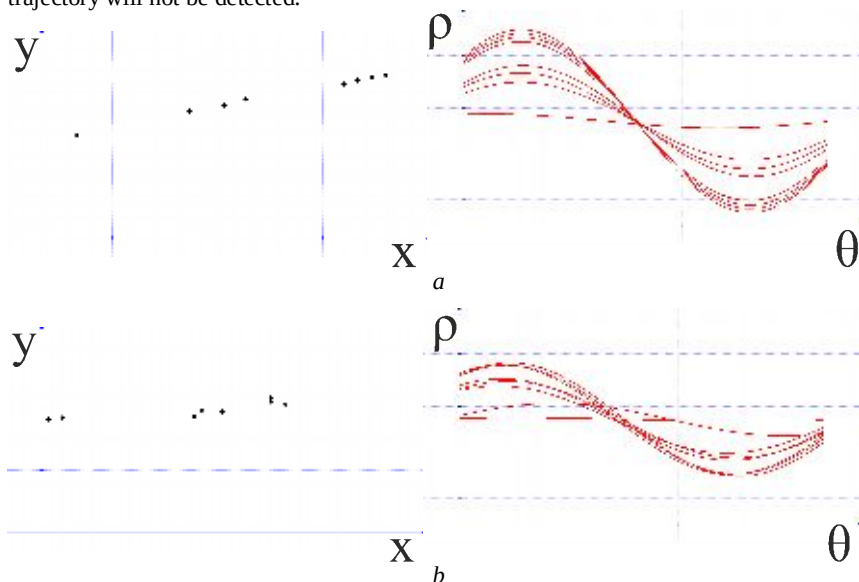


Figure 3. Example of detection of a trajectory based on the HT

Also can be noted that the HT perceives a set of initial data as a one-time static picture obtained, information about the arrival time of the marks in it is lost. As a result, a situation may arise where false marks that are far from the true position of the target in their receipt (gating does not completely prevent such a situation) are accumulated on the position of the target in subsequent scans, thereby distorting the result of the assessment.

Thus, in the implementation of classical HT, the choice of the size of the accumulator and the value of the threshold becomes important.

An additional source of error is the need to use an accumulator. The matter is that, due to the sampling of the parameter space, the final result of the transformation is reduced to the center of the cell. Even if there are no noises, the conversion yields an accurate result only if the true value of the trajectory parameters will fully correspond to the center of the cell. Otherwise, errors will occur. The maximum error will be observed when the value of the parameters is exactly in the middle between the centers.

Hough transform was originally intended for the processing of digital images, which are characterized by the sampling of the observation space, so the sampling of the parameter space is essential. Meanwhile, in radiolocation, the initial sampling of the observation space is absent, since the measured coordinates of the target take values from the continuum. Therefore, it is possible to refuse to use the accumulator and the losses associated with it.

There is a version of the algorithm for detecting the trajectory based on the HT, which checks whether N of the taken measurements in N consecutive scans can represent the trajectory of the target. Here, after calculating the values of $\rho_i(\theta_n)$, the average values of $\bar{\rho}(\theta_n)$ for each θ_n are calculated:

$$\bar{\rho}(\theta_n) = \frac{1}{N} \sum_{i=1}^N \rho_i(\theta_n) = \bar{x}_i \cos \theta_n + \bar{y}_i \sin \theta_n \quad (8)$$

where $\bar{x}_i = \sum_{i=1}^N x_i$, $\bar{y}_i = \sum_{i=1}^N y_i$. Then the maximum deviation of ρ from the average value for each $\theta_n, n=1, \dots, N_\theta$ is sought:

$$\Delta\rho(\theta_n) = \max \left\{ \rho_i(\theta_n) - \bar{\rho}(\theta_n) \right\} \quad (9)$$

after that, the minimum value is searched among $\Delta\rho(\theta_n)$:

$$\Delta\rho = \min \Delta\rho(\theta_n)$$

A new trajectory is considered to be detected if obtained value of $\Delta\rho$ does not exceed some predetermined threshold value of γ_0 .

This algorithm can detect only one trajectory and has no filtering ability. It should consider all sets of N marks on N consecutive strobes, which potentially can correspond to a trajectory. The mark on each subsequent review is selected taking into account the gating by speed, i.e. from the number of accumulated only those marks are selected that can belong to targets moving at speeds in the range of $v_{\min} \dots v_{\max}$.

$$v_{\min} \leq \left| \frac{Z_i - Z_{i-1}}{t_i - t_{i-1}} \right| \leq v_{\max} \quad (10)$$

4. Conclusions

Summarizing the analysis of the algorithm for trajectory detection based on the Hough transform, we note that it poses much more problems to the developers of real systems than the traditional methods. First of all, it concerns the optimal and the prognostic value of the counter. However, the intensity of research in this direction gives hope for their solution in the foreseeable future.

The detection of the trajectory by means of the Hough transform is used as an independent algorithm, and is also often realized as a component of the identification-tracking algorithms, such as MHT, JPDA, Track Before Detect (TBD), responsible for trajectory detection and estimation of the number of objects in the group target. There are also variants of algorithms for trajectory detection on the basis of HT, pre-existing for multi-position radar systems.

References

1. **Carson, B.D. and E. Evans, S. Wilson.** *Search Radar Detection and Track with the Hough Transform. I.* s.l. : IEEE Transactions on Aerospace and Electronics System, 1994, Vol. 3.
2. **Smith, M.C. and Winter, E.M.** *On the detection of target trajectories in a multi-target environment..* s.l. : IEEE Conf. on Decision and Control, 1978.
3. **Семёнов, А.Н.** *Обнаружение радиолокационных целей с помощью преобразования Хафа.* №12, с.609-619, Москва, Россия : Наука и Образование МГТУ им. Н.Э. Баумана, 2014 г.
4. **Коновалов, А.А.** *Основы траекторной обработки радиолокационной информации часть 1.* Санкт-Петербург : Издательство СПбГЭТУ "ЛЭТИ", 2013. 918-5-7629-1449-9.

CORRELATION-PULSE METHOD FOR INCREASING THE SENSITIVITY OF THE PROXIMITY RADAR RECEIVER

Matey K. Kirov, Ivan A. Iliev

National Military University "Vasil Levski", Faculty „Artillery, Air defense and Communication and information system“, Shumen, Bulgaria

Abstract: The proximity radars are widely used in modern radar systems to provide radar information required for taking off and landing of aircrafts. The noise stability depends on the signal-to-noise ratio at receiver output. This article provides a method for reducing the noise level in the receiver, justifies the method and theoretical estimates of its capabilities.

Keywords: proximity radar, noise stability, signal-to-noise ratio

Formulation of the task

Figure 1 presents a schematic diagram of a standard radar detector [1]. Ultra-high frequency (UHF) carrier with frequency oscillation f_0 is transmitted through the transmitting antenna A_1 . The reflected signal with frequency $(f_0 \pm f_D)$ from the receiving antenna A_2 enters at the mixer input from the receiving device. At the other input of the mixer a signal arrives from the transmitter and after transformation a signal is formed with a frequency equal to f_D . After gain in a Low Frequency Amplifier (LFA), the signal enters the indicator equipment.

The presence of noises in the receiver is determined by: the noise that make the mixing diodes, the fluctuations of the amplitude of the UHF oscillations of the generator, and the noise from the amplifier [1].

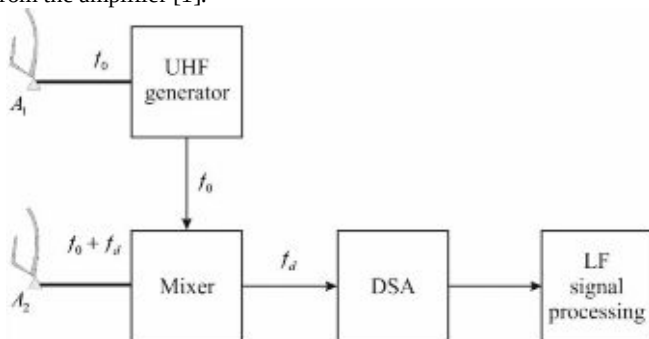


Figure 1

The noises from the generator get into the receiver in two ways [1]. The first one – they get into directly with the UHF fluctuations coming from the mixer heterodyne. These noises are suppressed at 15-20 dB using a balanced mixer. The other way is by penetrating the transmitted oscillation from the transmitting antenna in the receiving antenna because of their poor separation. This oscillation spreads through the useful signal way and therefore its amplitude fluctuations are not suppressed by the balanced mixer.

In the noise energy spectrum of receiver $S(f)$ there are two areas - low-frequency and high-frequency. In the low-frequency area, also called the flicker area, the spectral density of the noise is inversely proportional to frequency $S(f) = \frac{1}{f}$, and for the high frequencies the spectrum is steady. The frequency f_H for which the intensities of the flicker and the steady components are equal is the frequency of the spectrum bending in the proximity detectors of UHF $f_C > 100 \text{ kHz}$. The Doppler signal amplifier cuts the part of the spectrum falling into its bandwidth $f_C \leq f \leq f_B$, the width of which depends on the detector's assignment.

Typical of the Doppler Proximity Detector (DPD) is that the Doppler amplifier bandwidth is located in the low frequency band where the flicker noise is. The correlation function of flicker noise decreases slowly by logarithmic law [2], which determines the large correlation interval. In addition, the flicker noise, unlike the delta-correlated white noise, which has a steady spectrum, is related to the conductance of the semiconductor, that modulates the current and do not depend on it.

These two features of the flicker noise are at the base of the proposed method for increasing the sensitivity of the DPD receiver.

The essence of the correlation-pulse method is the following:

1) Two periodic sequences of shifting pulses are created $\Phi_1(t)$ and $\Phi_2(t)$. The duration of the pulses τ_1 and τ_2 as well as the time intervals between them t_{p1} and t_{p2} are related to the period of the sequence of pulses T in the following relation: $\tau_1 + t_{p1} + \tau_2 + t_{p2} = T$. We apply $\tau_1 = \tau_2 = \tau$ and $t_{p1} = t_{p2} = t_p$. The period T , the frequency of change f_C and the upper frequency of the Doppler spectrum f_B are related in the following relation: $\frac{1}{T} \gg f_B$ and $f_B < f_C$.

2) For every time interval τ_1 when the receiving antenna is switched off and imitation of incomplete separation between the two antennas at the mixer outlet, a noise voltage is formed. The imitation is made of a special high frequency circuit. It is assumed that the imitation of division is accurate. A signal with a Doppler frequency over time interval τ_1 is absent. This process can be presented in the form of a periodic sequence of meander pulses modulated by the noise $\delta U_1(t)$ of the generator that would be obtained with a switched on antenna:

$$(2) \quad u_1(t) = \delta U_1(t) \cdot \Phi_1(t) ;$$

$\Phi_1(t) = \sum_{k=-\infty}^{+\infty} \varphi_1(t - k.T)$, where $\varphi_1(t) = \begin{cases} 1, & 3a \ 0 < t \leq T \\ 0, & 3a \ t \leq 0, t > T \end{cases}$ is function describing the pulses form.

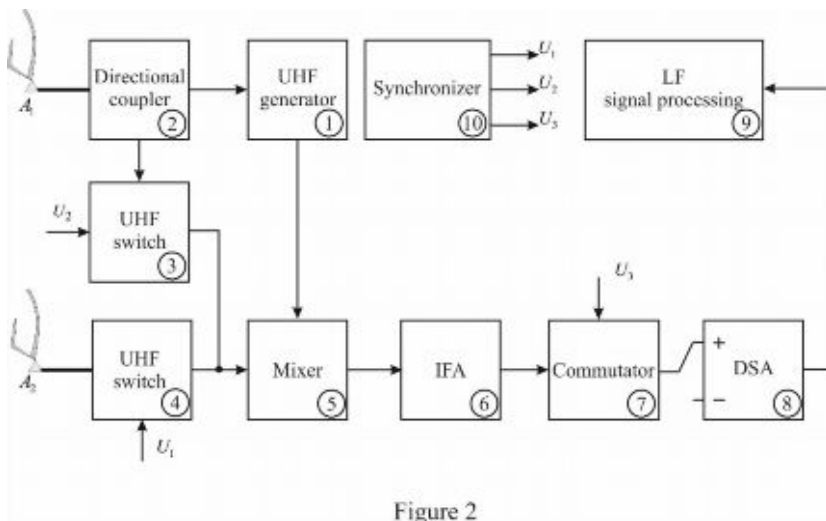


Figure 2

3) For each time interval τ_2 the mixer is connected to the receiving antenna and a signal is received at its output in accordance with the expression:

$$(2) \quad u_2(t) = [V_d(t) + \delta U_1(t)] \Phi_2(t);$$

$\Phi_2(t) = \Phi_1(t - t_u - \tau)$ where $V_d(t)$ is the desired signal reflected by the target.

The output voltage of the intermediate frequency amplifier (IFA) is the sum of the voltages $u_1(t)$ and $u_2(t)$ and the continuous noises $\delta U(t)$ of the mixer and the IFA.

$$(3) \quad u(t) = u_1(t) + u_2(t) + \delta U(t)$$

4) Signal pulse processes are formed from signal $u(t)$

$$(4) \quad u_-(t) = u(t) \cdot \Phi_1(t)$$

And Doppler signal + noise:

$$(5) \quad u_+(t) = u(t) \cdot \Phi_2(t)$$

The Doppler signal + noise $u_+(t)$ subtract the noise $u_-(t)$ and the resulting signal $n(t) = u_+(t) - u_-(t)$ does not contain flicker noises. The structural scheme of the device that implements the proposed algorithm is presented in Fig. 2. The periodic switching of the operating modes is performed in the following order: the switch 4 does not pass the signal from the receiving antenna A_2 to the mixer input 5 and the UHF switch 3 is open. This key switches the mimic signal coming from the directional coupler 2. The switch 7 is in the (-) position to form the noise voltage.

The signal + noise are formed in the following state of the circuit: the UHF switch 4 is open, the UHF switch 3 is closed and the switch 7 is in the position (+). The control of the keys is carried out by the synchronizer 10, the control voltages U_1 , U_2 and U_b of which go to the UHF switches 4 and 3 and the switch 7.

The own noises of modern low-noise UHF switches are considerably smaller than the mixer noises and can be ignored. To reduce the input of own noises from the low frequency switch 7 and to reduce the noise of the elements as a whole, a low-noise IFA 6 is placed between the mixer 5 and the switch 7. The periodic impulses $u_+(t)$ and $u_-(t)$ formed at the output of the switch 7 are received at the corresponding inputs of the Doppler Signal Amplifier 8. This is a Differential Amplifier with bandwidth $f_C \leq f \leq f_B$ which includes a subtraction device and an integrator for forming the output signal $n(t) = u_+(t) - u_-(t)$.

Thus, at the output of the Doppler Signal Amplifier, there is the useful signal against the background noise. From the DSA output, the signal enters the device 9 for processing the low-frequency Doppler signal.

It is assumed that the IFA bandwidth is $\Delta f_{IFA} \gg \frac{1}{T}$, PFC (phase-frequency characteristic) is linear and the pulses pass through the IFA without distortion. It is assumed that the operation of the UHF switches 3 and 4 and the switch 7 is strictly synchronized and the useful signal is absent, i.e. $V_d(t) = 0$. In this case it is considered that the voltages $u_+(t)$ and $u_-(t)$ are obtained after the modulation with $\Phi_1(t)$ and $\Phi_2(t)$ of the resultant continuous noise $U(t) = \delta U_1(t) + \delta U(t)$, where $\delta U_1(t)$ is the noise of the generator, and $\delta U(t)$ is the noise of the mixer and the IFA. The transform of continuous noise into pulsed noise leads to a change in its energy spectrum.

The detector noise resistance is determined by the ratio of average signal power to average noise power [2]. The noise suppressed index is the ratio of the average noise power in an ordinary DPD to the DPD noise power, realized according to the proposed method. The average power of the suppressed noise in the DSA bandwidth

$$\text{is } P_n = \int_{-t}^t G_{DSA}(f) df.$$

The noise suppressed index is:

$$(6) \quad K = \frac{P_0}{Q^2 P_n},$$

where $P_0 = \int_{-t}^t S(f) df$ is the average noise power in the DPD bandwidth operating in continuous mode.

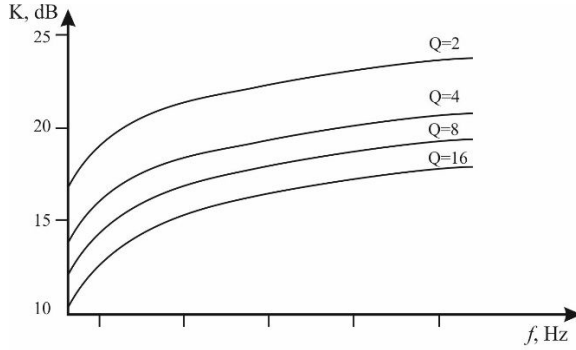


Figure 3

The noise suppressed index depends on the pulse rate $F_R = \frac{1}{T_R}$, the fill factor Q , the frequency of change f_C in the noise spectrum, the bandwidth of the IFA and the DSA. Figure 3 shows the dependence of the suppressed index on the pulse rate at the frequency of change in the spectrum $f_C = 100\text{KHz}$ and the different fill factor Q values. The graph refers to the DPD with the bandwidth of the IFA $\Delta f = 100\text{KHz}$. When the pulse rate F_R increases the suppressed index, which is explained by a reduction in the contribution of the composite noise components associated with the pulse rate harmonics $\Delta S(f)$. Gradually the rate of growth decreases and endeavors to saturation due to the increase in the contribution of the combined noises associated with the steady noise in the spectrum $S(f)$. The suppressed index is maximal at the fill factor $Q = 2$, in which there are no even harmonics to pulse rate, and the odd meanings are minimal. It is best to work with the fill factor $Q = 2$ and pulse rate transcendent the frequency of change f_C .

Figure 4 shows the relationship of the suppressed index of the frequency change spectrum noise on the pulse rate $F_R = 100\text{KHz}$ and the bandwidth of the DSA $\Delta f_{DSA} = 10 - 200\text{Hz}$. The increase of the index when f_C increases, is explained by the decreasing of the contribution of the composite components from the steady noise.

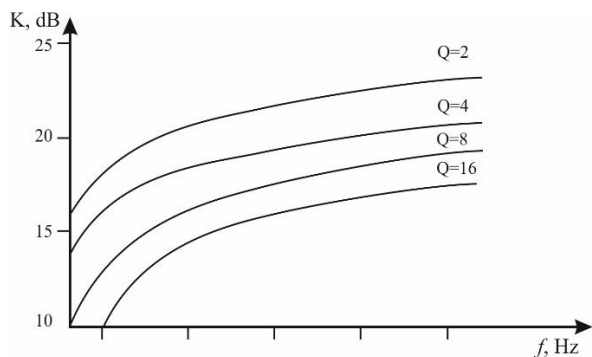


Figure 4

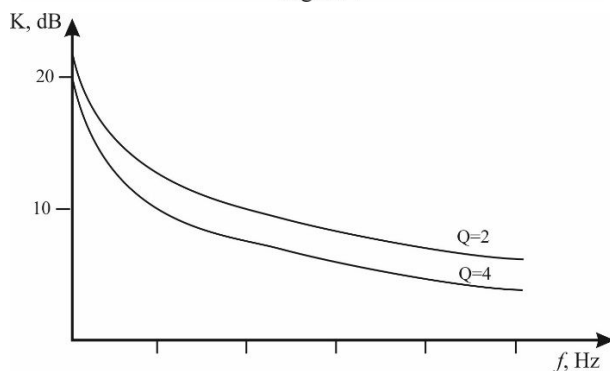


Figure 5

Figure 5 shows the relationship of the suppressed index on the upper frequency of the bandwidth of the DSA f_B at a fixed lower frequency $f_C = 10\text{Hz}$. The decreasing of the suppressed index at an increase of f_C is explained by an increase in the contribution of the combining components with frequency approaching $f = \frac{f_B}{2}$.

Conclusions

The suggested correlation-pulse method for suppressing the flicker noise can be used to increase the sensitivity of Doppler systems for proximity radars, the useful signal bandwidth in which does not exceed several tens of kilo hertz.

References

1. Merrill I. Skolnik „Radar handbook” – 2008
2. Mahafza Bassem R „Radar Systems Analysis and Design Using MatLab” – 2000
3. Финкельштейн М.Н. „Основы радиолокации” - М.: Сов. радио, 1973

В. Т. Стоянова, Н. Ж. Кулев,

АНАЛИЗ НА ПОКАЗАТЕЛИТЕ ЗА КАЧЕСТВОТО В СТЕГАНОГРАФИЯТА С ИЗОБРАЖЕНИЯ

**Веселка Т. Стоянова
Николай Ж. Кулев**

*НВУ „Васил Левски“, Факултет „Артилерия, ПВО и КИС“,
гр. Шумен, ул. „Карел Шкорпил“ 1, veselka_tr@abv.bg,
mobile +359 896 785 902*

ANALYSIS OF QUALITY INDICATORS FOR STEGANOGRAPHY IMAGE

**Veselka T. Stoyanova, PhD
Nikolai Kulev, PhD**

*National Military University, Faculty of Artillery, AAD and KIS,
1 Karel Shkorpil Str., 9700 Shumen, Bulgaria, veselka_tr@abv.bg*

Abstract: *The main goal of hiding data is to conceal the very existence of the hidden information, therefore there is a significant demand for steganographic approaches that can ensure imperceptibility of such information. However, there is a limited corresponding evaluation parameters available. Most of the studies use the Peak Signal to Noise Ratio (PSNR) as a metric for imperceptibility evaluation, although it could provide less accurate results than the Human Visual System (HVS) evaluation. This paper provides a review of the existent evaluation metrics that are used to assess the quality of steganography. The examination of the correlation between the existing objective and subjective metrics is also conducted. Pixel differences metrics have a poor correlation with the subjective metrics, hence the HSV based metrics have better correlation than pixel metrics.*

Keywords: *steganography, PSNR, HVS, UQI*

1. Въведение

Скриването на данни се превърна в ключов въпрос в областта на информационната сигурност. Стеганографията е наука за скриване на информация в рамките на друга цифрова без да буди подозрение в стегоанализатора. Стего файлът трябва да бъде идентичен със прикриващия файл. Успехът на всяка стеганографска система зависи от три основни фактора, които са: незабележими, недоловими и капацитет. Скрытата информация не трябва да предизвиква съмнение за наблюдателя, който следи за скрито съобщение в образа на носителя. Това може да доведе до шум в носителя, обаче той трябва да остане невидим и неоткриваем от всички статични средства или човешката визуална система. Ето защо, недоловимата скри-

та информация е важен аспект, за да се развива всеки стенографски подход. Следователно недоловимия стего файл е от съществено значение за повечето подходи, които се занимават с изображение или видео стеганография. Най-точен и надежден начин за определяне на визуалното качество на такива стего файлове е човешката визуална оценка (субективна оценка). Въпреки това, този вид оценка, отнема време и не може да бъде част от автоматична система. Поради тези причини през последните години са разработени много обективни показатели за оценка, които могат да работят по същия начин, както на основния процес на човешкото възприятие. Най-простият и най-широко използван параметър за оценка на качеството е Mean Squared Error (MSE, средноквадратична грешка), изчислява се чрез осредняване на квадратни изменения концентрирани в прикриващото и стего изображението. Освен това в отношение на размера на шума към сигнала Peak Signal to-Noise Ratio (PSNR), MSE и PSNR са атрактивни параметри, тъй като са статистически подходящи от гледна точка на оптимизирането. PSNR измерва математическите разлики между скритото изображение и стего изображението и не вземат под внимание характеристиката на човешката визуална система Human visual system (HVS). Следователно, те имат слаба корелация с качеството на възприемане от човешката визуална система (HVS) според Wang и сътр. [4, 5].

2. Изложение

Оценки за качеството на изображението може да се класифицират като обективна и субективна оценка. Обективната оценка оценява качеството на изображението на базата математически алгоритми. Субективната оценка оценява качеството на изображението въз основа на човешкото зрение, способности и характеристика. Обективните показатели за оценка на базата на математически процес за измерване на недоловимото между оригиналния файл и стего файла.

2.1. Pixel Differences Measurements

Mean Square Error (MSE): Нарушаването на изображението се изчислява чрез осредняване на квадратична интензивност на скрито изображение и получените стего пиксели на изображението като

$$(1) \quad MSE = \frac{1}{m \times n} \sum_{i=1}^{m-1} \sum_{j=1}^{n-1} [C(i, j) - S(i, j)]^2,$$

където i, j са сумата на разликите за грешки между оригиналното и стего изображението, C е оригиналното изображение, S е стего изображението.

2.2. Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR): Изчислява съотношението на полезния сигнал към шума за скрито изображение със стего изображението, както е дадено в (2), където MAX е стойността на максималния брой на пикселите от изображението, скритите и стего изображения, които трябва да са с еднакъв размер и тип. Повисоката стойност PSNR сочи по-високо качество и съответствие между двата входни изображения.

$$PSNR = 10 \cdot \log_{10} \left(\frac{I_{max}^2}{MSE} \right) \quad (2)$$

2.3. Weighted Peak Signal to Noise Ratio

Weighted Peak Signal to Noise Ratio (wPSNR): е качествен показател разработен от Voloshynovskiy и сътр., които основно на базата на стойността на Noise Visibility Function (NVF) като коефициент за корекция, който е класифициран в изображението въз основа на текстурирана и периферната зона, както вграждането на данните в тази област може да се скрие в данните ефективно с малко смущения.

2.4. Human Visual Based Measurement

HVS е друг важен фактор за измерване на недоливимото между скрито и стего изображение. Основната идея е, че хората се занимават с различни характеристики на конкретни изображения, които включват ориентация, контраста, яркост, текстура и т.н. Скритото изображение и стего изображението трябва да се трансформира в честотен домейн с помощта Discrete Wavelet Transform (DWT) или Discrete Fourier Transform (DFT). След това, Contrast Sensitivity Function (CSF) се използва за скриване в стего изображения. След CSF се използват филтри с различни техники, които могат да бъдат използвани за изчисляване на качеството на изображението. Освен това се използват различни HVS модели за изчисляване на качеството на изображението. В действителност, HVS качествените показатели са най-близки до показателите на субективните измервания.

2.5. Universal Image Quality Index.

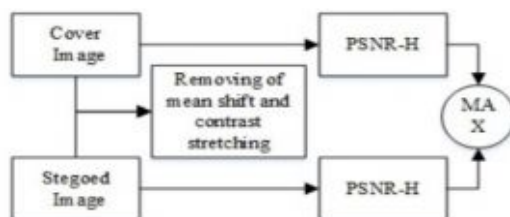
Universal Image Quality Index (UQI): Индекс за универсално измерване на качеството на изображението между две входящи изображения[3]. Този подход се основава на конфигуриране на три фактора, които са яркост- изкривяване, контрастно изкривяване и структурни сравнения. Въпреки този индекс е математически дефиниран без да се отчита HVS, експериментални резултати показват, че от него се разкрива невероятна надеждност със субективна оценка за качество. UQI е по-ефективна оценка на качеството в сравнение с MSE и PSNR.

2.6. Structural Similarity Index.

Structural Similarity Index (SSIM): През 2004 г. Wang и неговият екип разработили SSIM [6]. SSIM измерва качеството на изображението на базата на оригиналния образ, който е без изкривяване. SSIM индексните възприемат грешки, които означават, че изкривяването на изображението е в промяната на структурната информация. Оценката се основава на пикселите, които са взаимосвързани особено когато тези пиксели са пространствено близо.

2.7. PSNR-HVS

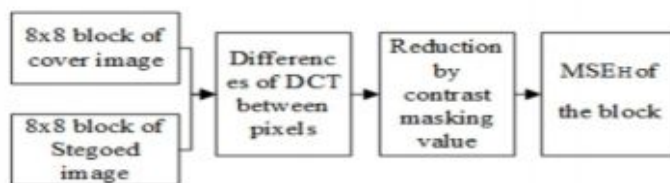
Според Egiazarian и др. в [1] е представен адаптивен качествен показател на PSNR, като се вземат предвид HVS. Основава се на средна стойност на изместване и контрастно разширяване, използвайки прозорец за сканиране, както е показано на фигура 1.



Фиг.1. Сравняване стего и прикриващо изображение

2.8.PSNR-HVS-M

Според [2], този показател е създаден с цел да повиши ефективността на PSNR и MSE. Разделя входното изображение в 8×8 припокриващи блокове чрез прилагане на DCT като $\delta(i, j)$. След това, разликите в $\delta(i, j)$ за скритото и стего изображението се пренасят в блоковете с помощта на Contrast Sensitivity Function (CSF). Фигура 2 показва основната блок-схема за PSNR-HVS-M.



Фиг.2. Блок схема на PSNR-HVS-M

2.9. Субективна оценка

Субективното качество на стего изображенията се оценява чрез осреднен резултат. Резултата е описан в [7], качеството на изображение е оценено по скала от 1 до 5, като след това се нормализират до 1. Difference Mean Opinion Score (DMOS) се изчислява и се нормализира до сравнение с обективните показатели за качество. Изисква се да се изясни кое изображение е прикриващо и кое е стего изображение. Оценяват се на базата на MOS рейтинг, който може да бъде от отлично (5) до лошо (1), както е посочено в таблица 1.

Табл. 1. MOS рейтинг

MOS	Quality	Impairment
5	Excellent	Unnoticeable
4	Good	Noticeable but not irritating
3	Fair	Slightly irritating
2	Poor	Irritating
1	Bad	Very irritating

Разликите са нулеви в случай на препращане на изображението, отстранено е за допълнителна обработка, превръщат се в Z-резултати [8]. Получените Z-резултати се мащабират от $[0,1]$, за да се създаде подходящ модел за оценка. DMOS

може да се изчисли като средната стойност на всички тествани Z- резултати за конкретно изображение.

2.10. Корелационен анализ

За да се анализира връзката между субективна оценка и PSNR, експериментът включва скриване на едно и също тайно съобщение в червена, зелена и синия компонента на пикселите на изображенията Lenna and Pepper с помощта на LSB (least significant bit) метода. Стойността PSNR за вграждане на същата червена, зелена и синия компонента на пикселите в стего изображения е подобен на Lenna and Pepper изображението, както е показано в таблица 2. Стего изображенията са разгледани от човешки очи, сравнено е качеството на оригиналното изображение за всеко стего изображение. Проверката е извършена, за да се направи оценка на всеко стего изображение с помощта на 10 наблюдателя. На фигура 3 и 4 са представени, най-близко до оригиналното стего изображение, а именно това с вграждането на данните в синия цветови канал. Лошо стего изображение е получено с вграждането на данните в зеления цветови канал. Тази оценка позволява да се решава въз основа на чувствителността на човешкото зрение, човешките очи са по-чувствителни към зелен цвят и по-малко чувствителни към син цвят.

Табл. 2. Стойности на PSNR

Color	PSNR (Lenna)	PSNR (Pepper)
Red	45.3087	44.8547
Green	45.3057	44.8658
Blue	45.3158	44.8789

В допълнение, обективни и субективни оценки за качеството на изображениянето са нормализирани, за да представят сравнение. Фигура 3 и 4 показват резултатите от качеството на изображението (Lenna and Pepper), съответно разликата показана в MOS е средна оценка. Тъй като нараства с увеличаването и се изкривява, докато другите показатели имат противоположно поведение.



Фиг. 3



Фиг. 4

Обективните качествени показатели, които се ръководят от функциите HVS имат по-добра корелация със субективна оценка в сравнение със стандартните MSE и PSNR. Индексът за универсално качество на изображението е показал най-висока корелация с субективна оценка, благодарение на способността си да откри-

ва яркост – изкривяване, а загубата на корелацията на скрити и стего изображения е оценката UQI.

Табл. 4. Качествени показатели

Quality Assessment Metric	Processing Time (second)
PSNR	0.2548
PSNR-HVS	11.6482
PSNR-HVS-M	11.9854
SSIM	0.3845
UQI	0.2578

3. Заключение

Сравнителното изследване на съществуващите показатели за качеството на изображението се извършва за стеганографични изображения. Оценката за качеството на изображението използва обективни качествени показатели в областта на стеганографията е сравнен със субективната оценка, извършена от 10 наблюдатели. Установено е, че избраните обективни показатели имат слаба корелация, а субективната оценка може да не успее да даде точна оценка за изпълнението на алгоритъм за стеганография. HVS базирани показатели имат по-добра корелация спрямо стандартните пиксели на база показателите като MSE и PSNR, това показва ефективността на използването на функциите на HVS в показателите за оценка на качеството.

References:

1. Karen Egiazarian, Jaakko Astola, Nikolay Ponomarenko, Vladimir Lukin, Federica Battisti, and Marco Carli. A new full-reference quality metrics based on hvs. In CD-ROM proceedings of the second international workshop on video processing and quality metrics, pages 2–5, 2006.
2. Nikolay Ponomarenko, Flavia Silvestri, Karen Egiazaria, Carli Marco, Jaakko Astola, and Vladimir Lukin. On between-coefficient contrast masking of DCT basis functions. CD-ROM Proc. of the Third International Workshop on Video Processing and Quality Metrics, 4(1):1– 4, 2007.
3. Zhou Wang and Alan Bovik. A universal image quality index. Signal Processing Letters, 4:81– 84, 2002.
4. Zhou Wang, Hamid R. Sheikh, and Alan C. Bovik. Objective video quality assessment. The handbook of video databases: design and applications, 2003.
5. Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, and Eero P. Simoncelli. Image Quality Assessment: From Error Visibility to Structural Similarity. Image Processing, IEEE Transactions, 13(600-612), 2004. [6] Zhou Wang, Eero P. Simoncelli, and Alan C. Bovik. Multiscale structural similarity for image quality assessment. In Conference Record of the Thirty-Seventh Asilomar Conference on, Signals, Systems and Computers,, pages 1398 – 1402 Vol.2, 2004.
7. Raniyah Abdullah Wazirali, Zenon Chaczko, and Anup Kale. Digital multimedia archiving based on optimization steganography system.
8. Sviatoslav Voloshynovskiy, Alexander Herrigel, Nazanin Baumgaertner, and Thierry Pun. A stochastic approach to content adaptive digital image watermarking. In Information Hiding, pages 211–236, 2000

Д. Т. Дойчинов,

МЕРКИ ЗА ЗАЩИТА НА УЕБ ПРИЛОЖЕНИЯ ОТ АТАКИ

Димитър Т. Дойчинов

гр. Шумен, ул Карел Шкорпил 1

MEASURES FOR PROTECTION OF WEB APPLICATIONS

Dimitar T. Doychinov

Abstract: The purpose of this paper is to make a review of most distributed attacks against web application and suggest some measures for protection.

Keywords: web-attacks, injection, cross-site scripting, web-security.

Увод

В днешно време ключово значение за сигурността на конфиденциалните данни е проектирането и използването на различни методи и техники за защита на използваните системи. Потенциален достъп до поверителните данни на компанията може да се получи дори през браузър. Съществуват множество стандарти за безопасност (PCI DSS, NIST и др.), международни критерии (ISO/IEC 27005:2011, ITIL, COBIT и др.) и законодателните норми. Сигурността на web - приложенията трябва да се залага в етапа на тяхното проектиране и реализиране, а не в последствие.

В изследване на Open Web Application Security Project (OWASP) в областта на уеб сигурността са посочени десетте най-разпространени заплахи за 2017 г. [1].

A1 – ИНЖЕКТИРАНЕ. Проява на SQL инжектиране е, когато непроверени данни се изпращат на приложението като част от команда или заявка. Във форма за заявка се подава параметър, който освен информацията, съдържа и допълнителен SQL код.

LDAP Injection е техника, използвана за атака на уеб сайтове, които конструират LDAP търсене от входни данни от потребителите. Сигурното уеб приложение да проверява данните, подадени от потребителя преди да конструира заявката за търсене. Уязвимото приложение не филтрира подходящо входните данни и дава възможност за инжектиране на код от страна на атакуващия. [{L_08]

Предотвратяване и избягване на атаки с SQL инжекция

Стъпки, които организацията може да предприеме:

- ограничаване на привилегиите за достъп на потребителите: на служителите и потребителите се предоставя достъп до информация, само от която се нуждаят за да изпълняване на своите задачи;
- бдителност на потребителите по отношение на сигурността: разработчици на уеб сайта познават заплахите от SQL инжекции и добрите практики, с които да обезопасяват сървърите.

- ограничаване на информацията, извеждана от софтуера на уеб сървъра при наличие на грешка.
- тестване на уеб приложението дали е податливо на атака с SQL инжекция.

A2 – Нарушен процес на автентифициране и управление на сесиите. Неправилното използване на функциите на приложението, свързани с идентифициране и управление на сесиите, позволява на атакуващите да компрометират пароли, ключове или сесийни идентификатори, с цел придобиване идентичността на други потребители.

Предотвратяване

Внимателното и правилното използване на механизмите за проверка на автентичността на потребителя и за управление на сесията значително намаляват вероятността за възникване на проблем в тази област. Добра първа стъпка е дефинирането в политиката за сигурност как ще се управляват пълномощията на потребителите. Изпълнението на тази е ключово за наличието на надежден и стабилен механизъм за удостоверяване и управление на сесията. Някои от най-важните елементи са:

- силни пароли – към пароли трябва да има изисквания за сложност, да се променят периодично и да не се допуска повторно използване на стари пароли;
- използване на паролата – ограничаване на броя опити за въвеждане на парола, многократните неуспешни опити за влизане трябва да се регистрират. Потребителите трябва да бъдат информирани за датата / часа на последното си успешно влизане и на броя на неуспешните опити за достъп до профила си;
- механизъм за смяна на паролата – при смяна на паролата потребителите за са длъжни да предоставят старата парола, както и други данни от профила си.
- съхранение на паролите – всички пароли трябва да се съхраняват и хеширана или криптирана форма, за да ги предпази от компрометиране, независимо от това къде те се съхраняват.
- защита на пълномощията при пренос – единствената ефективна техника е да криптира целия трафик.
- кеширане в браузера – данните за удостоверяване и сесия не трябва да бъдат представени като част от GET метод, трябва да се използва.

Управление на потребителските акаунти:

- проверка за неактивни акаунти;
- да не се използват общоизвестни потребителски акаунти;
- да не се използват вградени администраторски акаунти;
- използвайте различни администраторски акаунти и пароли за всеки сървър.

Управление на сигурността на сървъра:

- ограничаване на достъпа само до администраторите;
- автентикация на всички нива.
- използване на одитни записи и логови файлове. За предпочитане е логовите файлове да се пазят на отделен сървър.

A3 – Вмъкване на нежелан код (Cross-Site Scripting /XSS/). Възниква когато приложението изпраща непроверени данни за изпълнение към брауъра на потребителя. XSS позволява на атакуващите да изпълнят код в брауъра на потребителя, следствията от което са отвлечане на потребителската сесия, промяна вида на уеб сайта или пренасочване на потребителя към сайт с вредоносно съдържание. Тези пробиви обикновено се дължат на липсата на проверка на входните данни на приложението, постъпващи чрез уеб форми или параметри в клиентските заявки.

XSS атаките се делят на три основни вида:

- Non-persistent (Reflected) – възможна е при сайтове, в които входни данни, предоставени от уеб клиента се визуализират директно в брауъра. При този тип инжектираният скрипт се връща от уеб сървъра под формата на съобщение за грешка, резултат от търсене или друг отговор, включващ част или целите входни данни, подадени като заявка. Атаката може да се осъществи и чрез изпращането на специално подготвена връзка, (по e-mail например), маскирана да изглежда като нормална препратка към сайт. Тъй като потребителят има доверие на сайта, той отваря връзката и става жертва на атаката.
- Persistent (Stored). Този тип XSS атака е възможна при сайтове, в които данни предоставени от потребителя се съхраняват на сървъра и се използват за генериране на динамично съдържание, без да се проверяват. Атакуващият изпраща злонамерено съдържание, което се съхранява на сървъра. Когато други потребители посетят страницата, където това съдържание се визуализира, те стават жертва на атаката. Атаки от този тип са най-често срещани в приложения, които позволяват на потребителите да изпращат коментари към съдържанието на страниците. Вместо стандартен коментар, атакуващият изпраща код, който при липса на проверка се изпълнява за всички потребители, които видят коментара. Този тип атаки са по-мощни, тъй като достигат до всички потребители, които отворят компрометираната уеб страница.
- DOM Based. По-рядко се срещат DOM базираните атаки, които се изпълняват изцяло от страна на клиента. Те са възможни, когато JavaScript код използва директно данни от DOM обекти.

Предотвратяване

Някои общоприети практики за предотвратяване на XSS включват тестване на кода на приложението преди внедряване и отстраняване на уязвимостите своевременно. Уеб разработчиците трябва да филтрират въвежданите данни на потребителите, премахвайки възможните злонамерени знаци и скриптове.

Колкото времето върви напред, толкова подобри стават хакерите, използвайки колекция от набори с инструменти, за да ускорят процеса на експлоатиране на уязвимостите. Това означава, че простото внедряване на тези общи XSS практики за защита вече не е достатъчно. Процесът на защита и предотвратяване трябва да започне от основата и да се изгражда нагоре. Процесът на предотвратяване трябва да започне по време на разработването. Уеб приложенията, които са изградени с използване на солидна методология за сигурно разработване на жизнения цикъл, е по-малко вероятно да покажат уязвимости в окончателната версия. Това ще подобри не само сигурността, но също и ефективността и общата цена за притежание,

тъй като поправянето на проблема на живо е по-скъпо, отколкото по време на разработването.

A4 – Нарушен контрол на достъпа. Възниква при неправилно прилагане на ограниченията за действията на автентикациите потребители. Злоумишлени лица могат да използват тези недостатъци за достъп до неоторизирани функции и/или данни, като например достъпа до други акаунти, да разглеждат чувствителни файлове, да променят данните на други потребители, да променят правата за достъп и др.

Предотвратяване

Предотвратяването на недостатъците в контрола на достъпа изисква избиране на подход за защита на всяка функция и всеки тип данни (например номер на обект, име на файл).

- Проверяване на достъпа. Всяко използване на директно обръщане от надежден източник трябва да включва проверка за контрол на достъпа, за да се гарантира, че потребителят е упълномощен за искания ресурс.
- Използване на указания за индиректно обръщение към потребител или сесия. Този модел на кодиране предотвратява нападателите да се насочват директно към неоторизирани ресурси. Например, вместо да се използва ключът на ресурса, падащият списък от шест разрешени за текущия потребител ресурси може да използва номерата от 1 до 6, за да покаже коя стойност е избрала потребителя.
- Автоматизирана проверка. Автоматизиране на проверката за правилното оторизиране.

A5 – Грешки в конфигурациите за сигурност. За постигането на високо ниво на сигурност е необходимо да се дефинират и приложат допълнителни настройки за сигурност на приложенията, сървърите и операционните системи, тъй като настройките по подразбиране често са несигурни.

Предотвратяване

Основните препоръки са да се приложат следните мерки:

- Непрекъснат процес, който улеснява бързото и лесното разполагане на друга среда, която е правилно конфигурирана. Средите на разработка, качествен анализ и продуктивната трябва да бъдат конфигурирани идентично (с различни пароли, използвани във всяка среда). Този процес трябва да бъде автоматизиран, за да се сведе до минимум усилието, необходимо за създаване на нова защитена среда.
- Процес за своевременното поддържане и прилагане на всички нови софтуерни актуализации и корекции на всяка разгърната среда.
- Архитектура на приложенията, осигуряваща ефективно и сигурно разделяне на компонентите.
- Автоматизиран процес за проверка, че конфигурациите и настройките са правилно конфигурирани във всички среди.

A6 – Изтичане на чувствителна информация. Много уеб приложения не защитават в достатъчна степен чувствителната информация като номера на кредитни карти, лични данни и данни за удостоверяване. Това дава възможност на атакуващите да откраднат или да модифицират такива слабо защитени данни с цел извър-

шване на измами с кредитни карти, кражба на самоличност, или други престъпления. Чувствителните данни се нуждаят от допълнителна защита като криптиране в място или при пренос, както и специални предпазни мерки, когато се обменят с браузъра.

Предотвратяване

За всички чувствителни данни трябва да се спазват следните препоръки:

- Вземане предвид на заплахите за данните, които се защитават, всички чувствителни данни трябва да са криптирани при съхраняване и пренос по начин, който ги защитава от тези заплахи.
- Да не съхраняват чувствителни данни, без да са необходими. Излишните данни да се унищожат своевременно.
- Използване на силни стандартни алгоритми и силни ключове и правилно управление на ключовете.
- Паролите да се съхраняват с алгоритъм, специално предназначен за защита на парола, като bcrypt, PBKDF2 или scrypt.
- Деактивиране на автоматичното довършване на формуляри, изискващи чувствителни данни, и деактивиране кеширането за страници, съдържащи чувствителни данни.

A7 – Недостатъчна защита от атаки

Приложенията трябва да откриват, предотвратяват и отговорят на както на ръчните, така и на автоматизирани атаки. Идеята е да се премахнат невалидните входни данни чрез блокиране на опитите и маркиране на въпросния акаунт. {{L_00}}

Предотвратяване

Има три основни мерки, предприемането на които предоставя достатъчна защита от атаки:

- Откриване на атаки. Признаци за атака са: възникването ли нещо, което е невъзможно да бъде причинено от легитимни потребители, приложението се използва по начин, който обикновеният потребител никога не би направил.
- Отговор на атаки: Дневниците и известията са от решаващо значение за навременния отговор. Трябва да се вземе решение дали ще се блокират автоматично заявки, IP адреси или IP обхвати, да се обмисли възможността за деактивиране или наблюдение потребителски акаунти, с необичайно поведение.
- Своевременно отстраняване на грешки в приложението. Откритите грешки в приложението е необходимо да се отстраняват за един ден. Ако това е невъзможно, трябва да се анализира HTTP трафика, потока от данни и/или изпълнението на кода, за да се предотврати използването на уязвимости.

A8 – Подправена междусайтова заявка Cross-Site Request Forgery (CSRF).

Тази атака протича в две стъпки. В първата атакуващият принуждава браузъра на атакувания да изпрати заявка, включваща автентифицираща информация. Във втората се изпращат заявки към уязвимото приложение, изглеждащи легитимни от страна на атакувания.

Предотвратяване. Включване на непредвидим токен във всяка HTTP заявка, който е уникален за всяка сесия на потребителя. Токена може да бъде включен в скрито поле, за да се избегне показването му в URL адреса. При браузърите, позволяващи използването на cookies, може да се използва флага "SameSite = strict".

A9 – Използване на уязвими компоненти. Компоненти като библиотеки и други софтуерни модули се изпълняват с пълни привилегии. Използването от атакуващия на уязвимостта на даден компонент често води до сериозна загуба на данни или поемане на контрол над сървър. Приложенията използващи компоненти с известни уязвимости компрометират защитата си и дават възможност за извършването на редица.

Предотвратяване

Повечето компонентни проекти не създават поправки на уязвимости за стари версии, така че единственият начин за отстраняване на проблема е надстройване до следващата версия, което може да изисква други промени в кода. Разработчиците на софтуер е необходимо да спазват следното:

- Непрекъснато наблюдение на версиите на компонентите от страна на клиента и сървъра и техните зависимости, като използвате инструменти за проверка на версии.
- Непрекъснато следене на източници като NVD за уязвимости в компонентите си. Използване на инструменти за анализ на състава на софтуер, за автоматизиране на процеса.
- Анализиране на библиотеките, за да се провери, че те са действително извикани по време на изпълнение, преди да се правят промени, тъй като голямата част от компонентите никога не се зареждат или не се извикват.
- Въвеждане на виртуален слой, който анализира HTTP трафика, потока от данни или изпълнението на кода и предотвратява експлоатирането на уязвимости.

A10 – Непроверени пренасочвания и препращания. Уеб приложения често пренасочват и препращат потребителите към други страници и сайтове, използвайки ненадеждни данни за определяне на дестинацията. Липсата на проверка дава възможност на атакуващите да пренасочат жертвата към лъжливи сайтове или да използват препращане за получаване на неотсориизиран достъп до страници.

Предотвратяване

Безопасното използване на пренасочвания и препращания може да се извърши по няколко начина:

- Избягване на използването на пренасочвания и препращания.
- При използване да не се включват параметрите на потребителя при изчисляване на местоназначението.
- Ако параметрите на местоназначението не могат да бъдат избегнати, трябва да се провери дали предоставената стойност е валидна и разрешена за потребителя.
- Препоръчва се всички такива параметри на местоназначението да бъдат кодирани, а не действителният URL адрес или част от URL адреса, а на сървъра този код да се преобразува в целевия URL адрес.

Избягването на такива недостатъци е изключително важно, тъй като те са обичайна цел на злоумишлени лица, опитващи се да спечелят доверието на потребителя.

Заключение

Атаките срещу уеб приложенията може да костват не малко време и финансови ресурси, компрометиране на репутацията на организацията, да доведат до пробиви в сигурността на данните. Всичко това налага използването на стратегии и механизми за защита. Необходимо е да се обърне голямо внимание на сигурността на уеб приложението още в етапа на изграждането му. Добрата информираност на разработчиците с уязвимостите и начините на защита от тях, толкова по-сигурно ще е даденото уеб приложение.

Литература

1. Alonso C., Bordón, R., Guzmán, A., Beltrán M., LDAP Injection & Blind LDAP Injection In Web Applications, [онлайн], [прегледано на 16.06.2013] достъпно от: <https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf>
2. Two New Vulnerabilities added to the OWASP Top 10, [онлайн], [прегледано на 14.06.2017] <https://www.contrastsecurity.com/security-influencers/two-new-vulnerabilites-added-to-the-owasp-top-10>
3. Newsham T., Format String Attacks, [онлайн], [прегледано на 12.06.2016] достъпно от: <http://hackerproof.org/technotes/format/FormatString.pdf>
4. OWASP Top Ten 2017 Project, [онлайн], [прегледано на 11.07.2017] достъпно от: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project.

Д. К. Хубенов,

ТЕХНИКИ ЗА ПОДДЪРЖАНЕ НА ИНФОРМАЦИЯ ЗА СВОБОДНИЯ РАДИОЧЕСТОТЕН СПЕКТЪР В КОГНИТИВНИТЕ РАДИО МРЕЖИ, ИЗГРАДЕНИ ПО СТАНДАРТ 802.22

Дянка К. Хубенов

Национален военен университет „Васил Левски“,
Факултет „Артилерия, ПВО и КИС“, гр. Шумен, ул. Карел Шкорпил“ 1
e-mail: d_hubenov@abv.bg

MANAGEMENT TECHNIQUES OF AVAILABLE RADIO FREQUENCY SPECTRUM INFORMATION IN 802.22 COGNITIVE RADIO NETWORKS

Dyanko K. Hubenov

Abstract: In this paper are given the techniques for management of available radio frequency spectrum in 802.22 cognitive radio networks. These techniques provide the ability of efficient utilization of radio spectrum and robust detection of incumbents in order to avoid occurrence of harmful interference.

Keywords: cognitive radio, radio spectrum sensing, broadband wireless access network, regional area network.

Въведение

В настоящия доклад са разгледани способите на когнитивното радио, поддържани от стандарт IEEE 802.22 за защита на официалните ползватели и ефективната работа на мрежите изградени по този стандарт. Способностите свързани с когнитивното радио включват: управление на честотния спектър (SM) на базовата станция (BS), автоматизация на сканирането на честотния спектър (SSA), достъп до база данни, управление на настройките на каналите, спазване на приетите политики, регистриране и следене на клиентските устройства (CPE), сканиране на честотния спектър и геолокация.

Всички IEEE 802.22 устройства разполагат със способностите на когнитивното радио, което им дава възможност да вземат решения, свързани с поведението им в определена обстановка, с помощта на информация получена от различни източници, като сканиране на честотния спектър, геолокация, достъп до база данни и др. Информацията се придобива чрез свързване с базата данни и/или чрез директно сканиране на честотния спектър за официални ползватели, чиято нормална работа може да бъде засегната при използване на определени канали от страна на IEEE 802.22 устройствата. Освен това информацията може да бъде следствие на спазването на политики регламентирани от официалната организация отговаряща за това в зависимост от държавата на чиято територия е разположено IEEE 802.22 устройството.

Освен това IEEE 802.22 устройството сканира честотния спектър за да открие присъствие на официални ползватели в района, преди и по време на работата си. Сканирането включва както канали, които се очаква да бъдат свободни, така и такива, които вероятно биха причинили зловредно влияние при използването им. Сигналите, които IEEE 802.22 устройството трябва да сканира са:

- Телевизионно излъчване;
- Сигнали от безжични микрофони;
- Сигнали излъчени от защитни устройства, като например IEEE 802.22.1 безжичен маяк;
- Други устройства на официални ползватели, като например устройства, предназначени за медицинска телеметрия.

IEEE 802.22 системите избират набор от работни, резервни и кандидат канали, следвайки зададените процедури. Излъчването на IEEE 802.22 устройствата се контролира от редица политики заложи в SM.

Трябва да се отбележи, че IEEE 802.22 устройствата сканират също и за други IEEE 802.22 системи, които евентуално могат да се намират в същия район и ако такива бъдат открити, то устройствата трябва да прилагат процедурите за съвместна работа (self-coexistence).

1. Управление на честотния спектър

SM е разположен в когнитивната структура и е част от всяка IEEE 802.22 BS. SM отговаря за най-важните задачи, като поддържане на информацията за свободния честотен спектър, селектиране на каналите, управление на каналите, задаване на график за сканиране на честотния спектър, достъп до база данни, прилагане на процедурите за съвместна работа, налагане на политиките зададени от IEEE 802.22 и официалните организации и др.

Всички IEEE 802.22 устройства (BS и CPE) разполагат с автоматизация за сканиране на честотния спектър (SSA). SSA се свързва с SSF и изпълнява командите от SM за сканиране на честотния спектър.

SM заема централна част от WRAN BS и отговаря за повишаването на сигурността на официалните ползватели и ефективното разпределяне на радиочестотния спектър при следване на регулаторните политики. Във връзка с това SM централизира вземането на всички решения във WRAN клетката, като се съобразява със свободния честотен спектър и оптималното му използване. Основните функции на SM са:

- Поддържане на информация за свободния радиочестотен спектър;
- Класификация и селектиране на каналите;
- Контрол при асоциирането;
- Управление на набора от канали;
- Достъп до база данни;
- Планиране на тихи периоди за сканиране на радиочестотния спектър;
- Налагане на политиките зададени от IEEE 802.22 и официалните организации;
- Вземане на решение за смяна на канала на едно или повече CPE или на цялата клетка;
- Изпълнение на процедурите за self-coexistence със други WRAN и др.

2. Поддържане на информация за свободния радиочестотен спектър

SM поддържа информация за статуса на честотния спектър, който е на разположение за утилизирание, в съответствие с наложените политики за дадения район. SM получава информация за статуса на каналите, по отношение на присъствието на официални ползватели и други WRAN мрежи в района и използва тази информация при вземане на решения относно избиране на канали, управление на състоянието на каналите и процедури за self-coexistence.

За поддържането на статуса на каналите свободни за използване, SM трябва да събере достатъчно информация от следните източници:

1) База данни: SM има достъп през по горните протоколни слоеве до базата данни за официалните ползватели, съществуването на която е задължително съгласно изискванията на официалните организации в някои страни. Базата данни е услуга, която разполага със списък на свободните канали и стойността на максималната ефективна изотропна излъчена мощност EIRP (Effective isotropic radiated power), която е позволена за тези канали на базата на запитвания за геолокацията на WRAN устройствата. В страни където не е задължително да бъде предлагана услугата база данни, списъкът със свободните канали следва да бъде предоставен от оператора.

2) Геолокация: SM има достъп до информацията съхранявана на BS за идентификация на собственото местоположение и местоположението на свързаните към BS CPE, както и на CPE, които искат да се свържат с BS.

3) Сканиране на честотния спектър: SM има интерфейс към SSA разположена в BS и CPE. SM използва функционалните възможности и фреймове за управление на PHY и MAC слоевете за да контролира и координира сканирането на честотния спектър във WRAN клетката. SM стартира заявки към SSA разположена в BS и CPE за извършване на сканиране на честотния спектър, събира докладите след неговото завършване и ги обединява.

SM определя статуса на каналите, по отношение наличието на официални ползватели като комбинира информацията от геолокация, информацията от база данни за официалните ползватели и резултатите от сканирането на честотния спектър. За да работи IEEE 802.22 системата, BS трябва да поддържа връзка с база данни (ако има такава) съдържаща списък със свободните канали за района. Когато системата работи в страна където няма такава база данни, всички канали първоначално се приемат за свободни. В този случай SM определя дали каналите са свободни след сканиране на честотния спектър. Състоянието на каналите се определя при инициализирането на мрежата и периодически се обновява по време на работа на мрежата.

2.1. Класификация и селектиране на каналите

SM определя работния канал (operating channel) на MAC/PHY модулите на WRAN. SM определя също резервните канали (backup channels) и съответния им приоритет. Останалите канали, които са потенциално свободни за използване, но не са определени за работен или резервни, могат да бъдат класифицирани като кандидат канали, заети канали или забранени канали. Свободните канали (Available) са тези, които са на разположение да бъдат разгледани като евентуално работни за WRAN в дадения район, според базата данни. Канали, които не са available според базата данни се изключват от WRAN.

Available каналите допълнително се класифицират в една от четири категории:

- **Забранени (Disallowed):** канали, които са изключени от оператора вследствие на работни ограничения или такива наложени от местния регулатор;

- **Работен (Operating):** Каналът, който се използва за свързка между BS и CPE в една WRAN клетка. Работния канал следва да бъде сканиран на всеки две секунди за различни видове сигнали, в съответствие с изискванията на официалните органи. Освен това работния канал се сканира на всеки две секунди за сигнали от IEEE 802.22.1 маяци, ако в страната е разрешено използването на такива.

- **Резервни (Backup):** Канали, които са подготвени да станат незабавно работен канал в случай, когато WRAN трябва да превключи на друг канал. BS може да поддържа няколко резервни канал по всяко време и да ги заменя в зависимост от зададения им приоритет. Резервните канали се сканират за официални ползватели на всеки шест секунди. Един канал може да бъде в списъка на резервни канали докато не бъде открит официален ползвател на него, което да предизвика зловредна намеса от страна на WRAN излъчването.

- **Кандидат (Candidate):** Канали, които са кандидати да станат резервни. Базовата станция изпраща заявка до CPE за сканиране и оценка на възможността за добавяне на тези канали към списъка с резервни канали. Въпреки че, сканирането на кандидат канали не се извършва често, всеки от тях трябва да бъде сканиран за наличие на официален ползвател на всеки 6 секунди за не по-малко от 30 секунди преди да се добави към резервните канали. Ако бъде потвърдено отсъствието на официален ползвател в първия канал от списъка с кандидат канали за разглеждания период от време BS ще го добави към списъка с резервни канали. Списъкът на кандидат канали съществува непрекъснато, тъй като на CPE е необходимо допълнително време за сканиране, след което списъка с резервни канали се обновява.

- **Защитени (Protected):** Канали, на които са открити официални ползватели при извършването на сканиране. Защитените канали да бъдат добавени към списъка с кандидат канали, когато официалните ползватели или други WRAN мрежи ги освободят. За целта се използва информацията получена от база данни и чрез сканиране. Защитен канал може да бъде приет за резервен канал ако след сканиране на всеки 6 секунди се установи, че през последните 30 секунди не е бил зает от официален ползвател. Винаги когато е възможно SM трябва да определя вида на сигнала във всеки защитен канал.

- **Неопределени (Unclassified):** Канали, които не са били сканирани. Те могат да бъдат сканирани в съответствие с използвания SM. Щом бъде сканиран, неопределения канал може да бъде прекласифициран като защитен или кандидат в зависимост от резултата на сканирането.

Описаните по-горе класификации на каналите са взаимно изключващи се т.е. един канал не може да бъде класифициран към повече от една категория. От друга страна поради същността на WRAN coexistence механизма един канал, който е работен за една WRAN система, може да бъде работен и за друга WRAN система или да бъде в списъка с резервни или кандидат канали.

2.2. Преминаване на канали от един набор към друг

Всеки канал от списъка със свободни канали в базата данни е класифициран от SM към едно от възможните състояния. В края на тихия период, в зависимост от активността на CPE и качеството на канала, всеки канал може да бъде преместен към друго състояние. Състоянията на каналите първоначално са класифицирани на базата на резултатите получени от сканирането на радиочестотния спектър извър-

шено при инициализиране на WRAN системата. Вероятните събития при преминаване от едно състояние към друго са както следва:

Събитие 1: Канал, който е бил работен или е бил в списъка на резервните или кандидат канали става защитен, когато бъде открит официален ползвател при сканиране.

Събитие 2: Не е бил открит официален ползвател на канала.

Събитие 3: Не е открит официален ползвател на канала и са удовлетворени изискванията, дефинирани за резервните канали относно продължителност на сканиране от всички CPE, изращащи доклади до BS. (Допълнително може да се извърши приоретизация на каналите в списъка с резервни канали на базата на измереното качество на канала.)

Събитие 4: Каналът е освободен, тъй като WRAN вече не го използва.

Събитие 5: Каналът става работен след неговото избиране от WRAN за такъв.

Събитие 6: Не са удовлетворени изискванията, дефинирани за резервните канали относно продължителност на сканиране от едно или повече CPE. (Допълнително може да се извърши приоретизация на каналите в списъка с кандидат канали на базата на измереното качество на канала.)

Събитие 7: Когато неопределен канал бъде сканиран от всички активни CPE, той може да бъде прекласифициран като кандидат канал от SM ако не бъдат открити и докладвани официални ползватели за регламентирания период от време.

Събитие 8: Ако канала не е сканиран за периода от време регламентиран в IEEE Std 802.22 или съгласно изискванията на регулационния орган, каналът става неопределен. Ако той е в списъка с защитени канали и не е сканиран според изискванията си остава със защитен статус. (Каналът трябва да бъде сканиран от всички активни CPE за регламентирания период от време и резултатите от сканирането да бъдат изпратени до BS за да не бъде класифициран като неопределен.)

Преминаването на канали от една група в друга е представено и в табл. 1. Всеки ред показва промяната на състоянието предизвикано от дадено събитие. Всяка колона дава промяната на състоянието предизвикано от събитията на всеки ред за дадено състояние.

Затъмнените клетки в таблицата показват, че определено събитие не може или не трябва да се случва за даденото състояние. Ако събитието се случи, SM трябва да го игнорира. Например кандидат канал не може да стане директно работен канал.

Състояния Събития	Неопределен	Кандидат	Резервен	Работен	Защитен
Събитие 1	Защитен	Защитен	Защитен	Защитен	
Събитие 2					Неопределен
Събитие 3		Резервен			
Събитие 4				Кандидат	
Събитие 5			Работен		

Събитие 6			Кандидат		
Събитие 7	Кандидат				
Събитие 8		Неопределен	Неопределен		Неопределен

Таблица 1 – Преминане на канали от една група в друга

2.3. Приоритизиране на резервните и кандидат каналите, чрез използване на етикети на честотния спектър

При селекцията на канали в дадена клетка се спазват правилото на даване на етикети на честотния спектър, така че избраният канал да не влияе или да влияе на минимален брой канали, използвани от съседни клетки. Без коопериране честотната селекция на дадена клетка може да доведе до недостиг на канали за някои BS. Например ако свободните канали за BS1, BS2 и BS3 са съответно {1,3}, {1,2,3} и {1,2,3}, но BS2 решава да използва канал {1}, а BS3 канал {3}, то BS1 няма да разполага с канал, който да ползва. Освен това, кооперирането минимизира вероятността за колизия, когато няколко клетки сменят работните си канали, чрез избягване използването на идентични списъци с резервни канали.

Подобна е концепцията за централна клетка и съседни на нея клетки. Освен разгледаните вече групи от класифицирани канали при създаването на етикети се дефинират допълнителни групи:

- Група на каналите заети от WRAN: канали, които са работни за откритите съседните WRAN клетки.
- Група на резервните канали на съседните WRAN клетки: канали, които са в групата на резервни канали на откритите съседни WRAN клетки. Тази група се създава чрез проверяване на SCH/CBP на откритите съседни WRAN клетки, носещи информация за резервните канали.
- Група 1 на локален приоритет: всички канали от групите на резервните и кандидат каналите, с изключение на работните канали на съседните WRAN клетки и резервираните от тях резервни канали.
- Група 2 на локален приоритет: всички канали от групите на резервните и кандидат каналите, с изключение на работните канали на съседните WRAN клетки.
- Група 3 на локален приоритет: групата на каналите заети от съседни WRAN.

Поставянето на етикети на честотния спектър се задейства от следните събития:

- Откриване на официален ползвател;
- Откриване на нови съседните WRAN клетки или обновяване на списъка с открити такива;
- Принудителна смяна на работния канал (например поради интерференция);
- Заявка за съперничество получена от съседни WRAN клетки.

Процедурата за даване на етикети е показана на фигура 102 и се обяснява така:

1) SM създава и обновява групите с канали чрез получаване на информация от геолокационната база данни или чрез осведомяване за присъствие на официални ползватели и други WRAN в честотния спектър. По съответния начин се създават и обновяват групите с работни и резервни канали на съседните WRAN клетки.

2) SM обновява групата с резервни канали, като избира един или няколко канала от група 1 на локален приоритет. Ако група 1 на локален приоритет е празна, се избират канали от група 2 на локален приоритет, които са резервни канали за най-малък брой съседни WRAN клетки (ако няколко канала са резервни за еднакъв брой съседни клетки се избират произволни канали). Ако група 2 на локален приоритет е също празна се избират канали от група 3 на локален приоритет, които са работни за най-малък брой съседни клетки. (ако няколко канала са работни за еднакъв брой съседни клетки се избират произволни канали.)

3) Ако е необходима смяната на работния канал или е получено изискване за смяна от по-горен слой (при откриване на официален ползвател, силна интерференция или по-добро качество на някой резервен канал) SM прави първия канал от списъка с резервни канали работен и се връща на стъпка 2) за обновяване на списъка с резервни канали.

4) Ако новият работен канал е работен и за съседна клетка, се стартира процедура за self-coexistence съревнование.

5) Обновява съседните клетки с нови работни и резервни канали чрез SCH/CBP.

Ако се разгледа пример с централна клетка и шест съседни на нея клетки. Централната клетка има работен канал #1, резервен канал #2 и кандидат канал #7. В даден момент се появяват два официални ползвателя в централната клетка, при което тя е принудена да смени работния и резервния канал. Стартира се процес на поставяне на етикети. Кандидат канал #7 става работен, а канал #5 е избран за резервен, тъй като той е работен само за една съседна клетка. Всички съседни клетки стартират процес на поставяне на етикети след получаване на обновена информация от централната клетка и си обновяват списъка с резервни и кандидат канали, както се вижда на таблица 2. Ако се появи друг официален ползвател на канал #7, централната клетка ще трябва да ползва канал #5 за работен и ще стартира процедура за self-coexistence съревнование със съседната клетка. SM може да използва информация от CPE за приоритизиране на списъка с кандидат канали.

Състояние на централната клетка	Първоначално	След появяване на официални ползватели	След поставяне на етикети на честотния спектър
Работен канал	1	1	7
Група на резервните канали	2	2	5
Група на кандидат каналите	7	3,4,5,6,7,8	φ
Група на каналите заети от други WRAN	3,4,5,6,8	3,4,5,6,8	3,4,5,6,8
Група на резервните канали на съседни WRAN	4,5,6,7,8	3,4,5,6,7,8	4,5,6,7,8
Група 1 на локален приоритет	2	2	φ
Група 2 на локален приоритет	2,7	2 ,7	φ
Група 3 на локален приоритет	3,4,5,6,8	2 ,3,4,5,6,7,8	3,4,5,6,8

Таблица 2 – Процедура за поставяне на етикети на честотния спектър

Заклучение

В доклада са представени техниките за управление на честотния спектър в когнитивни радиосистеми, работещи по принципите на стандарт 802.22. Управлението на честотния спектър е част от когнитивната структура на устройствата. Когнитивната архитектура позволява да се вземат решения, свързани с поведението на системата в различни ситуации. Това се извършва с помощта на информация, получена по различни методи, като сканиране на честотния спектър, геолокация, достъп до база данни и др. Като резултат се определят свободните канали, ограниченията за максимална мощност на излъчване и правата за асоцииране на клиентското устройство към работния канал.

Литература:

1. IEEE Computer society, IEEE Std 802.22-2011, IEEE Standard for Information Technology — Telecommunications and information exchange between systems—Wireless Regional Area Networks (WRAN)—Specific requirements—Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands., June 2011
2. D. Cabric, S. Mishra, and R. Brodersen. “Implementation issues in spectrum sensing for cognitive radios.” In *Proc. ACSSC*, Pacific Grove, CA, USA, November 7–10, 2004.
3. J. Yang. “Spatial Channel Characterization for Cognitive Radios.” Technical Report UCB/ERL M05/8, EECS Department, University of California, Berkeley, Jan 2005.
4. Z. Yu and S. Hoyos. “Compressive Spectrum Sensing Front-ends for Cognitive Radios.” In *IEEE International Conference on Systems, Man, and Cybernetics*, 2009.
5. X. Chen, L. Zhao, and J. Li. “A Modified Spectrum Sensing Method for Wideband Cognitive Radio Based on Compressive Sensing.” In *IEEE International Conference on Communications and Networking in China*, 2009.
6. T. Yucek and H. Arslan. “A survey of spectrum sensing algorithms for cognitive radio applications.” 11(1):116–130, First Quarter 2009.
7. Dennis Wieruch and Volker Pohl. “A Cognitive Radio Architecture based on sub-Nyquist Sampling.” In *Proc. IEEE DySPAN*, 2011.

АНАЛИЗ НА ПРЕДИМСТВАТА И НЕДОСТАТЪЦИТЕ ОТ ИЗПОЛЗВАНЕТО НА МОБИЛНИ GPS ПРИЕМНИЦИ ЗА ВОЕННИ ЦЕЛИ

Ивелин Г. Кацев

katsev.i@abv.bg

ANALYSIS OF THE ADVANTAGES AND DISADVANTAGES OF USING MOBILE GPS RECEIVERS FOR MILITARY PURPOSES

Ivelin G. Katsev

Abstract: *The use of mobile GPS receivers for military purposes has been strengthened in the armies of more developed countries. Examining the capabilities and devices of military users is the basis for understanding the capabilities of the GPS system.*

Keywords: *GPS, Mobile GPS receiver, satellites, PLGR, DAGR.*

Глобалната система за позициониране GPS (global positioning system) позволява триизмерно да се определи местоположението и скоростта на всеки един земен, воден или въздушен обект. Системата работи 24 часа в денонощието, независимо от атмосферните условия. Създадена е в САЩ за нуждите на отбраната, а в последствие е достъпна за ползване от цивилните потребители.

Структурата на GPS позволява практически непрекъснато определяне на координатите и скоростта на движение на обектите във всяка точка от земното кълбо. Системата се състои от минимум 24 спътника, разположени на 6 орбити на височина около 20000 километра и наземен контролен център с наблюдателни станции, разположени в различни точки на Земята. Принципът на действие се основава на измерването на разстоянието от мястото на устройството-приемник до групата спътници, чиито координати са точно определени и известни. Разстоянието се пресмята на база времето за достигане на радиосигнала от спътниците до потребителя. GPS работи в пасивен режим, а пот-



Фиг. 1. Групиранката от сателити и орбитите им.

ребителските устройства са само приематели, което от своя страна позволява използването на системата от неограничен брой клиенти .

GPS се състои се от три основни сегмента [8]:

- космически;
- контролен;
- потребителски.

Космическият сегмент се състои от групировка от 24 оперативни GPS – спътница, като максималният им брой е 32. Спътниците обикалят около земята по 6 геоцентрични орбитални равнини, разположени равномерно през 30° по дължина на Екватора. Всяка орбитална равнина е с наклон 55° спрямо екватора и съдържа минимум 4 спътника. Височината на орбитите над земята е около 20000 километра. Времето за една обиколка около земята е 11.58 ч. (половин звезден ден). При пълна констелация могат да се наблюдават по всяко време на денонощието при ограничения:

- до 15° над хоризонта - 8 спътника;
- при 10° над хоризонта - 10 спътника;
- при 5° над хоризонта - 12 спътника.

Спътниците са снабдени с платформа за радиопредаватели, атомни часовници, компютри и различно допълнително оборудване. Всеки спътник генерира основна честота на системата с номинална стойност 10.23 MHz и излъчва сигнали по две носещи честоти : L1 – 1575.42MHz и L2 – 1227.60MHz., които са модулирани с C/A – (coarse/acquisition) и P (precise) кодове. Целта при използването на двете честоти е елиминирането на грешката от закъснението на сигнала при преминаването му през йоносферата .

Категориите спътници, които се използват са:

- Блок I – изстреляни в периода 1978-1985 година. Броят им е 5 и са разположени на орбити с наклон 63° . Продължителността на експлоатация е 4,5 години с тегло – 845kg.

- Блок II – първият е изстрелян на 14.02.1989г. от космическия център „Кенеди“, Кейп Канаверал, с ракета Delta II. През юни 1989г. са изведени в космоса още два спътника със совака. Продължителността на експлоатационния цикъл е 7,5 години.

- Блок II A – (Advanced – усъвършенстван) те имат отражатели за извършване на лазерни измервания. Изстрелването им започва след 1990г.

- Блок II R – (Replenishment – попълване заместване) те притежават гарантиран 10 годишен срок на експлоатиране и имат тегло около 2 тона. Извеждането им в орбита започва през 1997г . Атомните часовници за заменени с водородни мазери с точност от 10^{-14} до 10^{-15} .

- Блок II F – (Follow – следящ) Изведени в орбита след 2007г . Продължителност им на живот е до 15 г. и тегло над 2 тона. Те имат подобрения в навигационната апаратура и в структурата на сигнала.

Контролният сегмент служи за управление на системата като цяло и отговаря за измерване на параметрите на орбитите на спътниците и на отклонението на часовниците, прогнозиране на параметрите на орбитите, синхронизиране на атомните часовници и подаване на данни за препредаване на сателитите. Състои се от главна станция, разположена във военновъздушната база „ Шрийвър“, Колорадо Спрингс (САЩ) и четири станции за следене на спътниците от системата, разположени

съответно на островите Възнесение (в Атлантическия океан), Диего Гарсия (в Индийския океан) и Куаджалеин (един от Маршаловите острови) в Тихи океан и Хавай. Те денонощно приемат радиосигналите, излъчвани от спътниците от системата и ги препредават в реално време на главната станция.

Потребителският сегмент се състои от GPS приемниците на потребителите, използващи военни и цивилни приложения. Приемника декодира подавания от няколко сателита сигнал и изчислява позицията си с помоща на трилатерация (сходен, но различен от триангулацията метод).

Потребителите на системата се разделят на няколко категории:

- в зависимост от категорията им:
 - военни;
 - граждански (цивилни).
- според изискваната точност:
 - с висока;
 - със средна;
 - с ниска.
- според мобилността:
 - мобилни;
 - статични.
- според актуалността на резултатите:
 - в реално време;
 - извън реално време.
- от конструктивна гледна точка:
 - самостоятелна GPS апаратура;
 - модули за вграждане в други потребителски системи, т.нар OEM модули.

От тук идва и голямото разнообразие на потребителските устройства, предлагана на пазара от различни производители, които въз основа на измерените величини и достиганата точност може да се класифицират като:

- GPS приемници за единични кодови измервания;
- диференциални (DGPS) приемници;
- геодезически фазови GPS приемници.

Принципът на действие се базира на метода трилатерация, чрез който позицията на една точка се определя като пресечката точка на няколко окръжности с известен радиус и известни координати на центровете. Всеки спътник може да се определи като център на сфера с координати – позицията на спътника и радиус – разстоянието до приемника. За да се определи положението на приемника, то трябва да се определят разстоянията до спътниците и техните точни координати. Разстоянието от всеки спътник до потребителя се пресмята като времето за което сигналът изминава разстоянието от спътника до приемника и се умножава по скоростта на светлината (скоростта с която се разпространяват електромагнитните вълни). Времето, за което сигналът достига до потребителя, е разликата във времето на приемане и на изпращане на сигнала.

Както всяка техническа система, GPS има грешки при определянето на позицията. В идеалния случай системата би трябвало да определя координатите точно, но на практика грешките достигат от няколко до десетки метра.

Причините за грешките в GPS могат да бъдат:

- Неточна позиция на спътниците – тази грешка се появява, когато навигационните съобщения не предават точните координати на спътниците. Позицията им обикновено е известна с грешка от 1 до 5 метра и води до отклонение в положението до няколко метра. Грешката в позицията на спътниците има тенденция да нараства с времето, тъй като орбиталните параметри, необходими за изчисляване на положението на спътника, се обновяват на два часа и това води до натрупване на грешка при изчисленията с времето.

- Грешки в часовниците – грешката в точността на часовниците се отнася както за приемниците, така и за спътниците. Както стана ясно, грешките в приемниците могат да се пресмятат с помоща на допълнителни измервания, но за разлика от тях, отклоненията в часовниците на спътниците не могат да се изчислят. Всяка неточност от 10 наносекунди води до грешка в измерването на разстоянието до спътника с около 3 метра.

- Йоносферата – основната причина за грешки при определяне на позицията с GPS. Поради наличието на свободни електрони в йоносферата, скоростта на електромагнитните вълни намалява при преминаването през тази област. В резултат на това се променя разстоянието до сателитите, изчислено на базата на скоростта на светлината във вакуум и се получават грешки от порядъка на 10 метра.

- Тропосфера – както йоносферата, така и тропосферата води до промяна на скоростта на разпространение на GPS сигнала. Промяната на температурата, налягането и влажността на въздуха са фактори за промяна на скоростта на радиовълните.

- Многократни отражения (мултипат) – се нарича грешката, предизвикана от отразяването на сигналите от различни повърхности. При отражението на сигнала, пътят, който той изминава, се удължава, а с това се променя и измереното разстояние до спътниците. По този начин, когато се използват отразените сигнали, а не директните се получава неточност при определянето на стойността на разстоянието и се получава грешка при определяне на положението.

За подобряване на точността при определяне на координатите се използват диференциални GPS системи. Тези системи включват една или няколко неподвижни контролни станции с точно известни координати, в които се сравняват действителното и изчисленото положение, пресмятат се корекциите и се предават към потребителите в зоната на обслужване. Наред с диференциалните системи съществуват и други методи за подобряване на точността на изчислената позиция, като съчетаване на GPS приемници с инерциални системи или използване на алгоритми за определяне на изправността на спътниците. В първия случай, GPS приемниците се комбинират с жирокомпас и акселерометър, които позволяват на приемника да определя позицията дори при загуба на сигнала. Във втория случай използват алгоритми за определяне на изправността на спътниците и изключват от навигационното уравнение тези, които не са достатъчно надежни.

Използването на GPS системата има много предимства[5]:

- Системата е безплатна. Единственото нещо, което потребителят трябва да закупи, е GPS устройството.
- Не изисква пряка видимост между точките за измерване.
- Точен и бърз начин за измерване.
- Изключително лесна за употреба.
- Осигурява 3D координати.

- Работи независимо от метеорологичните условия.
- Има 100% покритие на земната повърхност.
- Постоянна поддръжка и развитие.
- Лесна за интеграция на софтуерни инструменти на географски информационни системи.

Недостатъците на GPS системата могат да се сведат до:

- Необходима е пряка видимост на сателитите – трябва да има видимост на 15° и повече над хоризонта от зададената точка.
- Трябва да бъдат на разположение най-малко 4 спътника – това е причината, поради която не може да се използва под вода, в тунели, в помещения, под земята и т.н.
- Загуба на сигнала при: гъста растителност, многобройно населени области, долини, геомагнитни бури.
- Висока консумация на енергия на устройствата – батерията издържа до няколко часа при непрекъсната работа.

- Понякога GPS приемникът може да откаже по определени причини и тогава трябва да се работи по алтернативен метод за определяне на координатите.

Във въоръжените сили на САЩ се използват два основни модела мобилни GPS приемници. Те осигуряват бързо и достатъчно точно определяне на координатите, навигация, устойчивост на заглушаване, надеждност, работа при всякакви условия и са лесни за употреба [3].

Precision Lightweight GPS Receiver (PLGR или още наричан „plugger”) е по-стария модел мобилен GPS приемник. Той е на въоръжение в армията на САЩ от през 1990г. и осигурява[6]:

- работа до 2000 часа;
- до 5 използвани сателита;
- PPS-SM защита;
- устойчивост от заглушаване до 24 dB;
- време за първоначално определяне на координатите 360 s;
- време за до-уточняване около 60 s;
- поддържащ само една носеща честота L1.

Точност:

- времева – 100 ns;
- при определяне на координатите:
 - o SDGPS - < 1 m;
 - o CEPWAGE <4 m;
 - o CEPGPS <16 m;
 - o SEGPS <100 m.
- при определяне на скоростта – 0.03 m/s.

Defense Advanced GPS Receiver (DAGR или още наричан „dagger”) е подобрен мобилен GPS приемник. Той е на въоръжение от 2004 г. и замества остарелия PLGR, като осигурява[2]:

- работа до 5000 часа;
- до 12 използвани сателита,
- SAASM защита,



Фиг. 2. Precision Lightweight GPS Receiver (PLGR)

- устойчивост на заглушаване до 41 dB,
- време за първоначално определяне на координатите 100 s
- време за до-уточняване < 22 s,
- поддържащ само две носещи честоти L1и L2.

- графичния му интерфайс също съдържа и географски карти.

Точност на DAGR[1]:

- времева– 52 ns;
- определяне на координатите;
 - o DGPS < 2.4 m,
 - o PPS < 6.7 m.
- при определяне на скоростта – 0.4 m/s.

Основното приложение на системата е за военни цели, но в последно време намира широко приложение и сред цивилните потребители. С помоща на GPS е възможно практически непрекъснато определяне на координатите и скоростта на движение на обектите, а също и точното време във всяка точка на земното кълбо или околоземното пространство. Масовото използване на GPS устройствата е за определяне на координатите на местоположението. Динамичността на бойните (и небойните) действия налагат мобилност на използваните устройства, бързина в определянето на координатите, точност и издръжливост, а това че се използват за военни цели налага устройствата да имат устойчивост и на смущения[7].

В съвременната динамика на военните действия бързината, точността и сигурността трябва да бъдат на високо ниво. Един от основните елементи при изпълнение на задачите от войските е намирането на местоположението на формированията на местността. За бързото и успешно изпълнение на поставените задачи, привързването трябва да става бързо и точно, ето тук е мястото на GPS приемниците, като те осигуряват тази точност и бързо позициониране. Тяхната мобилност от своя страна ги прави удобни за употреба при всякакви условия. Използването на технологията на глобалните системи за позициониране трябва да става с известни резерви, но не бива да се пренебрегват нейните предимства.



Фиг. 3. Defense Advanced GPS Receiver (DAGR)

Литература:

1. Defense Advanced GPS Receiver (DAGR), Rockwell Collins official site, 26.07.2017г.
https://www.rockwellcollins.com/Products_and_Services/Defense/Navigation/Ground_Products/Defense_Advanced_GPS_Receiver_-DAGR.aspx
2. DAGR (Defense Advanced GPS Receiver), Army property site, 26.07.2017г.
<http://www.armyproperty.com/Equipment-Info/DAGR.htm>
3. Global Positioning System Receiver, Army property site, 26.07.2017г.
http://www.armyproperty.com/Equipment-Info/PLGR_96_NSN.htm
4. Global Positioning System, Wikipedia site, 24.07.2017г.

https://en.wikipedia.org/wiki/Global_Positioning_System

5. GPS: new technology solves an old problem, army-technology site, 25.07.2017 г.

<http://www.army-technology.com/features/featuredssi-military-gps-global-positioning-system/>

6. PLGR GPS Family, prc68.com site, 26.07.2017 г.

<http://www.prc68.com/I/PLGR.shtml>

7. US Military GPS, Army-technology site, 24.07.2017 г.

<http://www.army-technology.com/projects/gps-block-iif-satellites/>

8. What is GPS, GPS.gov site, 25.07.2017 г.

<http://www.gps.gov/systems/gps/>

Г. Р. Парашкеванова, В. П. Василев, В. В. Лилов,
**ВИДЕОНАБЛЮДЕНИЕ ОТ НОВО ПОКОЛЕНИЕ С INTELLIGENT VIDEO
MANAGEMENT SYSTEM**

Геновева Р. Парашкеванова, Васил П. Василев, Виктор В. Лилов

Геновева Радослава Парашкеванова, e-mail: g.parashkevanova@abv.bg

Васил Панайотов Василев, e-mail: kpecno93@hotmail.com

Виктор Венков Лилов, e-mail: solaviki@abv.bg

**A NEW GENERATION VIDEO SURVEILLANCE WITH INTELLIGENT
VIDEO MANAGEMENT SYSTEM**

Genoveva R. Parashkevanova, Vasil P. Vasilev, Viktor V. Lilov

Abstract: A VMS can be the software component of a network video recorder and digital video recorder, though in general a VMS tends to be more sophisticated and provide more options and capabilities.

Keywords: recording, software, video management

1. Увод

Продуктът iVMS-4200 е многостранен софтуер за видео управление на DVR (дигитални видео рекордери), NVR (мрежови видео рекордери), IP (мрежови) камери, кодиращи устройства, декодери, VCA устройства, алармени бази и др. Той предлага множество функции, включително картина на живо в реално време, видео записване, отдалечено търсене и възпроизвеждане, архивиране на файлове, получаване на аларми и др., за да могат свързаните устройства да задоволят изискванията на задачата за наблюдение. Със своята гъвкава структура и лесни за използване функции,

Наблюдение на живо на до 64 камери в един екран Поддържа 4 VGA монитора Възможност за експортиране на видеоинформация на външен носител Централизирано получаване и обработка на алармени сигнали от свързаните устройства Поддръжка на USB джойстик. Всичко това е особено полезно в една разнородна среда за видеонаблюдение

2. Функционални модули

- Софтуерът притежава следните функционални модули:
- Модулът Основен изглед предлага картина на живо на мрежовите камери и видео рекордери и поддържа някои основни дейности като улавяне на снимки, записване, PTZ контрол и др.
- Модулът Отдалечено възпроизвеждане предлага търсене, възпроизвеждане, изнасяне на записани файлове.
- Модулът Видео стена предлага управление на декодиращото устройство и видео стена и функцията да се показва декодираното видео на видео стена. Моду-

лът Видео стена се показва само, когато към клиента са добавени декодиращи устройства

- Модулът Електронна карта предлага показването и управлението на електронни карти, входящи аларми, горещи региони и горещи точки.

- Модулът Управление на устройствата предлага добавяне, променяне или изтриване на различни устройства като устройствата могат да се внасят на групи за управление.

- Модулът Управление на събитията предлага настройките за график на охраняване, съвместни действия, алармите и други параметри за различни събития.

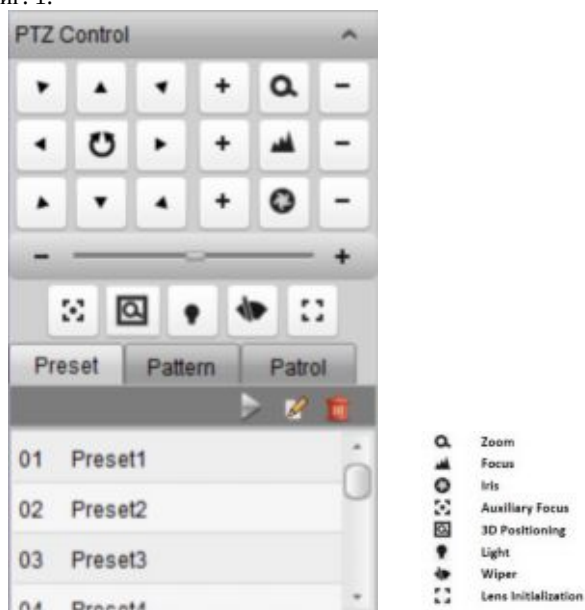
- Модулът График на записите предлага настройка на графика за записване.

- Модулът Управление на акаунта предлага добавяне, променяне и изтриване на акаунти на потребители като различни разрешения могат да се дават на различни потребители.

- Модулът Търсене в log предлага заявка към системните log файлове като log файловете могат да бъдат филтрирани по различни видове.

- Модулът Конфигуриране на системата предлага конфигуриране на общите параметри, пътеките за запис на файлове, звуците на алармите и други системни настройки.

Софтуерът предлага PTZ контрол на камерите с функции за панорама /наклон /приближаване (Pan /Tilt /Zoom). Може да се зададат предварителни настройки, патрулиране и шаблон на камерите в контролния PTZ панел. Също така може да се отвори PTZ контролен прозорец за действията на PTZ камерите, а този инструмент е видим на фиг. 1.



Фиг. 1. PTZ контрол

3. Отдалечени график, настройки и възпроизвеждане на запис

Когато устройствата за съхранение на видео са твърдите дискове, мрежовите твърди дискове, SD/SDHC карти на локалното устройство или свързан отдалечен сървър за съхранение, можете да се зададе график на записите за камерите за продължително, стартирано с аларма или стартирано с команда записване. Файловете със записи могат да бъдат търсени за отдалечено възпроизвеждане. Видео файловете могат да се записват на твърдите дискове, мрежовите твърди дискове, SD/SDHC картите на локалното устройство или на свързан сървър за съхранение. Някои локални устройства, включително DVR, NVR и мрежови камери, предлагат устройства за съхранение като твърди дискове, мрежови твърди дискове и SD/SDHC карти за файловете със записи. Може да се зададе график на записите или график на заснемането за каналите на локалните устройства.

Може да се зададе VCA правило към търсените файлове със записи и да намерите видео, в което има VCA събитие, включително VCA търсене, навлизане и пресичане на линия. Тази функция помага да се открие видео и да го маркира с червено и да се персонализира скоростта на възпроизвеждане на въпросната част от видеото и на останалото видео.

- VCA Search: Намира всички сродни събития със засичане на движение, които са се случили в предварително определен район.
- Intrusion: Засича, дали съществуват хора, превозни средства и други подвижни обекти, които навлизат в предварително определен район.
- Line Crossing: Двупосочно засича хора, превозни средства и други подвижни обекти, които пресичат виртуална линия.

4. Управление на събитията

В клиентския софтуер iVMS-4200 могат да се зададат правила за стартиращите събитията и свързани действия. Може да се присвоят свързани действия към стартиращо събитие като зададете правило. Например, когато е засечено движение, се подава звуково предупреждение или се случва друго свързано събитие.

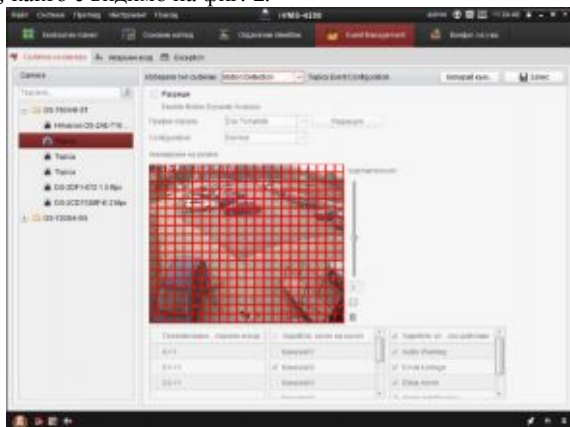
- Засичане на движение
- Аларма за намеса във видеото
- PIR аларма
- Загуба на видео
- Засичане на звук
- Засичане на разфокусираност
- Разпознаване на лице
- Пресичане на линия
- Навлизане
- Промяна на картината
- Входяща аларма
- Отказ на устройството

5. Конфигуриране на аларми

5.1. Аларма за засичане на движение

Алармата за засичане на движение се стартира, когато клиентския софтуер засече движение в определената зона. Свързаните действия, включително изпращане

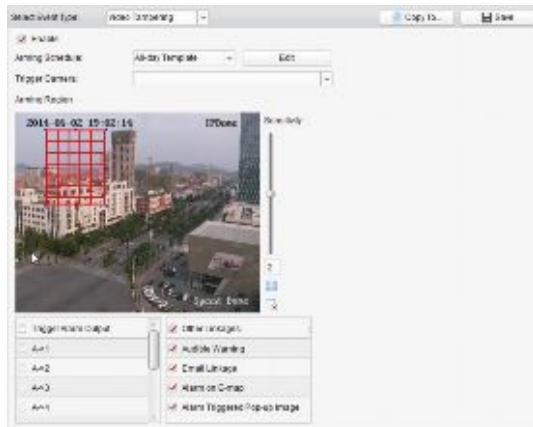
на аларма, записване на канала и действия на клиента, могат да се настроят. Съставя се решетка, както е видимо на фиг. 2.



Фиг. 2. Засичане на движение

5.2. Аларма за намеса във видеото

Аларма за намеса във видеото се задейства, когато камерата е покрита и наблюдаваната зона не може да се вижда. Могат да бъдат зададени свързани действия, включително изпращане на аларма и действие на клиента. На фиг. 3 е видна наблюдаваната зона.



Фиг. 3. Намеса във видеото

5.3. PIR аларма

PIR (Пасивна инфракчервена) аларма се задейства, когато нарушител се движи във визуалното поле на детектора. Топлинната енергия, излъчвана от човек или

друго топлокръвно същество като кучета, котки и др. може да бъде засечена. Да се има предвид, че PIR алармата изисква поддръжка от свързаното устройство.

5.4. Аларма за загуба на видео

Когато софтуерът не може да получава видео сигнал от източниците, ще се задейства алармата за загуба на видео. Могат да бъдат зададени свързани действия, включително изпращане на аларма и действие на клиента.

5.5. Аларма за разпознаване на лица

Камерата автоматично ще разпознае човешки лица в наблюдаваната зона, ако функцията е позволена. Ако се задейства алармата, серия от алармени действия ще се стартират. Може да се види на фиг. 4.



Фиг. 4. Разпознаване на лица

5.6. Аларма за засичане на навлизане

В наблюдаваната картина може да се зададе зона на засичане на навлизане и когато в зоната има навлизане за по-дълго от продължителността, която е зададена, се задействат набор от аларми.

Конфигурираме района за охраняване:

- **Region ID:** При отваряне на падащия списък, може да се избере ID на района за охраняване.
- **Trigger Time Threshold:** Обхват [0-10s], праг за времето, което обектът е прекарал в района. Ако се зададе стойност 0, алармата се задейства веднага, когато обектът навлезе в района.
- **Percentage:** Обхват [1-100]. Процентът определя отношението на частта от обекта, която, ако е вътре в района, ще се задейства алармата. Например, когато се зададе процент 50%, алармата ще се задейства, когато половината от обекта навлезе в района.
- **Sensitivity:** Обхват [1-100]. Стойността на чувствителността определя размера на обекта, който може да задейства алармата. Когато чувствителността е висока, много малък обект може да задейства алармата

5.7. Аларма за промяна на картината

Засичане на промяна на картината се използва да се засече промяна в наблюдаваната обстановка, причинена от външни фактори; като умишлено завъртане на камерата.

6. Замъгляване на участък

Възможността за скриване на участък при наблюдението е актуална при скриване на нещо. Софтуера търси точно този участък и дори при обход замъглява както е показано на фиг. 5.



Фиг. 5. Замъглен участък

7. Електронна карта

Функцията Е-мар (Електронна карта) дава визуален преглед на местоположенията и разпределението на инсталираните камери и устройства за входящи аларми. Може да се получава картина на живо от камерите на картата и съобщение от картата, когато се задейства аларма.

8. Функция Гореща точка

На картата от фиг. 6 могат да се добавят камери и входящи аларми и се наричат горещи точки. Горещите точки показват местоположенията на камерите и на входящите аларми и освен това през горещите точки можете да се получават картина на живо и информация за алармите в наблюдаваните зони.



Фиг. 6. Гореща точка

9. Заключение:

Полезността на софтуера е особено голяма в използването му на много големи обекти, където има унаследяване на участъци с остарялото аналогово видеонаблюдение. VMS има тенденцията да бъде по-изтънчен и да осигури повече възможности.

Литература

1. Дамьяновски, В. (2006). CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии. Превод от англ. – М.: „Ай-Эс-Эс Пресс“, 480 с.
2. Цанков, Ц. С. (2013). Администриране на мрежи. Център за дистанционно обучение на Шуменски университет „Епископ Константин Преславски“.
3. Ръководства по експлоатация на софтуер за видеонаблюдение.
4. <http://www.hikvision.com/europe/>

Д. Р. Денев, Т. С. Исмаил, Т. Н. Тончев,
**ЦИФРОВА АУДИО РАБОТНА СТАНЦИЯ FL STUDIO
ЗА АУДИО ОБРАБОТКА**

Даниел Р. Денев, Таркан С. Исмаил, Тончо Н. Тончев

*Даниел Росенов Денев, e-mail: slimshady33@abv.bg
Таркан Сали Исмаил, e-mail: tarkan_ismailov94@abv.bg
Тончо Насков Тончев, e-mail: toni1213@abv.bg*

DIGITAL AUDIO WORKSTATION FL STUDIO FOR AUDIO PROCESSING

Daniel R. Denev, Tarkan S. Ismail, Toncho N. Tonchev

Abstract: *The subject of study is showing the ability and use of digital audio workstations (DAW) software's for audio processing.*

Keywords: *DAW, Design, Sound processing*

1. Предмет на изследване

Предмет на изследване в предложената разработка е развитието на цифрови и аналогови сигнали в аудио обработваща среда Fruity Loops Studio.

Image-Line е белгийски производител на апаратно и програмно обезпечение за създаване на цифрова аудио обработка. Компанията е разработчик на най-иновативните аудио приложения и VST инструменти, и ефекти. Дадената ни софтуерна програма използва иновативна технология която позволява да се използва като VST инструмент в други Host програми за аудио обработка. Тя е разработена специално за редактиране и е основно подходяща за създаване на повтарящи се откъси от звукови сигнали.

Всеки модел може да се състои от неограничен брой инструменти или VST инструменти. Инструментите в модела могат да бъдат пренасочени и свързани към прозореца Mixer за преработка и добавяне на ефекти.

2. Fruity Loops Studio



Фиг. 1. Image-Line DAW Software – FL Studio 12

Fruity Loops Studio е програма за цифрова аудио обработка на компанията Image-Line. Програмата се разпространява в няколко различни издания: FL Studio Express, Fruity Edition, Producer Edition, Signature Bundle, All Plugin's Bundle и Mobile Edition; Програмата е показана на фиг. 1.

Системни изисквания

Минималните системни изисквания са: Поне 32 битова версия на Windows 7. Процесор с честота 2,0 GHz на Intel или AMD с поддръжка на SSE2 инструкции, 1 GB оперативна памет (препоръчително). Поне 2 GB свободно място за съхранение. Видео карта с поддръжка на минимална резолюция – 800 × 600 (Super VGA или по-добра). Самата звукова карта трябва да има инсталиран DirectSound драйвер и да бъде съвместим с ASIO/ASIO2 за аудио запис.

Препоръчителни системни изисквания: Задължително 64 битова версия на Windows 10. Процесор с 4,0 GHz честота, 8 GB оперативна памет. За съхранение са ни нужни около 6 GB свободно място на твърдия диск (при инсталиране повечето добавки).

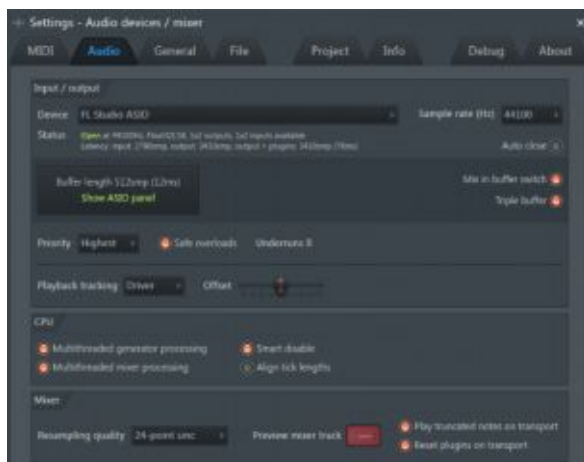
Изтегляне и установяване на програмата

Изтегляме продукта от официалния сайт на производителя <http://www.image-line.com/downloads/flstudiodownload.html>

Преди да инсталираме програмата в появилият се диалогов прозорец е желателно да маркираме FL Studio ASIO – тя осигурява ниска латентност и висока точност между софтуерното приложение и звуковата карта на компютъра.

Настройване на параметрите за аудио обработка:

Панела за настройки от фиг. 2 служи за конфигуриране на параметрите и опциите на аудио устройството.



Фиг. 2. Settings – Audio devices / mixer

В началото се настройва виртуалното аудио устройство, което се поддържа от компютъра, а след това и всички параметри.

Параметрите включват: честота на дискретизация, качество на вземане на проба, дължина на буфера и битовата дълбочина.

Честотата на дискретизация (Sample rate) е средно аритметичен брой от проби получен за една секунда $fs = 1/T$. Тази величина служи за възпроизвеждане на по-реален и качествен звук.

Качество на вземане на проба (Resampling quality) служи за подобрене на прецизността на обработвания се сигнал в процес на възпроизвеждане

Дължина на буфера (Buffer Length) служи за запис на Audio или MIDI информация. При намаляване на дължината на буфера се установява по-малко закъснение при запис в реално време, ако се увеличи дължината съответно и закъснението при възпроизвеждане ще нарасне.

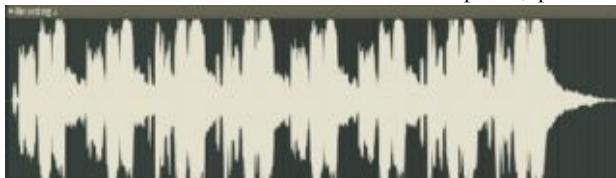
Битовата дълбочина (bit depth) е броя на битовете за информация за всяка проба от аудио сигнали. Практически този параметър отговаря за резолюцията на всяка проба от сигнала, като по този начин се задава качеството на звуковия сигнал.

Запис и редактиране на аудио сигнали и файлове

Записването на Audio Track в FL Studio става чрез натискане на бутона „Record“.

Преди запис е необходимо да се избере дадено входно устройство (микрофон).

Записания глас може да се запише в MONO TRACK и STEREO TRACK. Stereo Track-а е метод за възпроизвеждане на звука, което създава илюзия за многопосочна звукова перспектива, докато при Mono Track звука на възпроизвеждане идва от една позиция. Mono Track и Stereo Track са показани на фиг. 3, фиг. 4 и фиг. 5



Фиг. 3. Mono Audio Track



Фиг. 4. Stereo Audio Track

Приставката Edison служи за редактиране на аудио сигнали. Тя е съставена от многобройни свойства и инструменти за корекция. Основната ѝ цел е подобрен визуален показ на вълната на сигнала. Разполага с визуална спектрограма на честотните хармоники на звуковия сигнал.

Инструментите от Toolbar-а могат да обработят звуковия сигнал чрез различни ефекти. Свойствата се разделят на ефектни и музикални.

Ефектните могат:

- да нормализират началната амплитуда на сигнала
- може да изчистват шумовете

могат да увеличават и намаляват амплитудата на звуковия сигнал в маркирани части от сигнала

- могат да съставят ревербация да обръща аудио сигнала

Музикалните могат:

- да откриват нотацията в сигнала
- да намира и оказва темпо
- да записва и запаметява аудио.



Фиг. 5. Stereo Audio Track

Смесване и обработка на аудио сигнали, и файлове чрез ефект плъгини

Аудио смесване е процес, при който множество звуци са комбинирани в един или повече канали. В този процес, нивото на обема на източника, честотното съдържание, динамика, и панорамна позиция се обработва цялостното смесване да звучи ясно и чисто.

В процеса на смесване се използват ефект плъгини чрез които се подобрява качеството на аудио сигнала, изчистват се ненужни честоти, увеличават се други. Могат да бъдат добавени ефекти като филтри, еквилайзери, компресори, ограничители и специални ефекти като Reverb, Delay, ChorusFlanger.

Смесването на аудио сигнали използва следните процедури и ефект плъгини:

Честотно филтриране – това е процес при който се изрязват и премахват определен честотен диапазон ниски или високи честоти, както и може да се увеличи резонансната честота. Този процес се извършва чрез филтър ефект плъгин. Филтриран сигнал е показан на фиг. 6.



Фиг. 6. Филтриран сигнал

Честотна еквилизация – това е процес при който може да се усилят и намалят определени честотни диапазони, да бъдат изрязани честотни диапазони като ниски средни и високи. Осъществява се чрез еквилайзер плъгини. Те са съставени от няколко честотни групи из целия честотен спектър където всяка една честотна група отговаря за определен честотен диапазон. Еквилайзерите също могат да бъдат използвани като честотни филтри. Еквилизиран сигнал е показан на фиг. 7.



Фиг. 7. Еквилизиран сигнал

Аудио компресия е операция за обработка на сигнала където се намалява стойността на силните звуци и се усилят тихите звуци, където се стеснява целия динамичен диапазон на аудио сигнала.

Осъществява се чрез компресор ефект плъгини. Целта на компресията е да направи динамиката на сигнала еднаква. Компресиран сигнал е показан на Фиг. 8.



Фиг. 8. Компресиран сигнал

Ревербация – това е процес, при който се осъществява продължително отражение на звукови вълни (звукоотражение) в затворено помещение или в затворено ограничено пространство.

Целта на този ефект е да създаде в сигнала илюзията за пространственост. За ревербация се използват реверб ефект плъгини. Сигнал след Ревербация е показан на фиг. 9.



Фиг. 9. Сигнал след Ревербация

Аудио ограничителят е много подобен инструмент като компресора с това, че намалява динамичния обхват на сигнала, който преминава през него. Един компресор постепенно намалява нивото на сигнала над определен праг, но самия ограничител напълно предотвратява сигнал да надвиши определения праг. Осъществява се чрез ограничители (limiter) плъгини. На фиг. 10 е показан ограничен сигнал.



Фиг. 10. Ограничен сигнал

Аудио Delay (отломки)– този ефект се осъществява чрез Delay ефект плъгини. Където тези ефекти създават повторения (отломки) на аудио сигнала през определен период една от друга. С течение на времето повторенията затихват. Получава се ефект подобен на ехо

Менюто на Аудио Delay ефекта е показано на фиг. 11.



Фиг. 11. Аудио Delay

Предимства и недостатъци на Fruity Loops Studio

Предимства:

- Лесен и достъпен интерфейс за потребителя
- Безплатно обновявания на изданието
- Една от най-подходящите програми за създаване на музика
- Работи със синтезатори от високо ниво
- Екип за поддръжка в реално време с които може да се свържете по всяко време при възникнали проблеми
- Предлага най-голямата библиотека с звуци на пазара
- Поддържа MIDI контролер

Недостатък:

- Ограничения в ефектите в Мiхег-а

Заклучение:

Целта на изследването е да покажем как чрез дадена работна станция можем да запишем, редактираме, смесим и обработим аудио сигнал и да получим краен резултат.

Нашето изследване намира приложение в звукозаписни студиа, където може да се записва, редактира и смесва чрез хардуерни и софтуерни устройства.

Литература

1. Лалев Х. Л., Цанков Ц. С. (2008). Синтез на компютърни системи за работа в реално време. Международна научна конференция, посветена на 105-тата годишнина на Дж. Атанасов и Дж. фон Нойман, Шумен.
2. Friedman, S. (2014). FL Studio Cookbook. Packt Publishing, Birmingham.
3. Pease, S. (2009). FL Studio Power!: The Comprehensive Guide. Cengage Learning, Boston.
4. <https://www.youtube.com/watch?v=AtOrDf93jOk>

Т. Н. Тончев, А. Б. Александрова,
РАЗПРОСТРАНЕНИЕ НА ЕЛЕКТРОННИ КНИГИ

Тончо Н. Тончев, Албена Б. Александрова

Тончо Насков Тончев, e-mail: toni1213@abv.bg
Албена Бойкова Александрова, e-mail: alb.alexandrova@abv.bg

DISTRIBUTING ELECTRONIC BOOKS

Toncho N. Tonchev Albena B. Aleksandrova

Abstract: *Nowadays, the major libraries with printed editions gradually become unique museums. Digitized copies of the books are stored on a much smaller data media and practically may be available for all users on the Internet. Here the question arises how to manage access rights to the books.*

Keywords: *copyright, e-book, e-library*

Увод

От много години има реална възможност да се преустанови всякакъв печат на книги и много още други видове печатни издания. И тук не става въпрос само за спасяването на гори, чиято дървесина се използва за производството на качествена хартия. Отстраняването на всички тези хартиени издания ще освободи пространство например в гъсто населените градове. Всички тези тонове книги в обществените библиотеки заемат много голяма площ, рафтове, климатизация и осветление, обслужващ персонал и т.н.

Сега работят множество легални и пиратски електронни библиотеки и на нито едно не е ясно защо по законите в страната пиратството е престъпление, а когато го получим по законите на Еквадор например можем да четем много електронни издания. Библиотеките Либрусек, Максим Мошков, IRC bookz, LibGen, FictionBook, Альдебаран, Фензин, както и много други, са събирани главно от ентузиастични с цел да направят достъпна литературата до много потребители без да превеждат пари. Не са малко и сайтовете, които печелят от доставката на електронни книги, например с SMS-и до специален номер.

От другата страна на тази идея стои напълно легалното разпространение на книги и списания, възможно най-често на сайтовете на издателите, когато книга или списание е вече с голяма давност и всеки може да го изтегли. Издания на обширни ръководства и учебници за дадени прибори или машини в производството също са достъпни на сайтовете на производителите, т.к. за тях вече е заплатено.

Междина е ситуацията при учебниците и учебните помагала на преподавателите в университетите. На свои страници или в курсове за дистанционно обучение преподавателите поместват множество лекции, които са за студентите от даден курс. Щом студент се е записал за обучение, следва той да има право да използва

тези материали, но така той може да ги сподели и с трето лице, което не би трябвало да ги чете.

Можем ли да разчитаме на съвестта на потребителите да не разпространяват учебници и учебни помагала, или трябва да вземем някакви мерки срещу това? В този доклад ще разгледаме възможностите по зададения въпрос.

Защита на електронни издания

Електронните книги закупени от Amazon, Barnes & Noble, Kobo, Apple или Google, могат да бъдат четени на устройства, поддържащи DRM (digital rights management). Това са програмни или апаратно-програмни средства, които отключват права за действия с данни в електронна форма. Софтуерът в Windows също трябва да защитава правата на авторите. Такъв е например FBReader, даден на Фиг. 1, поддържащ няколко файлови формата и възможност за четене директно от архиви. В четеща няма възможност за отпечатване и не предоставя контекстно меню за копиране, но можем да копираме с клавишна комбинация.

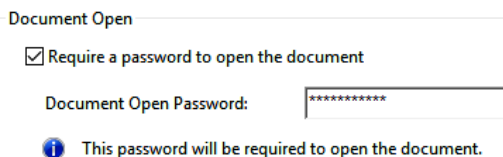


Фиг. 1. FBReader

Един от най-разпространените файлови формати, разпознаваеми от четците на електронни книги е PDF – Portable Document Format. Създаден е от Adobe Systems, той има възможност да бъде защитен на няколко нива.

В Adobe Acrobat ни предлагат два пътя за шифриране на документите – с помощта на парола и със сертификат. При избора с парола се отваря диалогов прозорец, в който могат да бъдат извършени следните основни заключения на документа:

- искане на парола за отваряне на документа, като на фиг. 2;



Фиг. 2. Заключение с парола за отваряне на PDF

- пълно заключване за отпечатване или нискокачествен печат (150 dpi);
- разрешения за няколко вида редактиране на документа;
- позволение за копиране на съдържанието, например текст, изображения и пр.;
- позволяване на инструмент за четене от екрана за слабо виждащи потребители.

Изброените се забелязват на фиг. 3.

Permissions

☒ Restrict editing and printing of the document. A password will be required in order

Printing Allowed:

Changes Allowed:

☐ Enable copying of text, images, and other content

☒ Enable text access for screen reader devices for the visually impaired

Change Permissions Password:

Фиг. 3. Права за PDF документите

Специален индикатор за сложността на паролата ни подсеща, че тя трябва да има поне средна сложност – достатъчен брой символи, включващи малки и главни букви, цифри и специални символи.

Заклучването за отваряне на файловете най-често се практикува с цел заплащане на ключа за отваряне, докато заключването за отпечатване и за копиране все пак ни дават възможност да можем да четем предоставеното ни издание.

Достатъчно по-добра е защитата с помощта на сертификат, т.к. поддържа дори и 256-битов AES алгоритъм за шифриране, видно от фиг. 4.

Select Document Components to Encrypt

☒ Encrypt all document contents

☐ Encrypt all document contents except metadata (Acrobat 6 and later compatible)

☐ Encrypt only file attachments (Acrobat 7 and later compatible)

 All contents of the document will be encrypted, and search engines will not be able to access the document's metadata.

☐ Ask for recipients when applying this policy

Encryption Algorithm:

Фиг. 4. 256-битов AES алгоритъм за шифриране

Файлт с цифровото удостоверение може да бъде създаден и при 2048-битов RSA алгоритъм на ключа, видно от фиг. 5.

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith): Моеро Име

Organizational Unit:

Organization Name:

Email Address: email@address.bg

Country/Region: BG - BULGARIA

Key Algorithm: 2048-bit RSA

Use digital ID for: Digital Signatures and Data Encryption

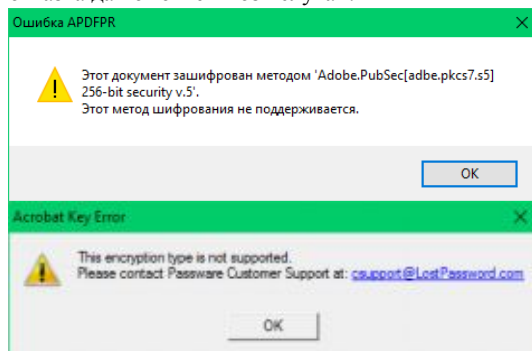
Фиг. 5. 2048-битов RSA алгоритъм на ключа за сертификата

Премахване на защита от PDF файлове

Заклучените файлове винаги са представлявали интерес за много софтуерни компании, работещи по снемането на защитата. Elcomsoft, VeryPDF и Passware са само една малка част от компаниите, предлагащи легален софтуер за премахване на защита от документи. Вероятно обосновката им е, че самите притежатели на документите забравят ключовете с които са заключени и без проблем си закупуват отключващия софтуер. В действителност и това е вярно, но по-знатни са потребителите, които искат и „консумират“ чуждото авторство, било само за да се запознаят с документа или да плагиатстват.

PDF шифриран със сертификат

Както бе отбелязано по-горе, най-сигурното заключване на документа е с помощта на сертификат. А именно липсата на такъв ни оставя с вързани ръце – не можем дори да отворим и да четем документа. На фиг. 6 забелязваме как „услужливия“ софтуер отказва да помогне в този случай.



Фиг. 6. Отказ за разшифриране на PDF със сертификат

При опит да се отпечата вече отворения документ, виртуалния Adobe PDF принтер изкарва отказ и следния рапорт във файл:

%[% ProductName: Distiller]%[%

This PostScript file was created from an encrypted PDF file.

Redistilling encrypted PDF is not permitted.

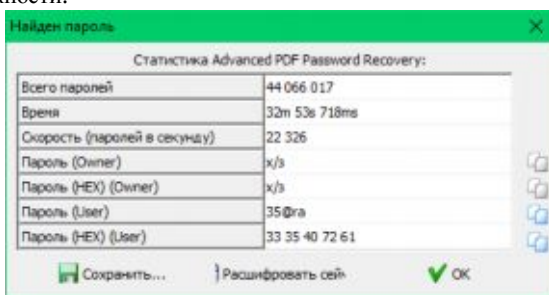
%%[Flushing: rest of job (to end-of-file) will be ignored]%%
%%[Warning: PostScript error. No PDF file produced.] %%

Този проблем обаче не стои пред нас, когато използваме виртуалния XPS принтер от Windows. По този начин вече другите потребители не е нужно да притежават сертификата, който навярно се закупува за да се отвори PDF документа.

PDF заключен с парола за отваряне

Другото „препятствие“ пред драгите ни читатели е документ, шифриран само с парола без сертификат. Тук е полезно наистина да се спазват всички правила за сложността на паролата.

За пример заключихме PDF с парола от пет символа – 35@ra. На фиг. 7 се забелязва, че дешифрирането е отнело почти 33 минути на съвременна машина със средни възможности.



Статистика Advanced PDF Password Recovery:	
Всего паролей	44 066 017
Время	32m 53s 718ms
Скорость (паролей в секунду)	22 326
Пароль (Owner)	x/3
Пароль (HEX) (Owner)	x/3
Пароль (User)	35@ra
Пароль (HEX) (User)	33 35 40 72 61

Сохранить... Расшифровать сей OK

Фиг. 7. Статистика за разкрита парола

Дотук разгледаните шифрирования по точки 3.1. и 3.2. могат да откажат прохаждащите в пиратство-плагиатстването, ако са първите им срещи със заключени PDF документи. За тяхно щастие обаче това са рядко срещани документи, т.к. обикновено се предоставя нещо, което поне да може да се прочете. Оттам следват по-малките проблеми и съответното им разрешаване.

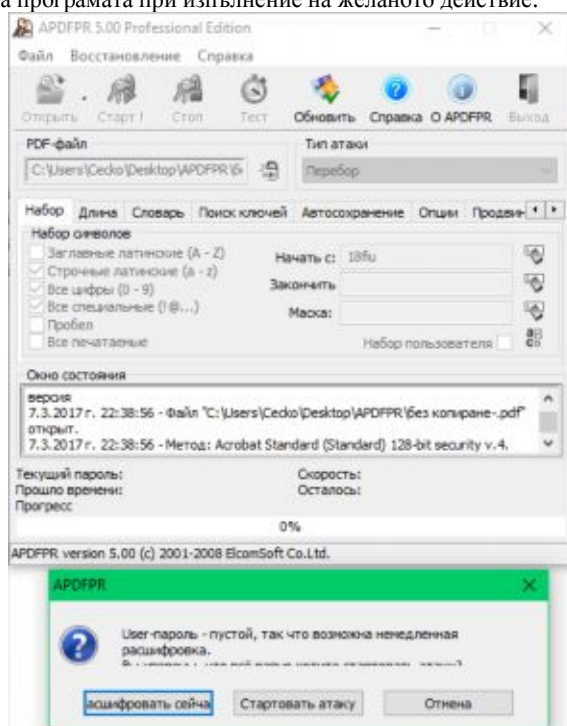
Разрешения за редактиране, копиране и отпечатване на PDF документ

Защитата на PDF документи в дадения случай лесно се премахват от почти всички софтуер, който е в услуга на плагиатстващия потребител. Отключването става обикновено и без да се четат ръководствата, интерфейса на програмите е доста приятелски настроен към потребителите. В случай че не проявим любопитство каква е паролата, можем много лесно и бързо да свалим защитата с помощта на PDF Password Remover на VeryPDF Advanced от фиг. 8.



Фиг. 8. Разрешаване на редактиране, копиране и отпечатване на PDF

PDF Password Recovery от Elcomsoft също може бързо да премахне защитата, но също ни предлага и атака по разкриване на паролата. На фиг. 9 се наблюдава общият вид на програмата при изпълнение на желаното действие.



Фиг. 9. PDF Password Recovery

Най-куриозното е, че даденият софтуер за събаряне на защитата на документи също е обект на авторско право, но дори и за него потребителите избягват да заплащат и го споделят безплатно с активационните му кодове.

Заклучение

Да защитим авторското си право, вече никак не е лесна задача. Хитрините на плагиатите далеч не са всички, описани в настоящия доклад. Днес всичко е в Интернет и могъщи глобални търсещи машини ни насочват къде е описана исканата от нас тема. Никак не е приятно, когато разберем, че много голям брой потребители са споделили напълно безплатно същото това издание, за което сме заплатили.

Литература

1. Мао, В. (2005). Современная криптография: теория и практика. Превод от англ. – М.: Издателска къща „Вилъямс“, 768 с.
2. Ръководства по експлоатация на софтуер за заключване и отключване на документи.
3. <https://acrobat.adobe.com/bg/en/>

BER PERFORMANCE FOR WCDMA SIGNAL IN A JAMMED RADIO ENVIRONMENT

Linko G. Nikolov, PhD
Dyanko K. Hubenov

linko.nikolov@aadcf.nvu.bg , d_hubenov@abv.bg

Abstract: Cellular systems are trending in a manner of increasing the data rates and coverage. Despite evolution to new generation networks (NGN), 3rd generation systems (3G) are widely deployed and still in use. Bit error rate (BER) against signal-to-noise ratio (SNR) defines the quality of the link. BER performance in a jammed radio environment is studied in this paper using simulation software. Barrage jammer is used in order to test system's noise resistance.

Keywords: WCDMA, SPREAD SPECTRUM, AWGN, BER, BARRAGE JAMMER, RAYLEIGH FADING

1. Code division and signal spread spectrum

The WCDMA system uses spread spectrum digital signal with rate 3,84 Msym/sec. The used Short codes, Long codes, interleaving, as well as convolutional and Turbo-coding, are improving the system's overall bit error rate (BER) performance. Spread spectrum has its benefits in comparison with narrowband signals according to noise immunity.

Most of the related work in the area of investigating the BER performance has been focused on the downlink channel as in [1] and [2]. While these investigations consider both shadowing and fading effects, they do not incorporate forward error correction in the analysis. The Performance of WCDMA using forward error correction with soft decision decoding has been given in some references. The performance of the forward DS-CDMA channel with power control in a Rayleigh fading channel was investigated in [5].

The effects of lognormal shadowing and Rayleigh fading using forward error correction in the form of Golay codes with hard decision decoding is given in [4] whereas in [6], Nakagami fading channels were considered using a weak Golay Code with hard decision decoding. The energy of the received signal suffers from degradation due to noise and fading which phenomenon causes digital errors.

2. Theoretical BER performance and Simulink™ model description

For the modelled WCDMA signal we have the equation:

$$s_{WCDMA}(t) = \sqrt{\frac{2E_c}{T_c}} \cdot p_i(t) \cdot c_i(t) \cdot g_T(t - t_c) \cos(\omega_0 \cdot t + \theta_M), \quad (1)$$

where E_c is the chip energy; T_c is the time duration of one chip; $p_i(t)$ is the information bit sequence; $c_i(t)$ is the code used for channel division; $g_T(t - t_c)$ is the impulse response of the RRC filter in the transmitter; ω_0 is the carrier frequency and θ_M ($M=1,2,3$ or 4) is the QPSK phase shift.

The Offset Quadrature Phase Shift Keying is used as a modulation technique in WCDMA. Its probability of error can be written theoretically by [8]:

$$p_s = (1 - p_b)^2 = 2 \cdot Q \left(\sqrt{\frac{2E_b}{N_0}} \right) \cdot \left[1 - \frac{1}{2} Q \left(\sqrt{\frac{2E_b}{N_0}} \right) \right], \quad (2)$$

where p_s is the probability of symbol error; p_b is the probability of bit error; Q is the complimentary error function „erfc“ and N_0 is the dispersion of the AWGN process.

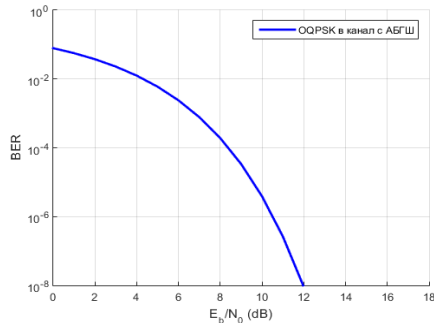


Figure 3 – Theoretical OQPSK BER Performance

The original model is modelled in MATLABTM and simulated in SIMULINKTM [9]. In this paper a Barrage jammer is added, influenced by a Rayleigh modelled fading channel in addition to the WCDMA signal. Barrage jamming is the process of noise addition to the whole signal spectrum, not only for a narrow area. The simulations are made for 1 W and 5 W effective radiated power of the Barrage jammer.

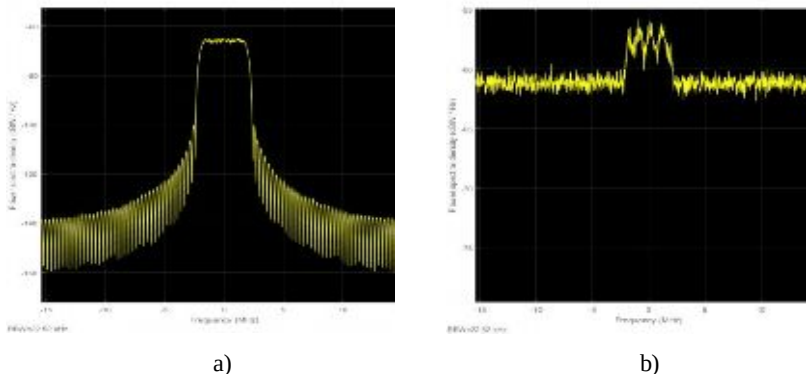


Figure 1 – Pure WCDMA spread spectrum signal without added noise (a) and the same signal affected by multipath propagation and AWGN (b).

Having implemented the properties of a WCDMA Downlink signal in a simulation model [9], an upgrade with jamming signal and multipath communication channel was created. The generated figure 1 represents the occupied bandwidth in the transmitter output and the result at the receiving antenna. These results were obtained by a series of simulations using the modified simulation model of the communication system.

Most important settings in the upgraded model are the Barrage jammer effective radiated electromagnetic power and the Rayleigh multipath channel settings. The jammer was chosen to have two powers: 1 W and 5 W ERP. Effective radiated power differs from the peak power as it is known from the theory of signals and systems [7]. In this paper for the Rake receiver we have chosen two enable fingers and two rays of the multipath propagation. One is the direct LOS ray and the other is 976.10^{-9} s delaying. The average power of Rx signals is 0 and 10 dB respectively. A Doppler frequency change is predicted for the receiving terminal speed of 3 km/h. The block error rate (**BLER**), the Dedicated Traffic Channel BER (**DTCH BER**) and the Dedicated Control Channel (**DCCH BER**) are calculated over simulation.

Figure 2 - WCDMA model [9] upgraded with Barrage jammer and multipath channel.

The results are obtained in the sense of a bit error probability. Table one and table two shows the results for 1 W and 5 W ERP of wideband jamming signal.

E_s/N_0 [dB]	BLER	DTCH BER	DCCH BER
3	0.009615	0.003096	0.0001449
6	0.004878	0.002872	0
7	0.003636	0.001693	0
9	0.004525	0.00072	0
12	0	0	0
15	0	0	0
18	0.01914	0.001112	0.0008696
20	0.02917	0.002905	0.00278
22	0.02966	0.003268	0.001795
25	0.9242	0.4476	0.446

In the table above an optimal Signal-to-Noise ratios are shown to be between 12 and 15 dB. It is assumed that SNR lower than 12 dB causes high error rate and link drop. SNR levels above 15 shows a phenomenon of overloading the antenna gain. Thus, ratios around 12 to 15 dB are provided as optimal for this radio environment case.

On the next table the results for 5 Watt ERP jamming signal are written. For detailed instruction, a next column is entered into: a simulated time column. In this field, the radio receiving simulated time is presented.

Table 2. BER Performance for 5 W ERP Barrage jammer

E_s/N_0 [dB]	BLER / bl. counts	DTCH BER	DCCH BER	Simulated time
0	0.01877 / 373	0.005547	0.007419	5 sec
3	0.010720 / 373	0.003358	0.002984	5 sec
6	0.009358 / 748	0.003967	0.002008	10 sec
7	0.008043 / 373	0.001992	0.001210	5 sec
9	0.005362 / 373	0.001827	0.001694	5 sec
12	0.008043 / 373	0.002666	0	5 sec
15	0.010720 / 373	0.026830	0.0009677	5 sec
18	0.018770 / 373	0.002732	0.004919	5 sec
20	0.04826 / 373	0.006896	0.003065	5 sec
22	0.19030 / 373	0.024110	0.03476	5 sec

Subject of research in this paper was WCDMA downlink channel BER performance in jammed radio environment. The WCDMA radio system with its DSSS signal has a threshold BER value of 10^{-3} . The results in the tables above show that this threshold is achieved at SNR of 11 dB for 1 W ERP jamming signal. For just 5 W ERP jamming signal even SNR of 18 dB couldn't achieve the specified threshold because of overloading the antenna gain. As it is seen, 5 W effective radiated noise jamming power is enough to jam the receiver at the receiver location.

REFERENCES

1. W. Ye and A. M. Haimovich, "Performance of Cellular CDMA with Cell Site Antenna Arrays, Rayleigh Fading and Power Control Error," IEEE Transactions on Communications, vol. 48, no. 7, pp. 1151-1159, July 2000
2. B. Hashem and E. S. Sousa, "On the Capacity of Cellular DS/CDMA Systems under Slow Rician/Rayleigh-Fading Channels," IEEE Transactions on Vehicular Technology, vol. 49, no. 5, pp. 1752-1759, Sep. 2000
3. Yang Qi Shi Haoshan, Han Zhongxiang, "Analysis of BER for Mc-CDMA with effect of Multipath" China, Vol.2, pp 136-140, ICEMI 2007
4. L. B. Milstein, T. S. Rappaport, R. Barghouti, "Performance Evaluation for Cellular CDMA," IEEE Journal on Selected Areas in Communications, vol. 10, no. 4, pp. 680-689, May 1992
5. O. K. Tonguz, M. M. Wang, "Cellular CDMA Networks Impaired by Rayleigh Fading: System Performance with Power Control," IEEE Transactions on Vehicular Technology, vol. 43, no. 3, pp. 515-527, Aug. 1994

6. S. W. Oh, K. L. Cheah, "Forward-Link BER Analysis of Asynchronous Cellular DS-CDMA over Nakagami-Faded Channels Using Combined PDF Approach," IEEE Transactions on Vehicular Technology, vol. 49, no. 1, pp. 173- 180, Jan. 2000
7. A. Oppenheim, „Signals and systems“, Prentice Hall 1983, ISBN 9540301475
8. J. Proakis, „Digital Communications“ – 5th ed., McGraw Hill, '08 ISBN 9780072
9. www.mathworks.com Copyright 2006-2014 The MathWorks, Inc.

SOCIAL SCIENCE

Г. Петков, М. Митевска

ИЗБОРЪТ НА КАРИЕРА КАТО ФУНКЦИЯ НА ЛИЧНОСТТА

Георги Петков, Майяна Митевска

Институт за научни изследвания и обучение на докторанти при УниБИТ

CHOOSING A CAREER AS A FUNCTION OF THE PERSONALITY

Georgi Petkov, Mayana Mitevska

Summary: *This study tracks the effects of the "Big Five" personality on career orientation in the "Big Six" model. For the purpose of the study, adapted and standardized questionnaires by H. Niebecken and colleagues for career guidance (Nybakken et al., 2003) and the model of P. Costa and R. McKruiy for the Big Five (Big 5) were used. The study was conducted on a sample of 262 people aged between 14 and 45 years. Data analysis reveals the specific combination of personality traits that predetermine the individual's orientation to a particular career type.*

Keywords: *career preferences, personality traits in the "Big Five"*

Традиционните разбириания за избор на кариера и кариерно израстване в една организация се сменя с кариера без граници (Arthur & Rousseau, 1996⁴⁰) и с разбиране за многообразната кариера (Hall, 1996), които стават широко признати. Кариерата е разглеждана в контекста на премахване на обхвата на традиционните граници, като например ограничения от работодателя, ограничения в работата поради нуждата от функции и умения на специалист, както и социалните ограничения, отделящи платената заетост от семейните позиции.

„Многообразната кариера е процес, който се управлява от индивида, а не от организацията. Той включва всички различни видове опит, които човек придобива по време на образованието си, допълнителното обучение, работата в различни организации, промените в естеството на работа и т.н. Многообразната кариера не е това, което става с човека в рамките на коя да е организация. Собствените многообразни кариерни избори и търсенето на себереализация са обединяващите или интегриращите елементи в живота на човека. Накратко, многообразната кариера е повече продукт на моделиране от самия човек, отколкото на организацията и може в различни периоди да бъде пренасочвана, за да отговори на

⁴⁰ Arthur, M., B., Rousseau, D., M. (1996). A career lexicon for the 21st century. *Academy of Management Executive*, 10 (4), 28-39.

специфичните потребности на индивида” Hall, D. T., & Mirvis, P. H. (1996)⁴¹. От една страна, кариерата се възприема като движение, напредък, развитие: „занимания, или професии; особено такива, изискващи специално образование”, или като „професионален успех”, „бързо израстване” (Stein е1 а1. 199642). От друга страна, се свързва с професионалните умения. Така при определянето на понятието „кариера“, освен обективни аспекти се включват и вътрешни (субективни), което се утвърждава с определението на Е. Шайн, който описва вътрешните аспекти на кариерата – нагласите, потребностите, ценностите и възприятията, които човек има за кариерата си, онези „теми и концепции, които човек развива и които имат смисъл за самата личност и нейните стремежи по отношение на работата”, като едновременно с това съществена роля се отделя на социалната среда във връзка с развитието на Аз-концепцията и по-доброто самопознание, които могат да помогнат на хората да правят по-добър избор за кариерата си (Stein е1 а1., 199043; Stephens, 1994).

Изборът на кариера като израз на личността се отразява в теоретичния подход на Дж. Холанд, според който личността е продукт едновременно на генетичните, социалните и психологическите характеристики, като по този начин обобщава разбиранията на Ф. Парсънс и А. Ру в същото време неговата теория за сходствата между човек и работна среда е една от най-въздействащите и използваните при кариерното консултиране. Тази логика на изследователя се основава на твърдението, че: „Ако професионалните интереси са израз на личността, тогава вътрешното проявление на личността е следването на тези вътрешни интереси” (Holland, 197344).

В тази перспектива основното допускане в изследването е, че личностните измерения по модела на „Големите пет“ могат да имат директен и индиректен ефект върху кариерните стремежи на младите хора

Първият въпросник е създаден от Ч. Нийбакен, Г. Сийгъл и К. Ферлацо (Nybakken, Siegel, Ferlazzo, 2003), адаптиран за и стандартизиран за българската социокултурна среда от С. Карабелъова (Карабелъова, 201545). Методът отчита кариерните предпочитания и се основава на теоретичния модел на Джон Холанд за „Големите шест“. Въпросникът се състои от 48 твърдения с четиристепенна скала за оценка от Ликъртов тип, която варира от „Изобщо не се отнася до мен“ до „Напълно се отнася до мен“.

Примерни твърдения на скалата за реалистичния тип личност са: „За мен е важно да имам атлетично тяло”, „Обикновено мога да се справям с майсторенето на нещата сам”, „Обичам да купувам практични неща, които мога да доизмайстора след това” и др.

⁴¹ Hall, D. T. (1996). Protean careers of the 21st century. *Academy of Management Executive*, 10(4), 8-16.

⁴² Schein, E. H. (1996). Career anchors revisited: Implications for career development in the 21st century. *Academy of Management Executive*, 10(4), 80-88.

⁴³ Schein, E., H. (1990). Career stress in changing times: Some final observations. *Prevention in Human Services*, 8(1), 251-261.

⁴⁴ Holland, J., L. (1973). *Making Vocational Choices: A Theory of Careers*. Englewood-Cliffs: Prentice-Hal.

⁴⁵ Карабелъова, С. Избор на кариера. Межкултурни и вътрекултурни сравнения. Класика и стил. 2015

Втората скала обединява твърдения, които определят изследователския тип личност. Те са от типа - „Имам нужда напълно да разбирам нещата“, „Харесва ми разговорите да бъдат интелектуално стимулиращи“, „Любопитен съм за това как е устроена природата“ и др.

В третата скала попадат твърдения, които описват артистичния тип хора. Примерни твърдения са: „Харесвам красивата обстановка, като цветовете и дизайнът значат много за мен“, „Обичам да изпробвам нови креативни идеи“, „Когато творя, съм склонен да не обръщам внимание на нищо друго“ и др.

Четвъртата скала определя социалния тип и включва твърдения като: „Хората обогатяват живота ми и му дават смисъл“, „Често мога да усетя, когато човек има нужда да поговори с някого“, „Хората често споделят с мен проблемите си“ и др.

Твърденията в петата скала описват предприемчивия тип личност. Примерните твърдения, които се отнасят към него са: „Уверен съм, че мога да направя нещата, които искам“, „За да имаш успех, трябва да се целиш на високо“, „Обичам да се пазаря“ и др.

Твърденията, които се включват в шестата скала, описват конвенционалния (традиционния) тип личност и са напр.: „Имам нужда от ясни инструкции, за да изпълня правилно нещата“, „Не обичам да съм отговорен за важни решения“, „Необходимо е да знам какво точно очакват хората от мен“ и др.

Вторият въпросник е създаден от М. Паркисън и се основава на теоретичния модел на П. Коста и Р. Маккрий за Големите пет (Big 5) характеристики на личността, адаптиран за български условия от С. Карабелюва (Миланов, Карабелюва, 201146). В оригиналния вариант той включва осемдесет и осем твърдения с дихотомна скала за отговори. При използването на въпросника в български условия е избран вариант, в който всяко твърдение се оценява с четиристепенна скала за оценка тип „Ликерт“, която варира от „изобщо не се отнася до мен“ до „напълно се отнася до мен“. М. Паркисън определя шест измерения, като пет от тях измерват големите пет фактора за личностните черти по теоретичния модел на П. Коста и Р. Маккрий, а шестото оценява социалната желателност.

При прилагането на въпросника в българската социокултурна среда напълно се потвърждава петфакторната структура и високата вътрешна консистентност на всяка една от скалите (Karabeliova, Petrov, Milanov, Ivanova, 201247). Първият фактор с най-голям процент на обяснена вариация е емоционална стабилност – лабилност/невротизъм (15,70; $\alpha=0,740$), вторият фактор е интроверсия – екстроверсия (14,50; $\alpha=0,740$), като трети фактор се оформя закритост – откритост към нов опит (11,45; $\alpha=0,742$), четвъртата скала е нецеленасоченост – целенасоченост (8,05; $\alpha=0,664$) и последният фактор е конкурентност – сътрудничество (7,59; $\alpha=0,649$). Общият процент на обяснена вариация е 57,29. Оценките по петте скали варират от 4 до 20, като ниските стойности (4-12) са

⁴⁶ Карабелюва, С. Избор на кариера. Межкултурни и вътрекултурни сравнения. Класика и стил. 2015

Миланов, М., Карабелюва, С. Негативни нагласи към ромското малцинство и взаимовръзката им с патриотизма и самооценката в български контекст. В: Българско списание по психология, с. 387-393.

⁴⁷ Karabeliova, S., Petrov, D., Milanov, M., Ivanova, E. (2012) Personality Dimensions and Risky Social and Health Behaviour. In: 26 Health Psychology Society.

индикатор за: интроверсия, конкурентност, нецеленасоченост, емоционална стабилност, закритост към нов опит (неоткликване на нововъведенията, съпротива срещу промените), докато високите стойности (13-20) показват екстраверсия, сътрудничество, добросъвестност (целенасоченост), невротизъм (емоционална нестабилност), откритост към нов опит.

В края на въпросниците изследваните лица са помолени да попълнят някои демографски данни като: пол, възраст, местоживеене, училище/университет, необходими за сравнителните анализи.

Изследването е проведено в периода септември 2016 - май 2017 г. и включва общо 262 души - ученици (152 души) и студенти (110 души), от София. От респондентите 61% са жени, а 39% - мъже. Учениците са между 15 и 19-годишна възраст, от 9 до 12 клас. Студентите са на възраст от 20 до 25 години. Изследваните лица са разпределени в три възрастови групи: 15-16-годишни (36 души), 17-18-годишна възраст (84 души) и 19-годишни (32 души). Анкетиранияте ученици са предимно от професионални гимназии, а студентите са основно от специалности на точните науки.

Анализът на данните разкрива уникалното участие на личността при формирането на кариерния тип. Нещо повече, някои автори интерпретират „Големите шест“ като кариерен личностен тип, т.е. като особена констелация от определени личностни черти, които са предпоставка за ориентиране на индивида към определен кариерен тип. Настоящото изследване потвърди тези твърдения (вж. табл.).

Таблица 1. Влияние на личността върху избора на кариера

Черти	Кариерни типове			
	R ²	Beta	T	p
Реалистичен				
Сътрудничество	.24	-.20	-3.05	.003
Изследователски				
Целенасоченост	.43	.30	4.73	.000
Откритост		.26	4.22	.000
Артистичен				
Невротизъм	.41	-.13	-2.14	.033
Откритост		.29	4.76	.000
Социален				
Екстраверсия	.53	-.22	-3.85	.000
Сътрудничество		.51	9.00	.000
Невротизъм		-.18	-3.29	.001
Откритост		-.11	-1.93	.050
Предприемчив				
Екстраверсия	.41	.40	6.60	.000

Традиционен				
Целенасоченост	.56	.57	9.90	.000
Невротизъм		-.10	-1.94	.050
Откритост		-.11	-2.04	.043

Регресионният анализ очерта посочените по-горе констелации от личностни черти. Изявената склонност към сътрудничество, например, ориентира индивидите към реалистичен и социален кариерен тип. За да се реализира оптимално в професионалните си прояви в рамките на социалния кариерен тип обаче, индивидът трябва да е в по-голяма степен интровертиран, емоционално стабилен, открит за опита и с добър самоконтрол върху социалните си контакти.

Изследователският тип и традиционният тип като кариерни прояви са по-привлекателни и по-подходящо поле за изява за индивидите, които в по-голяма степен от останалите са целенасочени и открити за опита.

По-откритите и търсещи нов социален опит индивиди, както и емоционално стабилните типове се ориентират към артистичния кариерен тип.

Към предприемчивия кариерен тип биха се насочили индивиди, които са по-силно ориентирани към интензивни контакти с хората от социалното обкръжение.

В обобщение на анализа, може да се каже, че както вродените, така и придобитите в процеса на социализацията черти на личността, оказват директно въздействие върху кариерния избор на индивида и активно участват в изграждането и реализацията на жизнените му планове. Непременно следва да се добави, че на обсъжданите тук личностни черти следва да се гледа само като на един, макар и ключов фактор при кариерния избор. Личността е само предпоставка, а останалото е образование, възпитание, квалификация, които, като се основават върху предпоставката, изграждат добрия професионалист.

Използвани източници

Александров, П. (1987). Професионалното самоопределяне на личността, София: народна просвета.

Иванова, Е. (2011). Взаимовръзка между Интернет зависимости и благополучие. Сборник по Клинична и консултативна психология. София: ИК „Стено“, 2011.

Иванова, Е., Карабелова, С. Киберхондрия и психологическо благополучие. // В: Сборник по Клинична и консултативна психология. София: ИК „Стено“, 2012.

Карабелова, С, Силгиджиян, Х. (2005) Приемственост и промяна на ценностите и културните практики в България. Сборник научни доклади. III Национален конгрес по психология. София: Софи-Р. с.305-309.

Карабелова, С. Избор на кариера. Межкултурни и вътрекултурни сравнения. Класика и стил. 2015

Карабелова, С., Андреева, Л. Саморегулативни механизми и нагласи за труд в ранна зрялост. // Годишник на СУ „Св. Кл. Охридски“, кн. „Психология“, т. 93, УИ „Св. Кл. Охридски“, С., 2008, 147-179.

Карабелова, С., Дорева, Д. Психологически аспекти на кариерния избор.// Годишник на СУ „Св. Кл. Охридски“, кн. „Психология“, т. 102, УИ „Св. Кл. Охридски“, С., 2011.

Карабелова, С., Поборникова, Г., Консулова, Д. Кариерните ориентации от модела

на „Големите шест „върху депресивните симптоми, тревожността и стреса, Leadership and Organizational Behavior, Sofia: Sofia, University “St. Kl. Ohridski”, 1168-1178.

Карастоянов, Г., Илиева, С. (2009). Структура и управление на конфликти. В: „Военна психология и лидерство“. ВА „Г.С. Раковски“.

Маркова, А.К. Формирование мотивации учения в школьном возрасте. М.: Просвещение, 1983.

Маслоу, Е. (2010). Мотивация и личност. София: Кибеа.

Миланов, М., Карабелова, С. Негативни нагласи към ромското малцинство и взаимовръзката им с патриотизма и самооценката в български контекст. В: Българско списание по психология, с. 387-393.

Силгиджиян, Х. (1998). Аз-концепцията и психосоциална идентичност. Живненият преход към зрелостта. София: Софийския университет "Св. Кл. Охридски", с. 35.

Силгиджиян, Х., Карабелова, С., Герганов, Е. (2006). Нарастващата несигурност в България: новата „котва“ на националната култура. Годишник на Софийския университет, кн. Психология, Т. 99. София: Университетско издателство „Св. Кл. Охридски“, (с. 19-34).

Силгиджиян, Х., Карабелова, С., Герганов, Е. (2003). Културна идентичност и ценности избори в контекста на всекидневното поведение. Годишник на СУ "Св. Кл. Охридски" кн. Психология, Т. София: "Св. Кл. Охридски", с. 5-50.

Силгиджиян, Х., Карабелова, С., Герганов, Е. (2011). Нарастващата несигурност в България: новата „котва“ на националната култура (сравнително-кохортно изследване на ценностите и културните практики по методологията на Х. Хофстеде 2000-2005 г.). Годишник на СУ „Св. Кл. Охридски“, кн. „Психология“, т. 101, София: УИ „Св. Кл. Охридски“, 5-36.

Силгиджиян, Х., Карабелова, С., Герганов, Е., Генов, Ю. (2007). Подобни и различни в рамките на българската култура (Резултати от представително изследване на ценностите и културните практики в България). Годишник на СУ „Св. Кл. Охридски“, кн. „Психология“, т. 96, №1, София: УИ „Св. Кл. Охридски“, 5-74.

Стоянова, Д., Цекова, С. современные университетские образовательные подходы к защите культурного наследия во время военно-политических кризисов. - В: Сборник материалы XI международной научно-практической конференции Фундаментальные и прикладные науки сегодня 10-11 апреля 2017 г. North Charleston, USA, с. 3-9, ISBN: 978-1545477830

Andrews, Frank M., Withey, Stephen B. Social Indicators of Well-Being Americans' Perceptions of Life Quality. ISBN 978-1-4684-2253-5 <http://www.springer.com/us/book/9781468422559>

Athanasou, J. (2002). Vocational Pathways in the early part of a career: An Australian Study, *The Career Development Quarterly*, 51 (1), 78-86.

Bandura, A., Barbaranelli, C., Caprara, G., V., & Pastorelli, C. (1996). Multifaceted impact of self-efficacy beliefs on academic functioning. *Child Development*, 67, 1206-1222.

Bandura, A., Barbaranelli, C., Caprara, G., V., and Pastorelli, C. (January/ February, 2001). Self-Efficacy Beliefs as Shapers of Children's Aspirations and Career Trajectories. *Child Development, Volume 72, N1*, p. 187- 206.

Greenberg, J., Baron, R. A. (2003) Behavior in organizations : understanding and managing the human side of work / - 8th ed. Upper Saddle River, NJ : Prentice Hall, 691 p.

Grimland, S., Vigoda-Gadot, E., & Baruch, Y. (2011). Career attitudes and success of managers: The impact of chance event, protean, and traditional careers. *The International*

Journal of Human Resource Management, 23(6), 1074-1094.

Guay F., Chanal J., Ratelle C.F. et al. Intrinsic, identified and controlled types of motivation for school subjects in young elementary school children // *Brit. Journal of Educational Psychology*. 2010. Vol. 80. P. 711—735.

Gubler, M., Arnold, J., Coombs, C. (2014). Reassessing the protean career concept: Empirical findings, conceptual components, and measurement. *Journal of Organizational Behavior*, 35, 23-40.

Hampson, S., Goldberg, L.R., Vogt, T.M. & Dubanoski, J.P. (2006). Forty years on: Teachers' assessments of children's personality traits predict self-reported health behaviors and outcomes at midlife. *Health Psychology*, 25(1), 57–64.

Hansen, S. (2000). *Preparing counselors for career development in the new millennium: ACES/NCDA position paper*. Retrieved October 22, 2007, <http://www.ncda.org/pdf/CommissionPaper.pdf>

Hinkelman, J.M. & Luzzo, D.A. (2007). Mental health and career development of college students. *Journal of Counseling & Development*, 85, 143-147.

Hirschi, A. & Hermann, A. (2012). Vocational identity achievement as a mediator of presence of calling and life satisfaction. *Journal of Career Assessment*, 20, 309–321.

Inkson, K. (2006). Protean and boundaryless careers as metaphors. *Journal of Vocational Behavior*, 69(1), 48-63.

Inkson, K., Gunz, H., Ganesh, S., & Roper, J. (2012). Boundaryless careers: Bringing back boundaries. *Organization Studies*, 33(3), 323-340.

Karabeliova, S., Ivanova, E. Do personality traits lead to cyberchondria and what are the outcomes for well-being? // To be presented at the 28th Conference of the European Health Psychology Society Beyond prevention and intervention: increasing well-being, Innsbruck, Austria, 2014

Karabeliova, S., Ivanova, E. Health anxiety, cyberchondria and well-being. // Presented at The 23rd Biennial Meeting of the International Society for the Study of Behavioural Development, Shanghai, China, 07–12.07.2014

Karabeliova, S., Ivanova, E., Mitev, K. Is Facebook Use Associated with Depression, Anxiety,

Karabeliova, S., Petrov, D. Personality traits, eating and alcohol attitudes as predictors of well-being of young adults. 27th conference of the European Health Psychology Society: "Well-being, Quality of Life and Caregiving", July, Bordeaux, 2013.

Karabeliova, S., Petrov, D., Milanov, M., Ivanova, E. (2012) Personality dimensions and risky social and health behaviour. EHPS 2012 abstracts, *Psychology & Health*, 27:sup1,p.240.

Karabeliova, S., Petrov, D., Milanov, M., Ivanova, E. (2012) Personality Dimensions and Risky Social and Health Behaviour. In: 26 Health Psychology Society

Komaraju M., Karau S., Schmeck R. Role of the Big Five personality traits in predicting college students' academic motivation and achievement. *Learning and Individual Differences*, 2009, 19(1), 47–52.

Lee K., Ashton M.C. The Dark Triad, the Big Five, and the HEXACO model. *Personality and Individual Differences*, 2014, Vol. 67, 2–5.

Lopez, S. J., & Snyder, C. R. (2003). *Positive psychological assessment: A handbook of models and measures*. Washington, DC: American Psychological Association.

Lounsbury, J. W., Hutchens T. and Loveland, J. M. (2005). An Investigation of Big Five Personality Traits and Career Decidedness among Early and Middle Adolescents. *Journal of Career Assessment*, 13 (1), 25-39.

Martincin, K. M. and Stead, G. B. (2015). Five-Factor Model and Difficulties in Career Decision Making: A Meta-Analysis. *Journal of Career Assessment*, 23, 3-19.

McCrae RR, Costa PT. The stability of personality: Observation and evaluations. *Current Directions in Psychological Science*. 1994; 3: 173–175.

McCrae, R. R., & Costa, P. T. Jr. (1999). A five-factor theory of personality. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (2nd ed., pp. 139-153). New York/London: Guilford Press.

McCrae, R. R., & Costa, P. T. Jr. (1999). A five-factor theory of personality. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (2nd ed., pp. 139-153). New York/London: Guilford Press.

McCrae, Robert R., Paul T. Costa Personality in Adulthood: A Five-factor Theory Perspective Guilford Press, 2003. 268 p.ISBN 1572308273.

Morf C.C., Weir Ch., Davidov M. Narcissism and Intrinsic Motivation: The Role of Goal Congruence. *Journal of Experimental Social Psychology*, 2000, 36(4), 424–438.

Nagler U.K., Reiter K.J., Furtner M.R., Rauthmann J.F. Is there a “dark intelligence”? Emotional intelligence is used by dark personalities to emotionally manipulate others. *Personality and Individual Differences*, 2014, Vol. 65, 47–52.

Nybakken, Ch., Siegel, G., Ferlazzo. C. (2003). *Merging Two Worlds. Transition/Career Planning*. Arizona: Arizona Department of Education.

Parris, G. P., Owens, D., Johnson, T., Grbevski, S., Holbert-Quince, J. (2010). Addressing the Career Development Needs of High-Achieving African American High School Students: Implications for Counselors. *Journal for the Education of the Gifted*. Vol. 33, No. 3, pp. 417-43.

Phillips P., Abraham C., Bond R. Personality, cognition, and university students' examination performance. *European Journal of Personality*, 2003, 17(6), 435–448.

Porter, Lyman W., Gregory Bigley, Richard M. Steers. *Motivation and Work Behavior*. 7th ed. New York, McGraw-Hill, 2002. (March 2013) <[http://\(www.referenceforbusiness.com/management/Mar-No\(Motivation-and-Motivation-Theory.html#ixzz2XqxgOzrg\)](http://(www.referenceforbusiness.com/management/Mar-No(Motivation-and-Motivation-Theory.html#ixzz2XqxgOzrg)>.

Positive education: Positive psychology and classroom interventions / M.E.P. Seligman, R.M. Ernst, J. Gillham et al. // *Oxford Review of Education*. – 2009. – Vol. 35. – P. 293–311.

Positive Psychology Progress: Empirical Validation of Interventions / M.E.P. Seligman, T.A. Steen, N. Park, C. Peterson // *American Psychologist*. – 2005. – Vol. 60. – No. 5. – P. 410–421.

Posner, M. I., & Rothbart, M. K. (2000). Developing mechanisms of self-regulation. *Development and Psychopathology*, 12, 427–441.

Prediger, D., J. (2000). Holland's hexagon is alive and well - thought somewhat out of shape: Response to Tinsley. *Journal of Vocational Behavior*, 54, 197-204.

Ratelle C.F., Guay F., Vallerand R.J. et al. Autonomous, controlled, and amotivated types of academic motivation: A person-oriented analysis // *Journal of Educational Psychology*. 2007. Vol. 99. P. 734—746.

Roberti, J. W., Fox, D. J., & Tunick, R. H. (2003). Alternative personality variables and the relationship to holland's personality types in college students. *Journal of Career Assessment*, 11, 308-327.

Ryan R., Deci E. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being // *American Psychologist*. 2000. V. 55. P. 68–78.

Savickas, M. L. (2011). New Questions for Vocational Psychology: Premises, Paradigms,

and Practices. *Journal of Career Assessment*, 19(3), 251-258.

Savickas, M. L., Nota, L., Rossier, J., Dauwalder, J.-P., Duarte, M. E., & Guichard, J. (2009). Life designing: A paradigm for career construction in the 21st century. *Journal of Vocational Behavior*, 75(3), 239-250.

Savickas, M., L. (2002). Career Construction. A Developmental Theory of Vocational Behavior. In: Brown, D. (Ed.) (2002). *Career Choice and Development*. San Francisco: Jossey-Bass.

ЛИЧНОСТНИ ПРОЕКЦИИ ВЪРХУ УДОВЛЕТВОРЕНОСТТА ОТ ЖИВОТА

Георги Петков, Майяна Митевска

Институт за научни изследвания и обучение на докторанти при УниБИТ

PERSONAL PROJECTIONS ON LIFE SATISFACTION

Georgi Petkov, Mayana Mitevska

Summary: *This study tracks the effects of the personality on life satisfaction. The relationship of the person with the feeling of happiness has also been studied. For this purpose, the adapted questionnaire to measure the "Big Five," the scale of subjective well-being of Pavot, WG, Diener, E., Colvin, CR, & Sandvik, E. (1991) and Subjective Happiness Scale - SHS - Scale of Subjective Happiness - Lyubomirsky & Lepper, 1999). The study was conducted on a sample of 262 students, students and students. The results show.*

Keywords: *Big 5, life satisfaction, happiness*

Стабилната представа на човека за собствените му характеристики, интереси, способности, умения и опит е от голямо значение както за формулиране на жизнено цели и бъдещи планове, така и за обема и сложността на задачите, чието изпълнение води до постигането им. Изравняването на планираните и положени усилия с получените резултати води до определено ниво на удовлетвореност, което се преживява като щастие.

Липсата на удовлетвореност и щастие произтича от критичното разминаване между желано състояние и получен резултат. Разминаването от своя страна би могло да се дължи на неадекватната представа за себе си, която се вгражда в основата на наивните бъдещи планове на индивида. Връзката на щастието и удовлетвореността от живота с положените лични усилия и изразходваните индивидуални ресурси може да се проследи в различни проучвания (Boehm & Lyubomirsky, 2008⁴⁸). Успехите при реализирането на жизнените планове увеличават мотивацията за повишаване на личностния потенциал и квалификацията. И така идентифицирането с високите нива на този потенциал, т.е. постигането на пълна идентичност с предизвикателните задачи, се превръща в предпоставка на удовлетвореността от живота (Hirschi & Hermann, 2012⁴⁹). Въпреки многобройните публикации все още остава открит въпросът за връзката между удовлетвореността от живота и факторите, които я предизвикват. Теоретичният обзор по темата позволява да се допусне, което е проверено и емпирично, че чертите на личността са във взаимовръзка с удовлетвореността от живота и субективното усещане за щастие. Личностното

⁴⁸ Boehm, J.K. & Lyubomirsky, S. (2008). Does happiness promote career success? *Journal of Career Assessment*, 16 (1), 101-116.

⁴⁹ Hirschi, A. & Hermann, A. (2012). Vocational identity achievement as a mediator of presence of calling and life satisfaction. *Journal of Career Assessment*, 20, 309-321.

благополучие на човека обикновено се свързва с принципите на целостта и йерархията на потребностите, като включва афективни, когнитивно-афективни и когнитивни компоненти.

С термина щастие С. Любомирски определя преживяването на радост, удовлетворение или благополучие в съчетание с усещането, че животът е хубав, че той има смисъл и щатието се състои в това, животът да се живее. Учените предпочитат термина благополучие, защото той им се струва по-научен и не носи излишна натовареност. С. Любомирски ги приема като синоними. Според нея не съществува термометър на щатието и затова изследователите обикновено разчитат на самооценката на изследваните лица.

Изследването е проведено в периода септември 2016 - май 2017 г. и включва общо 262 души на възраст от 15 до 45 години. От респондентите 61% са жени, а 39% - мъже.

За целите на изследването са приложени редица статистически методи: дескриптивна статистика, t-тест, корелационен анализ. Данните са обработени с IBM SPSS Statistics 21.

Използвана е комбинация от следните въпросници:

Първият въпросник е създаден от М. Паркисън и се основава на теоретичния модел на П. Коста и Р. Маккрий за Големите пет (Big 5) характеристики на личността, адаптиран за български условия от С. Карабелова (Миланов, Карабелова, 2011:50). В оригиналния вариант той включва осемдесет и осем твърдения с дихотомна скала за отговори. При използването на въпросника в български условия е избран вариант, в който всяко твърдение се оценява с четиристепенна скала за оценка тип „Ликерт“, която варира от „изобщо не се отнася до мен“ до „напълно се отнася до мен“. М. Паркисън определя шест измерения, като пет от тях измерват големите пет фактора за личностните черти по теоретичния модел на П. Коста и Р. Маккрий, а шестото оценява социалната желателност.

Първото измерение „**Екстраверсия**“, включва твърденията, които описват дали човек е енергичен, активен и обичаш социалните събирания или е скромен и резервиран.

Втората дименсия, „**Сътрудничество**“, отговаря на фактора „Насоченост към другите“ от модела на П. Коста и Р. Маккрий. От смисъла на твърденията се определя дали хората са загрижени за околните, внимателни във взаимодействията си с другите хора и сътруднически или по-скоро се стремят да се съревновават и са ориентирани към конкуренция.

Четвъртото измерение, наречено „**Целенасоченост**“, отговаря на фактора „Добросъвестност“ от модела на П. Коста и Р. Маккрий. Тази дименсия описва хората като силно мотивирани, самодисциплинирани, чувствителни към детайлите или като хора със слаби стремежи към постижения, непринудени в поведението си и в известна степен неорганизирани и непоследователни.

Следващата дименсия е „**Невротицизм**“. Смисълът на твърденията позволява респондентите да бъдат описани като напрегнати и тревожни или като емоционал-

⁵⁰ Карабелова, С. Избор на кариера. Межкултурни и вътрекултурни сравнения. Класика и стил. 2015

Миланов, М., Карабелова, С. Негативни нагласи към ромското малцинство и взаимовръзката им с патриотизма и самооценката в български контекст. В: Българско списание по психология, с. 387-393.

но стабилни, уверени и справящи се в стресови ситуации.

Последната дименсия „Откритост към нов опит“ описва дали човек предпочита да действа по нетрадиционен начин и приема промените като предизвикателство или по-скоро е консервативен, практичен и предпочита познатото.

Изследвани са и демографски показатели като: пол, възраст, местоживеене, необходими за сравнителните анализи.

Вторият въпросник е създаден от Pavot, W. G., Diener, E., Colvin, C. R., & Sandvik, E. (1991)⁵¹ и измерва субективното благополучие. Скалата се състои от 5 твърдения, замислена да измерва общите мисловни преценки за удовлетвореността от живота (не само измерване на положителното или отрицателното влияние). Участниците отбелязват доколко са съгласни или не с всяко от петте твърдения като ползват скала от 7 точки (7 – „Напълно съгласен“ до 1 – „Напълно несъгласен“). Структурата на субективното благополучие е замислена като конструкт, състоящ се от два основни компонента: емоционален или още компонент на въздействието и оценъчен или още мисловен компонент (Diener, 1984⁵²; Veenhoven, 1984⁵³). Оценъчният компонент също така се свързва с удовлетворението от живота (Andrews & Withey, 1976⁵⁴). Въпреки, че компонентът на въздействието на субективното благополучие се радва на значително внимание от страна на изследователите, оценъчният компонент общо взето се пренебрегва. Скалата на удовлетвореност от живота (SWLS; Diener, Emmons, Larsen, & Griffin, 1985⁵⁵) е разработена като скала за измерване на оценъчния компонент на субективното благополучие (Pavot, & Diener, 1993⁵⁶). Скалата „Удовлетвореност от живота“ е разработена за оценяване на удовлетвореността от живота на участниците в проучването като цяло. Скалата не оценява удовлетвореността от области на живота като здравето или финансите, а позволява на участващите в допитването да интегрират и преценят тези области както намерят за добре като скалата показва и достатъчна чувствителност, за да бъде евентуално ценен източник за определяне на промени в удовлетвореността от живота по време на клинична намеса (Diener, Sandvik, Seidlitz, Diener, 1993⁵⁷).

Третият въпросник измерва щастието (Subjective Happiness Scale – SHS – скала на субективно щастие) и е създаден от С. Любомирски и Лепър (Lyubomirsky &

⁵¹ Pavot, W. G., Diener, E., Colvin, C. R., & Sandvik, E. (1991) Further validation of the Satisfaction with Life Scale: Evidence for the cross-method convergence of well-being measures. *Journal of Personality Assessment*, 57, 149-161.

⁵² https://internal.psychology.illinois.edu/~ediener/Documents/Diener_1984.pdf

⁵³ Veenhoven, R. Sociological theories of subjective well-being. Michael Eid & Randy Larsen (Eds). "The Science of Subjective Well-being: A tribute to Ed Diener", Guilford Publications, New York, 2008, ISBN 978-1-59385-581-9. pp. 44-61

⁵⁴ Andrews, Frank M., Withey, Stephen B. Social Indicators of Well-Being Americans' Perceptions of Life Quality. ISBN 978-1-4684-2253-5 <http://www.springer.com/us/book/9781468422539>

⁵⁵ Diener, E., Emmons, R. A., Larsen, R. J., & Griffin, S. (1985). The Satisfaction with Life Scale. *Journal of Personality Assessment*, 49, 71-75.

⁵⁶ Pavot, W. G., & Diener, E. (1993). Review of the Satisfaction with Life Scale. *Psychological Assessment*, 5, 164-172.

⁵⁷ Diener, E., Sandvik, E., Seidlitz L., Diener, M. (1993). The relationship between income subjective well-being: Relative or absolute? *Social Indicators Research*, 28, 195-223.

Lepper, 1999⁵⁸), адаптиран за българския социокултурен контекст (Ivanova et al., 2015) и е една от най-популярните методики за психологично оценяване на щастието. Тя е методика от скрийнингovo ниво на психологично оценяване, съдържа 4 айтема с петстепенна скала за оценка с високо ниво на надеждност ($\alpha=0,786$) и оценява общото субективно възприятие на щастието от даден човек. Като общата "философия" на методиката и конструкта "щастие", се основава на т.н. "субективен" подход, т.е. разглежда щастието не от "обективна" позиция (напр. количествено измеримо материално благополучие, доходи, здравен статус и др. под.), а разглежда щастието от гледна точка на субективното преживяване и оценка на самия респондент. Едно от най-силните влияния върху щастието оказват социалните взаимоотношения.

Високата надеждност и доказаната валидност на описаните по-горе инструменти позволи да се пристъпи към измерване и анализ на изследваните конструкти.

В изследването е потърсен отговор на въпроса в каква степен на изявеност и кои черти участват във формирането и преживяването на удовлетвореност от живота и усещането за щастие. Данните в следващата таблица ясно показват, че хората изпитват удовлетвореност когато имат възможността да се докоснат до нов опит, когато живеят с чувството, че взаимодействията със средата ги обогатяват. Свидетелство затова са групата изследвани лица, чийто балови стойности по оценената с приложения въпросник черта «Откритост към нов опит» е с по-високи стойности.

По отношение на удовлетвореността и усещането за щастие се оказва, че почти целият набор от измерени черти, с изключение на сътрудничеството и невротизма, участва в неговото формиране и изразяване. По-щастливи и удовлетворени от живота се чувстват екстравертите, силно мотивираните и самодисциплинираните, както и откритите към нов опит.

Таблица 1. Взаимовръзки между личностните черти, удовлетвореността и щастието

Черти	Екстраверсия	Сътрудничество	Целенасоченост	Невротизъм	Откритост към нов опит
Удовлетвореност	<u>.238**</u>	<u>.009</u>	<u>.118</u>	<u>-.096</u>	<u>.201**</u>
Щастие	<u>.000</u>	<u>.891</u>	<u>.058</u>	<u>.123</u>	<u>.001</u>
	<u>.356**</u>	<u>-.021</u>	<u>.252**</u>	<u>-.106</u>	<u>.256**</u>

⁵⁸ Lyubomirsky, S., & Lepper, H. (1999). [A measure of subjective happiness: Preliminary reliability and construct validation](#). Social Indicators Research, 46, 137-155. The original publication is available at www.springerlink.com.

<https://positpsych-bg.alle.bg>

	.000	.741	.000	.087	.000
--	------	------	------	------	------

Интерес представлява влиянието на личностните черти в зависимост от степента си на изразеност. Разделянето на изследваните лица на две групи по всяка от измерените черти на интроверти и екстраверти, на нецеленасочени и целенасочени, на емоционално стабилни и емоционално лабилни и на закрити за опита и открити за опита позволи да се получат данните, посочени в следващата таблица.

По отношение на удовлетвореността от живота се оказа, че статистически значими различия съществуват само по отношение на откритостта към опита. В по-висока степен се чувстват удовлетворени лицата, които са по-открити за опита.

По отношение на щастието данните показват, че между всички групи с различна изявеност на личностните черти съществуват статистически значими различия. В по-висока степен щастливи се чувстват екстравертите, емоционално стабилните и откритите към нов опит. Резултатите сочат, че значително по-щастливи се чувстват нецеленасочените индивиди. Това би могло да се дължи на възрастта, тъй като респондентите са доста млади. Но тъй като няма достатъчно теоретични основания да се подкрепи едно такова твърдение, очевидно е, че тази хипотеза следва да се провери в бъдещи изследвания.

Таблица 2. Различия в удовлетвореността от живота и щастие, в зависимост от изразеността на личностните черти

Черти	Нива	Удовлетвореност от живота				Щастие			
		M	SD	F	Sig.	M	SD	F	Sig.
Екстраверсия	Интроверти	18.40	3.91	.67	.410	13.89	2.83	6.06	.014
	Екстраверти	18.81	3.87			14.82	3.21		
Целенасоченост	Нецеленасочени	18.26	3.92	1.28	.258	18.51	3.87	8.58	.004
	Целенасочени	18.80	3.81			13.76	2.82		
Невротизъм	Стабилни	18.64	4.15	.28	.599	14.61	3.09	4.50	.035
	Лабилни	18.38	3.50			13.82	2.85		
Откритост към нов опит	Закрити	18.01	3.59	8.64	.004	13.77	2.33	14.02	.000
	Открити	19.45	4.22			15.18	3.77		

Най-значимият домейн в скалите за измерване на личността противопоставя емоционалната стабилност на невротизма. Общата тенденция да се преживяват негативни афекти като страх, тъга, притеснение, гняв, вина, отвращение, е същността на невротизма. Съдържанието на фактора “Невротизъм” обаче не се изчерпва с предразположеността към емоционален дистрес. Лицата с ниски стойности по

„Невротизъм“ са емоционално стабилни. Те обикновено са спокойни, способни да се справят в стресови ситуации, без да загубят самообладание.⁵⁹

Изследването показва, че личността е ключов фактор за постигане на удовлетвореност от живота и получаване на усещане за щастие. Не бива да се подценява възможността те да бъдат катализирани и от участието на други фактори, като емоционалния статус, средата, социалните отношения с приятели, близки и колеги. Твърде много са факторите, които влияят за оптималното функциониране на индивида. В настоящия доклад беше разгледан само един от тях, макар и един от най-важните.

Използвани източници

Александров, П. (1987). Професионалното самоопределяне на личността, София: народна просвета.

Бакрачева, М., В. Недева. Предизвикателства пред кариерното консултиране в условията на социални промени. Психологични изследвания 2009

Бакалова, Д., М. Бакрачева, Б. Мизова. Какво са щастieto, удовлетвореността от живота и благополучието за българина днес? Психологични изследвания 2010

Бакрачева, М. (2010). Влиянието на възрастта, пола и дохода върху удовлетвореността от живота и щастieto Психологични изследвания 2010

Бессонова, Ю.В. О структуре психологического благополучия / Ю.В. Бессонова // Психологическое благополучие личности в современном образовательном пространстве: сб. статей / Составитель: Ю.В. Братчикова. – Екатеринбург: Изд-во Урал. гос. пед.ун-та, 2013. – С. 30–35.

Джонев, С. Социална психология. Т. 5. Изследователски дизайн. Статистическа обработка. Интерпретация, Софи – Р, 2004, 315 с. ISBN – 954-638-127-6

Иванова, Е. (2011). Взаимовръзка между Интернет зависимост и благополучие. Сборник по Клинична и консултативна психология. София: ИК „Стено“, 2011.

Иванова, Е., Карабельова, С. Киберхондрия и психологическо благополучие. // В: Сборник по Клинична и консултативна психология. София: ИК „Стено“, 2012.

Карабельова, С., Поборникова, Г., Консулова, Д. Кариерните ориентации от модела на „Големите шест“ върху депресивните симптоми, тревожността и стреса, Leadership and Organizational Behavior, Sofia: Sofia, University “St. Kl. Ohridski”, 1168-1178.

Любомирский, С. Психология счастья. 2007, ЛитРес, Питер, с. 450, ISBN: 978-5-496-00719-1.

Маслоу, Е. (2010). Мотивация и личност. София: Кибеа.

Стоянова, Д., Цекова, С. современные университетские образовательные подходы к защите культурного наследия во время военно-политических кризисов. - В: Сборник материалы XI международной научно-практической конференции Фундаментальные и прикладные науки сегодня 10-11 апреля 2017 г. North Charleston, USA, с. 3-9, ISBN: 978-1545477830

Andrews, Frank M., Withey, Stephen B. Social Indicators of Well-Being Americans' Perceptions of Life Quality. ISBN 978-1-4684-2253-5
<http://www.springer.com/us/book/9781468422559>

⁵⁹ Bolger N, Schilling EA. Personality and problems of everyday life: The role of neuroticism in exposure and reactivity to daily stressors. Journal of Personality. 1991; 59:356–386.

Bandura, A., Barbaranelli, C., Caprara, G., V., & Pastorelli, C. (1996). Multifaceted impact of self-efficacy beliefs on academic functioning. *Child Development*, 67, 1206-1222.

Bandura, A., Barbaranelli, C., Caprara, G., V., and Pastorelli, C. (January/ February, 2001). Self-Efficacy Beliefs as Shapers of Children's Aspirations and Career Trajectories. *Child Development*, Volume 72, N1, p. 187- 206.

Bolger N, Schilling EA. Personality and problems of everyday life: The role of neuroticism in exposure and reactivity to daily stressors. *Journal of Personality*. 1991; 59:356–386.

Diener, E., Sandvik, E., Seidlitz L., Diener, M. (1993). The relationship between income subjective well-being: Relative or absolute? *Social Indicators Research*, 28, 195-223.

Diener, E.; Seligman, M. E. P. (2004). "Beyond money: Toward an economy of well-being". *Psychological Science in the Public Interest*. 5: 1–31. Doi:10.1111/j.0963-7214.2004.00501001.x

Hansen, S. (2000). *Preparing counselors for career development in the new millennium: ACES/NCDA position paper*. Retrieved October 22, 2007, <http://www.ncda.org/pdf/CommissionPaper.pdf>

Hinkelman, J.M. & Luzzo, D.A. (2007). Mental health and career development of college students. *Journal of Counseling & Development*, 85, 143-147.

Karabeliova, S., Ivanova, E. Do personality traits lead to cyberchondria and what are the outcomes for well-being? // To be presented at the 28th Conference of the European Health Psychology Society Beyond prevention and intervention: increasing well-being, Innsbruck, Austria, 2014

Karabeliova, S., Ivanova, E. Health anxiety, cyberchondria and well-being. // Presented at The 23rd Biennial Meeting of the International Society for the Study of Behavioural Development, Shanghai, China, 07–12.07.2014

Karabeliova, S., Ivanova, E., Mitev, K. Is Facebook Use Associated with Depression, Anxiety,

Karabeliova, S., Petrov, D. Personality traits, eating and alcohol attitudes as predictors of well-being of young adults. 27th conference of the European Health Psychology Society: "Well-being, Quality of Life and Caregiving", July, Bordeaux, 2013.

Karabeliova, S., Petrov, D., Milanov, M., Ivanova, E. (2012) Personality dimensions and risky social and health behaviour. EHPS 2012 abstracts, *Psychology & Health*, 27:sup1,p.240.

Karabeliova, S., Petrov, D., Milanov, M., Ivanova, E. (2012) Personality Dimensions and Risky Social and Health Behaviour. In: 26 Health Psychology Society

Komaraju M., Karau S., Schmeck R. Role of the Big Five personality traits in predicting college students' academic motivation and achievement. *Learning and Individual Differences*, 2009, 19(1), 47–52.

Lee K., Ashton M.C. The Dark Triad, the Big Five, and the HEXACO model. *Personality and Individual Differences*, 2014, Vol. 67, 2–5.

Lopez, S. J., & Snyder, C. R. (2003). *Positive psychological assessment: A handbook of models and measures*. Washington, DC: American Psychological Association.

Lounsbury, J. W., Hutchens T. and Loveland, J. M. (2005). An Investigation of Big Five Personality Traits and Career Decidedness among Early and Middle Adolescents. *Journal of Career Assessment*, 13 (1), 25-39.

Lyubomirsky, S. (2013). *The myths of happiness* (X, Trans.). Seoul, South Korea: Knowledge Nomad.

Lyubomirsky, S. (2013). *The myths of happiness: What should make you happy, but doesn't, what shouldn't make you hoxforappy, but does* (X, Trans.). Beijing, China: Cheers Books.

Lyubomirsky, S. (2014). *The myths of happiness* (X, Trans.). Tokyo, Japan: Nihon Jitsugyo Shuppan.

Lyubomirsky, S. (2015). *The myths of happiness*. (X, Trans.). Tel Aviv, Israel: Kinneret-Zmora.

Lyubomirsky, S., & Lepper, H. (1999). A measure of subjective happiness: Preliminary reliability and construct validation. *Social Indicators Research*, 46, 137-155. The original publication is available at www.springerlink.com.

Lyubomirsky, S., & Lepper, H. (1999). A measure of subjective happiness: Preliminary reliability and construct validation. *Social Indicators Research*, 46, 137-155. The original publication is available at www.springerlink.com.<https://positpsych-bg.alle.bg>

Parris, G. P., Owens, D., Johnson, T., Grbevski, S., Holbert-Quince, J. (2010). Addressing the Career Development Needs of High-Achieving African American High School Students: Implications for Counselors. *Journal for the Education of the Gifted*. Vol. 33, No. 3, pp. 417-43.

Patton, W. and Dee, A. B., and Creed, P. A. (2004). Gender differences for optimism, self-esteem, expectations and goals in predicting career planning and exploration in adolescents. *International Journal for Educational and Vocational Guidance*. 4(3), 193-209.

Patton, W. and Spooner-Lane, R. and Creed, P. (2005). Validation of the Short Form of the Career Development Inventory - Australian Version with a Sample of University Students. *Australian Journal of Career Development* 14(3), 49-59.

Phillips P., Abraham C., Bond R. Personality, cognition, and university students' examination performance. *European Journal of Personality*, 2003, 17(6), 435–448.

Porter, Lyman W., Gregory Bigley, Richard M. Steers. *Motivation and Work Behavior*. 7th ed. New York, McGraw-Hill, 2002. (March 2013) <[http://\(www.referenceforbusiness.com/management/Mar-No\(Motivation-and-Motivation-Theory.html#ixzz2XqgOzrg\)](http://(www.referenceforbusiness.com/management/Mar-No(Motivation-and-Motivation-Theory.html#ixzz2XqgOzrg)>.

Positive education: Positive psychology and classroom interventions / M.E.P. Seligman, R.M. Ernst, J. Gillham et al. // *Oxford Review of Education*. – 2009. – Vol. 35. – P. 293–311.

Positive Psychology Progress: Empirical Validation of Interventions / M.E.P. Seligman, T.A. Steen, N. Park, C. Peterson // *American Psychologist*. – 2005. – Vol. 60. – No. 5. – P. 410–421.

Torgersen, S. & Vollrath, M. (2006). Personality types, personality traits, and risky health behavior, In: Vollrath, M., E. (Ed.) *Handbook of Personality and Health*. New York: John Wiley & Sons, 215–234.

Torrington, D., Hall, L. & Taylor, S. (2005). *Human Resource Management*. (6th Ed.). London: FT/Prentice Hall.

Valcour, M., & Ladge, J. J. (2008). Family and career path characteristics as predictors of women's objective and subjective career success: Integrating traditional and protean career explanations. *Journal of Vocational Behaviour*, 73(2), 300-309.

Valenzuela, S., Park, N., & Kee, K. F. (2009). Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust, and participation1. *Journal of Computer-Mediated Communication*, 14(4), 875-901.

Vallerand R.J., Fortier M.S., Guay F. Self-determination and persistence in a real-life setting: Toward a motivational model of high-school dropout // *Journal of Personality and Social Psychology*. 1997. Vol. 72. P. 1161—1176.

Vossel, G. Stress conceptions in life event research: Towards a person-centre perspective. —*European Journal of Personality*, 1987. Vol. 1, pp. 123 -140.

Н. М. Петров,

**ИЗСЛЕДВАНЕ СТЕПЕНТА НА УДОВЛЕТВОРЕНОСТ НА КОМАНДИРИТЕ
НА ФОРМИРОВАНИЯ ЗА КОМУНИКАЦИОННО-ИНФОРМАЦИОННА
ПОДДРЪЖКА ОТ НИВОТО НА ИЗГРАДЕНИТЕ ПРОФЕСИОНАЛНИ
КОМПЕТЕНЦИИ В ОФИЦЕРИТЕ, ЗАВЪРШИЛИ СПЕЦИАЛИЗАЦИЯ
„ВОЕННИ КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ“**

Николай М. Петров

*Национален военен университет „Васил Левски“, факултет „Общовойскови“
nmpetrov@nvu.bg*

**STUDYING THE LEVEL OF SATISFACTION OF THE COMMANDERS OF
ENTITIES FOR COMMUNICATION AND INFORMATION MAINTENANCE
WITH REFERENCE TO THE LEVEL OF PROFESSIONAL COMPETENCES
DEVELOPED IN THE OFFICERS WHO HAVE COMPLETED
THE SPECIALIZATION “MILITARY COMMUNICATION AND
INFORMATION SYSTEMS”**

Nikolay M. Petrov

Abstract: *Indications of the successful functioning of every system for education and training are the quality and quantity of the professional competences developed in the trainees. The level of competence acquisition can be evaluated by studying the level of satisfaction of the users of qualified personnel with reference to the professional competency which the latter demonstrate at their workplace. This serves as a feedback showing to what extent the planned training objectives correspond to the achievements.*

Keywords: *The Quality of Education, customer satisfaction, professional qualities and competencies.*

Въведение

За качеството на дадено обучение се съди по професионалната способност и нивото на притежаваните професионални компетенции на завършилите го и ако те отговарят на нуждите и очакванията на потребителите на кадри ще е налице удовлетвореност от тяхна страна. Отчитайки потребителската удовлетвореност от подготовката на кадрите и справянето им със задълженията на работното място чрез формираните у тях професионални компетенции, може да бъде установено до колко проведеното обучение отговаря на заложените държавни изисквания и е адекватно на потребностите на пазара на труда, т.е. какво е неговото качество.

На база зависимостта между качество на обучение и ниво на изградени компетенции и с отчитане на връзката между нивото на професионалните компетенции и потребителската удовлетвореност може да се приеме, че ако се изследва степенята на удовлетвореност на командирите във формиранията за КИП от ежедневната войскава дейност демонстрирана от младите офицери завършили специализация „ВКИС“, ще бъде установено:

- нивото на професионалните компетенции, които притежават новоназначените офицери завършили специализацията, като това от своя страна ще даде информация за нивото на военно-професионалната подготовка (ВПП);
- кой вид компетенции от изграждащите професионалните е значим за потребителите и каква е удовлетвореността им за всеки един от видовете;
- качеството на процеса на обучение по специална военна подготовка (СВП).

Обект на изследване са потребителите на кадри (командирите на формирования за КИП и органите по управление на КИС), а предмет на изследване – тяхната удовлетвореност от нивото на професионалните и в частност от специалните компетенции на завършилите специализация „ВКИС“.

Дефинираната теза е, че удовлетвореността на потребителите на кадри от нивото на притежаваните специални компетенции изградени в завършилите специализацията е пряко свързана с качеството на обучение по СВП. Поставени са следните две хипотези:

1. Специалните компетенции са приоритетни за потребителите;
2. Специалните компетенции формирани чрез обучението по специална военна подготовка на курсантите от специализация „ВКИС“ не удовлетворяват напълно потребителите.

Предложената методика предвижда провеждането на анкетно проучване мненията на експерти, извършено във формированията от ВС на Република България, които са основен потребител на офицерски кадри от специализация „ВКИС“. Като метод за набиране на първични данни за удовлетвореността ще бъде използвана пряка анкета под формата на стандартизиран въпросник.

Отчитане на нивото на притежаваните от новоназначените офицери компетенции може да се направи ако се зададат определен брой показатели, които чрез експертното оценяване да бъдат ранжирани по значимост (важност) и им се даде числова оценка касаеща удовлетвореността от тях.

- 1. Методика за комбинирана оценка за степента на удовлетвореност на потребителите на кадри от нивото на професионалните компетенции които притежават завършилите специализация „ВКИС“ с отчитане приоритетите на показателите.**

За определяне степента на удовлетвореност на потребителите на кадри от нивото на професионалните компетенции на офицерите завършили специализация „ВКИС“ по определени показатели с отчитане на техните приоритети е приложен методът „**значимост – удовлетвореност**“ [2]. Той е основан на графичното представяне, при което пространствено се оценява значимостта на всеки един показател чрез определяне на тегловни коефициенти и удовлетвореността от него, установени от мненията на експерти на базата на проведено анкетно проучване.

- 1.1. Определяне на показатели отчитащи нивото на професионалните компетенции на база провежданото обучение по ВПП в специализация „ВКИС“.**

При определяне показателите за ниво на професионалните компетенции трябва да се съобрази техния състав, а именно това, че те представляват съвкупност от ключови, общовоенни и специални компетенции. Това налага системата от показатели да обхваща целия обем от знания, навици и умения изграждащи компетенциите, които се получават като резултат на обучението по ВПП.

Ключовите компетенции съдържат езиковата култура, владееене на чужд език, компютърна грамотност, комуникативност, способност за учене през целия живот както и социална и гражданска отговорност, инициативност и предприемачество, културна осъзнатост и творчество. Във военната специалност те се изграждат посредством общата професионална подготовка чрез изучаването на конкретни дисциплини, като се развиват основно умения за създаване на здравословни и безопасни условия на труд, речевото общуване и чуждоезиковата подготовка. За отчитане нивото на ключовите компетенции са приети следните два показателя:

- **Езикова култура и използване на чужд език** – отразяващ културата на речевото общуване и чуждоезиковата подготовка и умения за използване на специализиран английски език в служебната дейност.

- **Постоянно учене и развитие** – отчитащ способността за надграждане на придобитите знания и развиване навиците и уменията.

Изграждането на общовоенните компетенции се извършва във взаимовръзка с отрасловата подготовка необходима за практикуването на военната професия. Съответните компетенции се формират в резултат на теоретично и практическо обучение, което е единно за всички специализации от специалността. За определяне нивото на общовоенните компетенции са определени следните показатели:

- **Базова и обща военна подготовка** – чрез показателя се отчитат знанията и уменията на завършилите специализацията по: строева подготовка, уставни на Въоръжените сили, обща тактика, огневата подготовка със стрелковото оръжие, инженерна подготовка и ЯХБЗ. Показателя оценява базовата и общата военна подготовка на новоназначените офицери, както и способността им за изпълнение на задълженията като дежурни лица от състава на денонощния наряд.

- **Управление на ежедневната войска дейност** – оценява придобитите компетенции за организиране и провеждане на бойната и специална подготовка, методическите умения на командирите за воденето на занятията с подчинените в ежедневния учебен процес.

- **Лидерство и организиране и управление на екип, инициативност, вземане на решения и постигане на резултати** – оценява изградените управленски и организаторски качества, уменията за лично влияние върху подчинените, фокусиране върху поставените задачи и постигане на целите.

- **Физическа подготовка и методически умения по ФП** – оценяват се личната физическата подготовка и компетенциите за провеждане на занятия по ФП с подчинените. Показателят е включен в системата от показатели за определяне нивото на професионалните компетенции поради високите изисквания предявявани към физическата подготовка на военнослужещите и на база хорариума от часове предвидени за модул „Физическа подготовка“ в учебните планове 2012 и 2016 година – 240 учебни часа.

Преди да бъдат определени показателите за ниво на специалните компетенции трябва да се отбележи, че този вид компетенции са свързани със знания, навици и умения за определена сфера или област, следователно в случая ще бъдат разглеждани и анализирани само тези специални компетенции, които са необходими за специализация „ВКИС“ от специалността „Офицер за тактическо ниво на управление“. За установяване на нивото им са избрани следните показатели:

- **Теоретични познания по специализацията** – чрез избора на този показател се цели да бъдат оценени знанията за предназначението, мястото в КИС,

техническите възможности, характеристики и принцип на работа на основни образци комуникационни и информационни средства, експлоатирани във формиранията за КИП. Тъй като това се явява комплексен показател в оценката са включени знанията по регламентиращите и стандартизационни документи по КИС, правилата и процедурите за установяване воденето на обмен.

- **Технически умения по експлоатация на материалната част** – За да бъдат реализирани задачите по каналобразуване и администриране на информационните мрежи е необходимо завършилите специализацията да притежават способности за работа с отделните комуникационни и информационни средства. Показателят оценява уменията свързани с настройката и конфигурирането на средствата, извършването на регламентни работи и воденето на съответната техническа документация.

- **Предоставяне на услуги** – Услугите предоставяни от КИС са продукт от функционирането на системата и са предназначени за удовлетворяване на комуникационните и информационните потребности на системата за командване и управление чрез използване на различни приложения, като същите изразяват функционалностите, които КИС предлага на потребителя [1]. Чрез показателя се оценяват познанията за същността на предоставяните потребителски услуги на органите за командване и управление, уменията за тяхната реализация чрез изграждане на комуникационни канали и администриране на информационните мрежи, както и познаването и прилагането на системата от мерки за защита на информацията в КИС.

1.2. Създаване на рангова матрица.

За да бъде установена комбинираната оценка е необходимо анкетираните да попълнят таблицата съставена от три колони, като в първата са подредени избраните показатели в случайна последователност без номерация пред тях, във втората тези показатели трябва да бъдат подредени по важност от анкетираните, а в третата се дава степента на удовлетвореност от всеки показател по пет степенна скала от Ликертов тип

Методиката за определяне на значимостта или тегловните коефициенти на всеки показател е следната: [3, 4]

Получените резултати от оценъчната карта се записват в тегловна матрица (таблица 1.). Всяко число в матрицата a_{ij} определя теглото (ранга), което експерта R преписва на показателя j .

Таблица 1.

Рангова матрица за показателите на качество

Показател Експерт	Π_1	Π_2	...	Π_j
1	a_{11}	a_{12}	...	a_{1j}
$\bar{i}$	a_{i1}	a_{i2}	...	a_{ij}
R	a_{R1}	a_{R2}	...	a_{Rj}
$\sum_{i=1}^R a_{ij}$	$\sum_{i=1}^R a_{i1}$	$\sum_{i=1}^R a_{i2}$	...	$\sum_{i=1}^R a_{ij}$
Δ_j				
V_j				
W_j				

1.3. Изчисляване коефициента на съгласие (конкордация) между анкетираните.

Съгласуваността в мненията на експертите се изчислява като се провери коефициента на конкордация (съгласие) ω_k по методите на рангова корелация [4]

$$\omega_k = \frac{12 \cdot \sum_{j=1}^m \Delta_j^2}{R^2 \cdot (m^3 - m)}$$

(1)

където:

$$\Delta_j = \sum_{i=1}^R a_{ij} - S_{cp}$$

(2)

$$S_{cp} = \frac{R \cdot (m+1)}{2}$$

(3)

m е броя на показателите за оценка нивото на професионалните компетенции.

$\sum_{i=1}^R a_{ij}$ $j = 1, 2, \dots, m$ - сумата от ранговете за всеки показател;

S_{cp} е средната сума от всички рангове;

Δ_j е отклонението на сумата от ранговете за всеки показател от средната сума.

1.4. Проверка коефициента на конкордация за значимост.

Коефициентът на конкордация може да приема стойности от 0 при пълна несъгласуваност в мненията на експертите до +1 при пълна съгласуваност. Оценяването на значимостта на получения коефициент ω_k съгласно използваната методика ще бъде проверен по χ^2 критерий, тъй като броя на показателите $m \geq 7$ [5].

$$\chi^2_{изч} = R \cdot (m-1) \cdot \omega_k$$

(4)

Коефициентът на конкордация е значим при условие че

$$\chi^2_{изч} > \chi^2_{табл}(\alpha, \nu)$$

(5)

Стойността на $\chi^2_{табл}$ се взема от таблица в [3] с указани ниво на значимост α и степени на свобода $\nu = m - 1$

1.5. Изчисляване на тегловните коефициенти за всеки показател.

При наличие на съгласуваност в мненията на експертите се изчисляват тегловните коефициенти.

$$W_j = \frac{V_j}{\sum_{j=1}^m V_j}; j = 1, 2, \dots, m$$

(6)

където:

$$V_j = \frac{\left(R.m - \sum_{i=1}^R a_{ij} \right)}{R.m - R}$$

(7)

След изчисляване на коефициентите трябва да бъде изпълнено условието:

$$\sum_{j=1}^m W_j = 1$$

(8)

1.6. Изчисляване средната стойност от удовлетвореността на всички експерти за всеки един от показателите.

За изчисляване средната стойност от удовлетвореността, даваща степента на удовлетвореност на експертите от всеки показател за професионалните компетенции е използван метода на простата оценка, който се основава на анализиране на данни получени чрез допитване. Данните от всички анкетираните се обработват като се изчисляват оценките на средните стойности от всички анкетираните.

Средната стойност за удовлетвореността от всеки показател за качество се определя по формулата:

$$\bar{k} = \frac{\sum_{i=1}^R k_i}{R}$$

(9)

където:

$\bar{k}$ е средната аритметична величина на удовлетвореността за всеки показател;

k_i са значенията на признака по който се прави осредняването;

R е броя на анкетираните.

2. Резултати и анализ на проведеното изследване за оценка удовлетвореността на потребителите на кадри от професионалните и специалните компетенции на завършилите специализация „ВКИС“.

В изследването чрез попълване на оценъчните карти са анкетирани двадесет и един офицера специалисти по КИС, заемащи командни длъжности в тактическото и оперативното ниво на управление на въоръжените сили.

След обработка и изчисления на резултатите от оценъчната карта са получени: **матрицата на ранговете** показана в таблица 2. и **удовлетвореността от показателите за качество на компетенциите** (таблица 3.).

Таблица 2.

Рангова матрица на показателите за качество на компетенциите

Показател Експерт	П ₁	П ₂	П ₃	П ₄	П ₅	П ₆	П ₇	П ₈	П ₉
$\sum_{i=1}^{21} a_{ij}$	76	129	86	65	81	109	120	156	123
Δ_j	76	129	86	74	72	109	120	156	123
V_j	0,673	0,357	0,613	0,685	0,696	0,476	0,411	0,196	0,393
W_j	0,149	0,079	0,136	0,152	0,155	0,106	0,091	0,044	0,087
ранг	3	8	4	2	1	5	6	9	7

Таблица 3.

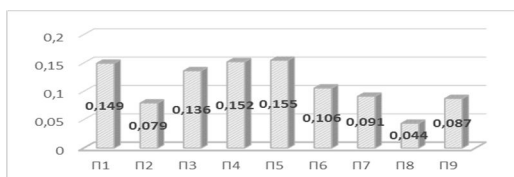
Удовлетвореност от показателите на качество

Показател Експерт	П ₁	П ₂	П ₃	П ₄	П ₅	П ₆	П ₇	П ₈	П ₉
$\bar{k}$	2,810	3,810	2,571	3,048	2,762	2,905	3,571	3,857	3,429

където:

Показател за определяне нивото на професионалните компетенции	Означение
Лидерство и организиране и управление на екип, инициативност, вземане на решения и постигане на резултати	П ₁
Езикова култура и използване на чужд език	П ₂
Управление на ежедневната войска дейност	П ₃
Теоретични познания по специализацията	П ₄
Технически умения по експлоатация на материалната част	П ₅
Предоставяне на услуги	П ₆
Постоянно учене и развитие	П ₇
Физическа подготовка и методически умения по ФП	П ₈
Базова и обща военна подготовка	П ₉

От резултатите в таблица 2., изобразени графично на фигура 1, е видно, че с най голямо значение за потребителите са показателите: П₅ (Технически умения по експлоатация на материалната част), П₄, (Теоретични познания по специализацията) П₁ (Лидерство и организиране и управление на екип, инициативност, вземане на решения и постигане на резултати) и П₃ (Управление на ежедневната войска дейност). Показатели П₅ и П₄ са съответно показатели за качеството на специалните компетенции и от получените коефициенти за значимост може да се направи извода че този вид компетенции е приоритетен за потребителите на кадри от формированията за КИП.



Фигура 1. Тегловни коефициенти на показателите за качество

На базата от получените резултати в таблици 2. и 3. е построена графиката значимост - удовлетвореност (фигура 2.), показваща връзката между показателите за качество на професионалните компетенции на офицерите завършили специализация „ВКИС“, тяхното значение и удовлетвореността на потребителите на кадри от тях. За получаване на четирите квадранта дефиниращи областите на значимост на показателите и удовлетвореността от тях е необходимо да се построят две перпен-

дикулярни прави, едната успоредна на абсцисата, а другата на ордината. Определянето на началните им точки се извършва по следният начин:

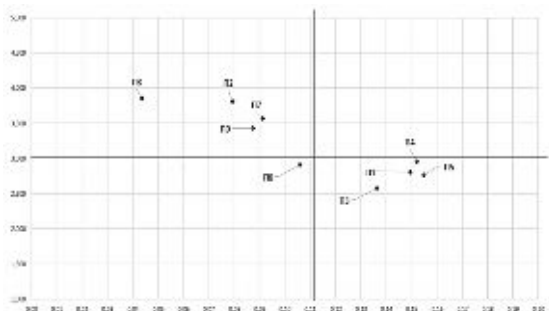
Началната точка на правата „ниво на удовлетвореност“ лежи на ординатната ос като същата може да бъде намерена по два начина. Първият е като се определи средата на стойността в статистическия ред наречена медиана. Медианата Me е средното положение на число, когато наблюденията в статистическия ред, когато наблюденията са подредени във възходящ или низходящ ред.

За реда 1,2,...,5 (оценките за удовлетвореност по скалата на Ликерт) броя стойностите в него е 5 т.е. нечетно число, следователно медианата Me е равна на числото, което се намира в средата на редицата, което в случая е 3. Вторият начин е като се намери аритметично средно $\bar{k}$, което за посочения ред също е 3. Вижда се, че медианата Me и аритметичното средно $\bar{k}$ в случая съвпадат. Построената права е успоредна на абсцисната ос.

Началната точка на правата „ниво на значимост“ отново може да бъде медианата на реда от показателите на значимост или тяхното средно аритметично. Медианата за посочения ред е $Me = 0,106$ (тегловия коефициент на показател P_6), а аритметичното средно е $\bar{k} = 0,111$. Ако за начална точка бъде избрана медианата то т. P_6 ще лежи на правата „ниво на значимост“ и ще се намира на границата между два квадранта. За това при построяването и за начална точка е избрана тази на аритметичното средно на коефициентите за значимост.

От изобразените графично резултати на фиг. 2 се вижда следното:

- Показателите P_5 и P_4 отразяващи специалните компетенции са с най-голям приоритет за потребителите, но те попадат в квадрант IV, който е област със висока значимост и ниска удовлетвореност. Другият показател за качество на специалните компетенции P_6 е в квадрант II, следователно е с по-ниска значимост, но отново потребителите не са удовлетворени от него;
- От общовоенните компетенции с най-голяма значимост за потребителите са показатели P_1 и P_3 , но те също попадат в квадрант IV, следователно удовлетвореността от тях е ниска.
- Всички останали показатели P_2 и P_7 (отразяващи ключовите компетенции) и P_9 и P_8 (общовоенни) са разположени в квадрант II, който е област на ниска значимост и висока удовлетвореност.



Фигура 2. Ниво на удовлетвореност и съответствие с приоритетите на показателите за качество на професионалните компетенции

От получените теглови коефициенти за показателите за качество установяващи нивото на професионалните компетенции става ясно, че приоритет за потребителите на кадри във формиранията за КИП са специалните компетенции, които трябва да притежават випускниците в специализация „ВКИС“. Резултатите отразяват мнението им за значимостта на този вид компетенции при изграждане на комплекса от професионални компетенции нужни за изпълнението на длъжностите, които ще бъдат заемани от младите офицери. Нивото им в случая е ниско и не отговаря на потребителските очаквания, от което следва да бъде направен извода, че качеството на обучение по специална военна подготовка, чрез която те се формират е незадоволително.

Заклучение

Получените резултати от изследването показват съответствие на получените знания, умения и методическа подготовка разглеждани като професионални компетенции на випускниците с изискванията предявени от потребителите на кадри. По-детайлният анализ обаче води до извода, че в отделни направления са налице недостатъци, които се явяват пречка за развитието на младите офицери в специализацията, което пък затвърждава мнението за наличие на пропуски в организацията и планирането на обучението по военната специалност.

Използвана литература:

1. Доктрина на Въоръжените сили на Република България НП-01, София, 2011г.
2. Недялков, А., Велева, Л., Емпиричен поглед върху релацията "Качество на услугите - удовлетвореност на потребителите", Русе, 2012 г.
3. Стоянов, С., Оптимизация на технологични процеси, Техника, София, 1993г.
4. Kendall M., J. D. Gibbons, Rank Correlation Methods, Oxford University, Press, New York, 1990.

Р. Б. Чалъков, К. А. Илиев, Д. К. Марков

ПОДХОДИ ЗА ОБУЧЕНИЕ НА БЪДЕЩИ ОФИЦЕРИ В НЯКОИ ОТ ВОДЕЩИТЕ АРМИИ НА НАТО

Радослав Б. Чалъков, Калоян А. Илиев, Дилян К. Марков

*Military academy "Georgi S. Rakovski", Faculty "Command-staben",
Department "Land forces"*

APPROACHES FOR THE TRAINING OF FUTURE OFFICERS IN ANY OF THE LEADING NATO ARMY

Radoslav B. Ghalakov, Kaloyan A. Iliev, Dilyan K. Markov

*Military academy "Georgi S. Rakovski", Faculty "Command-staben",
Department "Land forces"*

Abstract: *The profession of officer and the accompanying education is an occupation for people who have a sense of a specific vocation and wish to enter one of the so-called "systems". The army is a closed structure with structures other than the civil sector, working rules, hierarchy and career development. Generally speaking, military education involves training in military theory and practice, including the handling of weapons and military equipment, which will lead to the exercise of a profession in the defense system, often with a valid qualification in the civilian sector as well.*

Keywords: *education, officers, training, career*

За някои службата във въоръжените сили е само тежко бреме или пропилян живот. Дори и да се пенсионираят като офицери, освен заплата и пенсия такива хора нито получават нещо от армията, нито ѝ дават нещо от себе си, *но за други тя е безценен житейски опит.*

Професията офицер и съпътстващото я образование е занимание за хора, които имат усещане за специфично призвание и желаят да влязат в една от така наречените „системи“. Армията е затворена структура с различни от цивилния сектор структури, правила за работа, йерархия и кариерно развитие. Най-общо казано, военното образование предполага обучение по теория и практика на военното дело, включително боравенето с оръжия и военна техника, което ще доведе до правоспособност за упражняването на професия в системата на отбраната, често с квалификация валидна и в гражданския сектор.

Обучението на офицера е един непрекъснат процес, който започва от военното училище и продължава във военните формирования. Командирските знания и умения се формират още на „курсантската скамейка“ и през различните етапи на служебното му развитие.

Периодът на военното обучение в армията на Бундесвера започва с постъпването на бъдещия офицер като войник и преминава последователно през тримесечно единично обучение, след което следват три месеца на специализирано обучение

по програма за специалисти (артилеристи, пехотинци и т.н). Обучението на курсантите през този период се води във войските и след завършването му те се повишават в звание „ефрейтор“. Следва тримесечно обучение по управление на техниката, която е на въоръжение във вида въоръжени сили (родове и специални войски), курсът се провежда в тренировъчните центрове и в края на периода бъдещият офицер получава удостоверение за правоспособност.

Военноспециалната подготовка във военното училище започва след приключване на осемте месеца служба във войските. Общата продължителност на този период е дванадесет месеца, като първите пет са редовен учебен процес, три – войсков стаж като командири на отделение и още четири месеца редовен учебен процес в училище. Обучението завършва с едномесечен отпуск.

От 22-рия до 36-я месец от началото на службата, обучението е 6 месеца в общовойсковото училище, където се обучават всички специалисти от Сухопътните войски и 8 месеца войскова практика и самоподготовка като заместник-командири на взводове във войските.

В края на този период, т.е след 36 месеца служба, обучаваният получава първо офицерско звание „лейтенант“, след което в продължение на 3 месеца изпълнява длъжността „командир на взвод“. С това приключва етапът на основното военно обучение.

Следващият етап от обучението през първия период започва в началото на 40-я месец и по същество представлява следване в един от гражданските университети. Срокът му е 39 месеца, като военните студенти получават заплата за длъжност и звание. Специалностите по които се обучават са педагогически, политологически и инженерно-математически. След завършване на университета и връчване на дипломите лейтенантите получават и следващо военно звание „старши лейтенант“. Предстои тримесечен курс за опресняване на военната подготовка и офицерът достига до първото си служебно назначение като командир на взвод или командир на група.

Завършването на обучението през първия етап е свързано със сключването на договор, който около дванадесетата година може да бъде продължен или офицерът да напусне армията.

Подготовката на офицери за нуждите на Френската армия съчетава традициите и новите тенденции във военното образование. Висшите военни училища дават възможност за върхов път в кариерата на бъдещите офицери. Те са три:

- Висшето военно училище „Сен сир“ в Коеткидан (Ecole special militaire de Saint – syr – ESM);
- Висшето военноморско училище в Брест (Ecole navale de Breste – EN);
- Висшето военновъздушно училище в Салон дьо Прованс.

Последните две издават диплома за висше инженерно образование.

Обучението в училищата е три години плюс една година специализация за рода войска, като условията на подготовка са при пълен пансион. Към висшите военни училища има и военни училища за вътрешен достъп за подготовка на офицери и офицери от запаса. Това са общовойсковото военно училище в Коеткидан за СВ и военноморското училище в Брест. Срокът за обучение в тях е 2 години плюс една за специализация за рода войска.

Офицерите от техническия и административния корпус се обучават във военното училище на техническия и административния корпус в Коеткидан (Ecole

militaire de corps technique et administratif - ЕМСТА) и Училището за подготовка на административни кадри за нуждите на ВМС в Шербург (Ecole d'administratif de la marine). Обучението е с продължителност две години.

ЕСМ в Коеткидан подготвя офицери от кариерата за сухопътните войски. Набирането става чрез конкурсни изпити по различни предмети в зависимост от образователното равнище на кандидатите. Те могат да бъдат по математика, френски език, филологии и икономически науки, както и за придобиване на определено равнище на висше образование. Кандидатите трябва да бъдат французи по националност и да са под 22 години (23, ако са служили в армията). Подготовката за конкурсните изпити във висшите военни училища се извършва във военни лицей (гимназии) и подготвителни класове. Военните лицей са гимназии като останалите, като учебните програми се определят от Министерството на националното образование, но са военни, т.е. управляват се и се комплектуват от военната администрация. За това свидетелства носенето на униформа от учениците. Обучението се осигурява от хонорувани цивилни преподаватели. Освен функцията за подготовка на учениците за кандидатстване във висшите военни училища те изпълняват и социална функция. Приемат приоритетно деца на починали при изпълнение на служебния си дълг военни, магистрати, както и синове и дъщери на действащи военни при определени обстоятелства.

За подготвителните класове няма ограничение при приема. Всеки млад французин, отговарящ на възрастовите условия (20 или повече години) и физически годен, може да депозира документите си за конкурса. Ако бъде избран и при условие, че се ангажира да се яви най-малко на един от конкурсите във висшите военни училища и подпише „декларация за намерение“ да прави кариера в армията в случай на успех, ученикът се ползва от безплатно обучение и получава държавна стипендия. Този вид училища са основен източник на бъдещи офицери (над 50 % от курсантите във висшите военни училища). Освен военните, цивилните лицей също организират подготвителни специализирани класове (основно за морското и въздушното училище). Според общественото мнение извън военните гимназии и гражданските подготвителни класове да се издържи успешно конкурс във висшите военни училища е равностойно на подвиг.

Военните специалисти във Франция смятат обучението на курсантите във висшите военни училища за сложна задача. Там отдавна са осъзнали голямата отговорност и се полагат всички усилия за формиране на високо подготвени офицерски кадри. След строг подбор всяка година около 400 младежи постъпват в Коеткидан, около 160 в морското и 150 във въздушното училище. В Коеткидан са съсредоточени най-много училища. Продължителността на обучението в ЕСМ е три години плюс една година специализация за рода войска в училищата на родовете войски. Общовойсковото военно училище ЕМПА, основано през 1961 г., чиито възпитаници постъпват чрез вътрешно-армейски подбор, осигурява две години обучение, последвано от една година специализация в училищата на родовете войски.

Създаденото през 1977 г. военно училище за техническия и административен корпус ЕМСТА приема не само младежи, подобрани чрез конкурсен изпит и със завършено средно образование, но и офицери и подофицери с висше образование. За курсантите в ЕМСТА обучението в Коеткидан продължава една година.

Амбицията на ръководството е да разкрие на всички курсанти, независимо от избора от тях профил, качествата за развитие и пълен успех в кариерата на офи-

цер. Поради това през 1992 г. е въведен единен образователен проект. Целта му е да даде на курсантите обща култура, умения за оцеляване и способности за действие в различни кризисни ситуации. Стремешът на командването на училището е да обучава пълноценни офицери, което се открива и при трите компонента на образователния проект, разпределен в три години: военно обучение, академично обучение и обучение по упражняване на властта (formation a l'autorite - FEXA). Последното е фундаменталният и приоритетен компонент от обучението на бъдещите офицери и е негов ключов елемент. Военното обучение има за цел да даде на курсанта основните професионални познания, необходими на всеки офицер през първите 8-10 години от кариерата му. Част от тях се осигуряват от училищата на родовете войски с цел завършване на професионалното обучение в съответствие с избрания род войска. Тези училища са дванайдесет за сухопътните войски. По-важни от тях са Училището за подготовка на пехотинци (Ecole application de linfanterie) в Монпелие, Училището за подготовка на танкисти (Ecole application de l'artillerie blindée) в Сомюр и Училището за подготовка на артилеристи (Ecole application de l'artillerie) в Драгинян.

Второто измерение на обучението в ESM е академичният курс. Той дава на бъдещия офицер обща култура, която е безусловно необходима за разбирането на света, в който живеем. По този начин той разполага с набор от основни познания които улесняват правилния избор на поведение в различни ситуации, както във вътрешността на страната, така и зад граница.

Третият и последен компонент на проекта за обучение в ESM – по упражняване на властта, цели да придаде на курсанта поведение на офицер и командир. То присъства на всички образователни равнища и може да се нарече истински гръбнак на системата. В изпълнение на Хартата за властта на началника на Генералния щаб на СВ и Директивата на командващия учебните заведения към СВ (COPAT) това обучение поставя човека в центъра на проекта. *Основната му цел е да формира едновременно командирски, преподавателски, инструкторски и комуникативни умения.*

Обучението по упражняване на властта развива способностите на курсантите за адаптация и поставя основите на поведението им като офицери. Според ръководството на училище „Сен Сир“ гъвкавостта и адаптацията са ключовите думи за съвременния военен. То се осъществява в три самостоятелни, но взаимно допълващи се етапа. Първият цели да предаде на курсантите основните познания във връзка с провеждането на тримесечния им стаж по войсковите части още през първата година на обучение, при които те за първи път командват подчинени. След това идва етапът на задълбочаване на знанията, разпределен по цялата продължителност на образователния процес, който се състои от три типа курсове. Курсът по психология е насочен към доброто познаване на хората и себе си, тъй като за да командваш добре, трябва да бъдеш наясно със себе си. Дори и в армията да съществува определен стил на командване, за всеки офицер е необходимо да може да го прилага в съответствие със специфичните особености на личността си.

Следва „методът на изразяване“ – умението да слушаш и да бъдеш изслушван. Има и курс по „съвременно френско общество“, тъй като добрият офицер трябва да е в крак с обществото, в което той и неговите подчинени живеят.

Третият етап на обучението е завършващ. Това е цикълът по „етика и деонтология“. Започва от втората година на обучението и има за цел да даде на курсанта общ

поглед върху статута на офицера, неговата специфика, мястото, ролята и задълженията му. При този образователен цикъл се изучават четири учебни области: офицерът пред самия себе си, офицерът и националната сигурност, офицерът и мястото му в армията и националната отбрана, офицерът и мироопазващите операции.

Всяка тема е включена в самостоятелна лекция, водена от военен или граждански преподавател. Преди нея се провежда предварително занятие за подготовка, а след нея - обсъждане, ръководено от кадрови офицер, при което тя се затвърждава и доразвива.

В заключение може да се обобщи, че военните училища не дават рецепти за подготовка, а знания и умения, необходими за войсковата практика, френската военнообразователна система се доказва в наши дни и се оценява високо в чужбина. Успехът ѝ, както и този на определената концепция за нейното ефективно управление, се дължат на факта, че французите имат усещане за човека. Този успех се обяснява с традициите на френската култура и зачитането на човешките ценности, от които черпи вдъхновение и обучението във военните училища.

Командването на въоръжените сили в Турция отделя сериозно внимание на подготовката на офицерски кадри, като се стреми да осигури попълването на армията с квалифицирани и политически благонадеждни офицери.

В процеса на обучението се внедряват нови, по-ефективни методи, усъвършенства се учебно-материалната база. Важно значение се придава на морално-психическата подготовка на офицерските кадри, която способства за изработването на волеви качества и физическа закалка, необходими за водене на действия в различни бойни условия.

Офицерските кадри се готвят предимно в националните военни учебни заведения и само незначителна част от тях се обучават в чужбина, главно в САЩ и Германия, където се изпращат за усвояване на нова техника и оръжия, които се закупуват за въоръжените сили на страната.

Началното военно образование се дава във военните гимназии (лицеи), чиито випускници получават преимуществено правото на постъпване във военното училище, а средното образование (главно теоретическа подготовка) - във военните училища. Офицерите от турските въоръжени сили получават висше военно образование във военните академии, които са териториално обединени.

В гражданските ВУЗ се подготвят офицерски кадри за Въоръжените сили на Турция по специалности, по които не могат да бъдат обучени във военните училища.

Срокът на обучение в лицейте е четири години. Първата година е подготвителна. През този период се отделя основно внимание на изучаването на чужди езици. Онези, които не са издържали изпитите по програмата за подготвителния курс, се отчисляват.

Випускниците на езиковите общообразователни училища се приемат направо в първи курс.

Във въоръжените сили на Турция има пет лицея. По своята структура, програма за подготовка, учебна база и пропускателна способност лицейте на сухопътните войски са аналогични. Ежегодно във всеки от тях се обучават около 2000 курсанти. Учебната година започва на 25 септември и завършва на 30 май. В продължение на два месеца след завършването на учебната година курсантите се изпращат на лагери (в района на Ялова), където се провеждат практически занятия по тактика, огне-

ва, строева и физическа подготовка. Лицеите на сухопътните войски обучават ежегодно по 500 обучаеми, военноморският и военновъздушният - по 140-150. Те са основните кандидати за постъпване във военните училища.

Офицерските кадри по всички специалности се подготвят в училищата на видовете въоръжени сили. В тях се приемат младежи на възраст от 17 до 20 години, завършили военните общообразователни лицей и приравнените учебни заведения. От гражданските учебни заведения се приемат по правило не повече от 20 процента от общия брой курсанти.

Общовойсковото офицерско училище на СВ „Кара Харп Окулу“ (Анкара) подготвя офицери за СВ по всички специалности, както и за жандармерийските войски, за топографската служба и морската пехота (ежегодно по 10-12 обучаеми завършват подготовката за офицери за морската пехота). Освен това тук се осъществява и обучението на военните юристи и строители.

Ежегодно 450-500 офицери завършват училището с присвоено им воинско звание „лейтенант“. Те преминават годишна специализация в училищата на родовете войски, след което се назначават на длъжност командир на взвод и се отправят във войските.

В армиите на страните, членки на НАТО, обучението е организирано въз основа на приетия при тях системен подход към обучението (Systems Approach to Training). Моделът е отражение на системният подход в мениджмънта и е един много успешен опит за внедряване на постиженията на съвременната наука за управление в обучението и за повишаване на гаранцията за постигане на целите на обучението в армията.

Този модел е вече изпробван и се прилага, което дава възможност за ускорено преминаване през някои от процедурите. Онова, което го прави малко по - особен, е наличието на някои подходи при самия анализ на дейността, формулирането на целите и валидизация на обучението. По-обстойният анализ на този модел показва една значителна гъвкавост по отношение на насоките на обучение и според целите на обучаващата организация той може да даде преобладаваща тежест на обучение към знания, за умения или към обучаемия.

Разбира се, той не може да бъде приет, като универсално решение за всички проблеми в обучението за всякакви условия. На първо място, той предлага много точна кадрова политика, която изисква много ясна идея за реализацията на всеки произведен кадър. На второ място, този модел предлага разгърнатата мрежа от добре подготвени офицери в областта на мениджмънта на обучението, които да прилагат и направляват обучението на базата на този подход и съобразно конкретните условия.

Ако се придържахме към досегашната практика, следва да определим един от подходите като най- важен и да се опитахме всички учебни планове и учебни програми да удовлетворяват всички изисквания. Опитът обаче показва, че не може да има само едно вярно решение и още повече такова, което да е винаги валидно.

Използвана литература:

1. Жан-Пиер Байли, "La Gazette des Uniformes", № 193, Juillet-Aout 2001
2. Обучение на военните на Америка, Джонсън-Фрейс
3. http://www.nato.int/cps/ic/natohq/news_113548.htm

4. Military education: Past, Present, and Future by Gregory C. Kennedy; Keith Neilson, 2003, USA
5. https://en.wikipedia.org/wiki/Military_education_and_training
6. http://www.kho.edu.tr/eng_about_tma/history.html
7. <http://www.fueakbw.de/index.php/en/>

ИМИДЖЪТ И КОМУНИКАЦИОННИТЕ КАТО ВОДЕЩИ ФАКТОРИ В РАЗВИТИЕТО НА ВОЕННАТА ОРГАНИЗАЦИЯ

Валя М. Симеонова

гр. София ж.к. "Младост 3" бл.369 вх.1 ет.4 ап.14

THE IMAGE AND COMMUNICATIONS AS A LEADING FACTORS IN THE DEVELOPMENT OF THE MILITARY ORGANIZATION

Valya M. Simeonova

Abstract: *The image is one of the tools for realization of the organizational and communication goals. Communication creates the image of the organization. It means the professional communication between subordination levels in the organization.*

Keywords: *military organization, image, communication, defense, professional communication.*

Имиджът и военната организация

Понятието "имидж" е доста широко разпространено главно в две свои значения, имидж на организацията /корпоративен имидж/ или като имидж, който се отнася пряко до продуктите и услугите на дадена компания.

Имиджът - това е образът на лице или институция в съзнанието на хората. Това определение точно изразява генезиса на имиджа - той е плод на многообразна, идваща от различни източници информация за реално съществуващи обекти и явления. Имиджът създава една втора реалност, която силно влияе върху процеса на вземането на решение от индивида. Изграждането на подходящ организационен образ е бизнес инструмент, който за разлика от материалните средства представлява неизчерпаем ресурс за повлияване поведението на публиките. Имиджът е един от инструментите за реализиране на организационните и комуникационните цели.

Корпоративният имидж е капитал за фирмите, чиято стойност расте във времето. Той е основен фактор за нейния просперитет, политика и цели.[4]

Имиджът на една организация може да се разглежда като проекция на нейните действителни елементи в съзнанието на публиката. Образът на организацията, който съществува в съзнанието на отделния индивид е от огромно значение, защото той съдържа оценка - положителна или отрицателна. Създаденият образ може да се базира както на вярвания, така и на факти. Имиджът може да бъде позитивен, негативен или неутрален. Достигането на благоприятен имидж е една от целите за създаване на корпоративна идентичност. За правилното изграждане на корпоративен имидж значение имат: организация, структура и култура на организацията, комуникации, опитът на организацията, социална отговорност, отношението и поведението на служителите.

От първостепенно значение за благоприятния имидж за една организация са посланията, които тя комуникира, да бъдат свързани не толкова с конкретните й

интереси, колкото с нуждите на нейните публики. Организацията са наясно, че благоприятната представа се изгражда трудно, стъпка по стъпка, а може да рухне изненадващо лесно, следствие на един погрешен ход. Имиджът на една организация може да бъде такъв, какъвто го възприемат нейните служители, какъвто ръководството иска и мисли, че трябва да бъде, какъвто го възприемат потребителите. Когато външните публики имат сходно виждане за състоянието на една институция с това на нейното ръководство и вътрешните публики, имиджът на организацията определено може да се възприеме като положителен.

Във всяка организация работи различен екип, действат уникални писани и неписани правила, има различни ценности. Многократно е писано, че единственото конкурентно преимущество на организацията са хората. Те изграждат образа на организацията. Всеки служител е изключително важен за компанията, за която работи, както при осъществяването на корпоративните ѝ цели и интереси, така и за изграждането на подходящ корпоративен имидж.

Отбраната е най-важната област за една държава. Министерството на отбраната не е просто едно от многото министерства на Р България, а е своеобразна заявка за сигурност и стабилност. Във военното ведомство е необходимо да царят атмосфера на екипност, способност за избягване на конфликти, способност за вземане на решения, способност за комуникация, зачитане и съвместяване на военна и цивилна експертиза, необходим е баланс, а не изключване на едната от двете експертизи. Инвестирането в сектора за сигурност - въоръжение, техника, системи и човешки ресурси, увеличава позитивния имидж на институцията. Имиджът означава задържане на добре подготвените и с голям практически опит служители. Това е възможно чрез спиране на непрекъснатите промени в сектора.

Повече от всякога е необходима иновативност, креативност, способност за критично стратегическо мислене, адаптивност, отдаденост на каузата. Това са характеристиките на качественото лидерство, което ще направи военната организация, въоръжените сили способни да се справят с новите предизвикателства. Налага се разработването и провеждането на адекватна отбранителна политика, която да осигури изграждането, развитието и поддържането на необходимите отбранителни способности на българските Въоръжени сили.

Комуникационна среда на военната организация

В основата на благоприятния имидж стои успешната комуникация с публиките. Комуникацията създава обликът на организацията. Ролята на комуникацията е от първостепенно значение при изграждане на професионалната среда за развитие, при изграждане на корпоративната отговорност, при защита на конкурентоспособността на бизнеса.

Комуникацията в организацията е понятие, което се използва в управленската наука и практика за обозначаване на цялостната организация и процеса на професионалното общуване между субординационните нива и по хоризонтала в работните групи, съставляващи организацията. Чрез комуникациите в организацията се създава интегритет на хората и групите и целенасоченост на усилията за постигане на организационните цели. Чрез комуникацията в организацията се осъществяват следните функции: даване на разпоредителна информация отгоре надолу /ръководител-подчинени/ чрез заповеди, указания, разпореждания, препоръки и др.; получаване на

обратна информация отдолу нагоре /подчинени-ръководител/ за изпълнение на задачите; даване на оценка за изпълнение на задачите от подчинените.

Вътрешните комуникации са двустранна дейност, насочена към обмен на информация между служителите и структурните звена в организацията. [3]

От посоченото следва да се обобща, че чрез понятието комуникация може да се обозначи процеса на професионалното общуване в организацията.

Бизнес комуникациите вътре в организацията могат реално да съществуват и подкрепят нейните дългосрочни и краткосрочни цели, ако получават разбирането и необходимите финансови ресурси за развитието им. Подценяването на значението на вътрешнофирмените комуникации за добрата професионална атмосфера в организацията не води до интегритет и баланс, създава напрежение и постепенно - и недоверие в ръководството. [1]

Като социално явление процесът на общуване означава не само разпространение, но и възприемане на информация. От изключително значение за ефективната комуникация са двете основни форми на общуване - формална и неформална.

- Формална - преминава през формалните пътища в организацията и е под контрола на мениджмънта. Ръководители, желаещи да създадат подходяща социална среда, могат да установят формални канали за комуникация, чрез които подчинените изразяват своите идеи, желания и чувства, свързани с тях, с работата, с организационната политика и практика.

- Неформална - тя е резултат от функционирането на неформалните екипи или се предава от човек на човек. Тази комуникация се идентифицира с "комуникационен слух или клюки" и представлява неофициална система за предаване на информацията, спонтанно възникнала при социалните контакти на хората. Това е междупersonностна система, възникнала естествено от желанието на хората да създават приятелства и да си споделят идеи. Мениджърите имат интерес от тези комуникации, защото създават полезни обратни връзки с работещите. Според социологическо изследване на "Уолстрийтджърнъл" комуникациите "слух" са 75%-95% по-ефективни при пренасянето на информация в сравнение с формалните комуникационни канали.

В зависимост от посоката на движение на информацията комуникацията бива:

- Низходяща - основава се на електронни и вербални методи за информиране на служителите по въпроси, свързани с организацията по достъпен начин. Този тип комуникация се състои от информация, започваща от най-високото ниво в дължиностната йерархия на организацията и осведомява служителите какво е значимо и какви са целите на организацията. Най-често това са: инструкции за работа, официални бележки, процедури, наръчници за работа. Постоянното разясняване на плановете и резултатите от тяхното изпълнение на персонала, повишава неговата ангажираност и сътрудничество към фирмените интереси.

- Възходяща - тя пренася информация от служителите към мениджърите. Често включва информация за даден служител, за сътрудници, организационни практики и политики и за това какво трябва да се направи и как може да се направи, причини за конфликти, предложения за усъвършенстване на дейността, оплаквания и др. Важно е служителите да имат възможност да генерират възходяща комуникация, защото техните идеи и критики към плановете и идеите на мениджърите могат да бъдат полезни при намиране на решения за цялостно подобряване на постиженията

и доходността на организацията. Успешната възходяща комуникация зависи от междуличностната среда.

- **Хоризонтална** - ефективната организация се нуждае от хоризонтална комуникация. Тя се осъществява между намиращите се в равнопоставено положение по отношение на йерархията, отдели или хора.

- **Диагонална** - налице е, когато служителите не могат да комуникират помежду си по друг начин. Използва се най-рядко и се извършва чрез формалните канали в организацията.

Мотивирането на персонала да води постоянен и открит диалог за работата на организацията, насърчаването на свободата на мнения и нестандартните идеи са в основата на ефективните комуникации. Двустранният диалог дава възможност за фокусиране върху проблемите, за търсене на тяхното разрешаване и постигане на общо разбиращелство във вертикалните и хоризонталните структури на съвременната организация.

При необходимост от допълнителна информация комуникационният процес може да се повтори многократно. В хода на процеса се осъществява уточняване, изясняване, обобщаване, сравняване на възгледи, различия и др. на страните, участващи в процеса.

Комуникацията може да бъде от йерархичен тип, за който е отличително запоявдането, напр. началник-подчинен. В такъв случай най-важна е чистотата на канала за връзка, тъй като полученото съобщение винаги бива изпълнено, ако достигне до получателя си. Режимът на общуване между събеседниците е монологичен, защото властта поражда един текст. За демократичния тип комуникация, където приоритет има обратната връзка, отличителна черта е убеждаването, а получателят на съобщението има право на избор - да го изпълни или да откаже да го изпълни. Режимът на общуване е диалогичен. [2]

Основният извод е, че министерството на отбраната е гарант за сигурност и стабилност на държавата. В днешната динамична и несигурна среда военната организация се стреми да надгражда своя имидж и утвърдени позиции в общественото пространство чрез различни активности. Това трябва да донесе успех и да се повиши интереса към военната организация:

- спиране на непрекъснатите промени в сектора
- мотивиране и задържане на подготвените кадри
- редовно информирание на обществеността.

След всичко това имиджът може да бъде по-добър и позитивен, насочен към бъдещето, създава се благоприятна възможност военната организация да се представи като отговорна, надеждна, заслужаваща доверие организация.

В заключение може да се каже, че комуникациите са от ключово значение за развитието и позиционирането на една организация в публичното пространство. Те подпомагат нейната дейност и изграждат достоверен имидж пред обществото. Именно те гарантират прозрачността и коректността на организацията. Имиджът е съвкупност от редица фактори, насочващи вниманието към най-добрите качества на организацията.

Използвана литература

1. **Алексиева, С.** Бизнес комуникации. София: НБУ, 2011. 183 с.
2. **Захариева, Й.** Стратегии за езикова комуникация. София: Авангард Прима, 2010. 174 с.
3. **Кичева, Т.** Позициониране и значение на вътрешните комуникации в българските организации, Икономически алтернативи, бр.4, 2011. с.72-87.
4. **Райков, З.** Корпоративен имидж. София: Дармон, 2001, 204 с.

Х. А. Христов,
**СРЕДСТВА ЗА КОНТРОЛ И СПОСОБИ ЗА ПОЛУЧАВАНЕ
НА ИНФОРМАЦИЯ**

Христо А. Христов

**CONTROL INSTRUMENTALITY AND METHODS FOR INFORMATION
RETRIEVAL**

Hristo A. Hristov

Abstract: *The control's means and methods are used to measure parameters that are objects of control in order to process the information taken in. On this basis surveillance, comparisons and analyses are possible to be made. Certain contrivances helps to clarify the information accepted, create an opportunity to spread and assume easier this information. They make possible timely determination of contemporary condition of researched object or examined process as well as their deviations.*

Keywords: *security sector, control instrumentality, technical, organizational, psychological control methods, accounting, inquiry, data, survey, raid, research, interrogation.*

Средствата за контрол служат за измерване на параметрите, които са обект на контрол, за обработка на получената информация. Въз основа на тях могат да се извършат наблюдения, сравнения и анализи. Чрез определени средства се онагледява получената информация, създава се възможност за огласяване и по-лесно възприемане на тази информация.

Особено значение за контрола и неговата ефективност има използването на съвременни технически средства, предаващи точност и надеждност на информацията. Чрез тях е възможно както своевременното установяване на фактическото състояние, така и отклоненията в проверявания обект или процес.

В най-общия случай видът на средството за контрол се определя от целта, обхвата на контрола и характеристиките на проверявания обект.

За да се изучат по-цялостно и да се разкрие полето на тяхното приложение, средствата за контрол могат да се групират по следния начин:

А. Технически средства. Тези средства служат на субекта на контрола за метрифициране параметрите на обектите. Чрез тях се получава информация за количествени характеристики, като тегло, дължина, дебелина, плътност и др. Те могат да се използват непосредствено от контролния орган или могат да бъдат включени в автоматизирана система за получаване и обработка на информация, която би служила както за мениджмънта, така и за контролна дейност.

Б. Организационни средства. Тази група обхваща средствата, които са представени като стандарти, технологии, търговски марки, технически пломби и други. В същата група попадат и средствата за предаване и приемане на информация (телефон, телефакс, GPS системи), както и организационни средства, с които се идентифицират и доказват подобия или различия като инвентарни табели, пломби,

цифри, както и средства за доказване на резултати от проверката - печати, стикери, бланки с шифри, цифри и/или надписи.

Организационните средства според предназначението си се групират в две групи: средства обслужващи контролната дейност; средства доказващи извършена контролна дейност.

В. Психологически средства. Те се използват несъзнателно от контролните органи, в резултат на постигната рутина и ерудиция. Това обаче не пречи те да заемат своето съществено място в контролната дейност, особено при реализацията на отделните способности. Те могат да намерят израз в убеждение, въздействие, предразполагане към спокойна обстановка по време на ревизии и инспекции, вдъхване на увереност в контролния орган. Чрез тези средства се налагат определени подходи в работата на контролния орган, обектите на контрол се приобщават с действеността на субекта. За да може да използва посочените средства, субектът на контрол трябва да е добър психолог, да може да изучава поведението на обектите, когато те са отделни длъжностни лица или обикновени граждани, подлежащи на една или друга проверка.

Г. Средства за онагледяване на резултатите от контрола

Съвременните компютри и съпътстващите ги софтуерни продукти дават възможност за онагледяване на резултатите от контрола чрез таблици, диаграми, графики или схеми за технологичната последователност на контролния процес, обхват и крайни резултати. Това са средства, които визуализират контролната дейност и резултатите от нея и я правят прозрачна и по-лесна за възприемане. Тези средства намират приложение за изследване на криминални фактори, обуславящи различните видове престъпност и тяхното графично изобразяване с цел идентифициране и разкриване на престъплението.

Способи за получаване на информация за контрол

Способите заемат особено място в общата методология на контрола. Всеки метод се реализира въз основа на различни способности, които позволяват да се изучат отделни страни на явленията и процесите, които са части от цялостното изследване на обектите за контрол с помощта на определени методи. Това още веднъж потвърждава тяхното място при практическото усвояване на обектите, което предопределя и тяхната целенасоченост. Всеки способ на контрол се използва в определени случаи, в зависимост от конкретната нужда. Но и тук както и при средствата за контрол, може да се посочи, че за да се използва даден способ, той трябва да се познава от субекта на контрола и да може да се прилага в зависимост от поставената задача. В противен случай той губи своята практическа значимост.

Най-често използваните способности в практиката са стопанската (или друга) отчетност, наблюдението, сведенията, справката, анкетата, интервюто, фотоснимката, инвентаризацията, документалната проверка, писмените обяснения, разпита, претърсването и обиска и др.

Стопанска (или друга) отчетност

Стопанската (или друга) отчетност включва три направления: оперативно - техническа, статистическа и счетоводна отчетност.

Оперативно-техническата отчетност позволява осъществяването на наблюдение и контрол върху отделните стопански (или други) явления и процеси в момента на тяхното протичане. Информацията, осигурена от тази отчетност, служи на управлението за вземане на конкретни и бързи решения. Сведенията могат да се

предават по телефон, факс, чрез устни или писмени съобщения. Много често информацията не се документира и съхранява. Поради това оперативнотехническата отчетност не е точна, а приблизителна. При осигуряването на информация се ползват всички отчетни измерители. Чрез нея се осигуряват сведения за броя на работилите, за обема на продукцията, за наличните материални запаси, за изпълнението на договорите и др. Сведенията се осигуряват от персонала, работещ в различни отдели, производствени звена и др. Тъй като информацията се получава в процеса на протичане на процесите, тази отчетност има голямо значение за намесата на управленския орган в хода на дейностите.

Чрез **статистическата отчетност** се наблюдават, обобщават, групират и анализират сведения и данни за масово проявяващи се явления. Те могат да се разглеждат както в национален мащаб, така и по отделни териториални единици, по отрасли, по организации. За нуждите на контрола най-важно е, че благодарение на нея се разкриват закономерностите и тенденциите в развитието на явленията и процесите. Използват се специфични методи и средства за набиране, групиране, обобщаване и анализиране на данните - изчисляват се средни и относителни величини, индекси и др. Провежда се индексен факторен анализ, корелационен и регресионен анализ и др.

Счетоводна отчетност. В качеството си на информационна и контролна система счетоводството наблюдава, измерва, регистрира, анализира и контролира средствата на организацията, източниците на образуването им, капиталите и другите пасиви и тяхното движение в процеса на кръгооборота им. Нейният обхват е пълен и завършен, което прави счетоводството сигурен и надежден инструмент за ефективно управление. И най-важното - счетоводната отчетност има доказателствена и юридическа стойност.

Сведения

Вземат се когато трябва да се изяснят отделни въпроси свързани с извършено нарушение, нанесени щети или престъпление. Чрез тях може да се допълни съществуващата до момента информация, да се уточни положението на виновното лице в обекта и в населеното място.

Сведенията се вземат от местните органи на власт и управление в лицето на кмет, общински длъжностни лица, съдия, прокурор, полицейски инспектор, дознавател. Те могат да вземат сведения и от други длъжностни лица от обекта (ръководители, счетоводители, подотчетни лица), които могат да помогнат да помогнат за разкриването на характера на деянието и облика на лицето, което го е извършило. За тази цел сведенията могат да бъдат взети писмено или устно и се добавят за уточняване на изводите от контролния орган в процеса на предварителното производство и досъдебното дирене.

Справка

Тя е способ с широко приложение в контролната практика. Може да бъде писмена или устна. Устната има по-малка практическа значимост, тъй като при нея не може да се осигури спазването на изискванията, но които трябва да отговаря. Тези признаци доближават устната справка до сведението. Писмената справка се използва, когато трябва да се изучат процеси и явления, когато в контролирания обект не се води специален информационен носител. В този случай информацията, която ще съдържа справката има вторичен характер. Тя се формира въз основа на различни първични носители. Възможно е тази информация да се преработи за нуждите, за които се иска справката. Контролният орган определя формата и целта, за която се

иска справката. Самото съдържание на справката се формира от специалисти в контролирания обект или от субекти, които се намират в делови отношения с този, който се проверява.

Анкета

Използва се за набиране на допълнителна, помощна информация, необходима за формиране на цели, задачи на предстоящи ревизии, обследвания, инспекции и др. Това не изключва нейното провеждане в рамките на тяхното протичане. До подобни анкети се стига, когато събраната информация не може да послужи за целта, за която се провежда анкетата, а възниква нуждата от допълнителна информация.

Анкетата може да бъде писмена или устна. За провеждане на писмена анкета се съставя въпросник, по който се дават отговорите. Въпросникът се оформя като анкетен лист, който в последствие се обработва. Обработката се извършва по предварително определени критерии, свързани с целта на контролната дейност.

Интервю

Интервюто се използва като средство за установяване на контакт с персонала на организацията и събиране на качествена информация, която практически не може да се получи от документите или анкетите, например за степента на мотивация, предложения за усъвършенстване на работата, за неформалните връзки, за вътрешните конфликти, информация от личен характер и др. Интервюто обаче изисква по-голям разход на време, а ефективността му зависи от професионализма на интервюиращия, но получаваната информация оправдава положените усилия.

Интервюто е директен метод, тъй като изправя лице в лице контролиращия орган и респондентите, дава възможност да се видят непосредствените емоции и реакции и да се получи богата информация за това, което става в организацията. То е особено подходящо за събиране на данни за атитюдите, перцепциите и поведението на хората в трудовите ситуации. Интервюто обаче в сравнение с въпросниците предполага по-голяма гъвкавост, тъй като могат да се задават въпроси, които не са предварително предвидени и формулирани, но се оказват значими за разкриване на нужната информация.

2.6. Фотоснимка

Намира приложение и се практикува основно в криминалистиката. Добри резултати от нейното използване се получават, когато е налице разпиляване, умишлено повреждане, разбиване на складове, каси, магазини, офиси и присвояване на стоки и вещи. Може да се използва и когато видимо се докаже, че е проявена безотопанственост, установена кражба на имущество и при убийства. Използват се различни видове снимки, чрез които по нагледен начин се показват направените констатации по време на извършените контролни действия.

В практиката намират приложение следните видове фотоснимки: ориентиращи, обзорни, възлови, детайлни и позиционни.

2.7. Инвентаризация

Инвентаризацията е процес на подготовка и фактическа проверка чрез определени способности на натуралните и стойностни параметри на активите на организацията към точно определена дата, съпоставяне на получените резултати със счетоводните данни и установяване на евентуалните разлики. Използва се за проверка на парични средства, материални запаси, дълготрайни активи, незавършено производство и разчети.

По обхват инвентаризацията е цялостен процес, състоящ се от няколко дейности - издаване на заповед, формиране на комисия, подготовка на програма, инвентаризация, описване на наличностите, съставяне на сравнителна ведомост и отчитане на резултата.

В зависимост от повода, обхвата и времето на провеждане инвентаризациите имат различна *класификация*:

А. В зависимост от времето и повода за провеждането, инвентаризациите биват: редовни (планови) и извънредни инвентаризации.

Б. В зависимост от обхвата на обектите, инвентаризациите биват: пълна и частична инвентаризация;

2.8. Документална проверка

Използва се както от вътрешните, така и от външните контролни органи. Същността на способа се състои в преценка на правилността и съдържателността на документите при тяхното съставяне.

В работата на контролните органи основно място намират следните документални проверки: Формална; Фактическа; Пълна; Частична; Изчерпателна; Целева; Кръстосана; Верижна проверка; Систематизирана проверка и Несистематизирана проверка.

2.9. Писмени обяснения

Писмените обяснения заемат определящо място в работата на вътрешните и външните контролни органи. Чрез тях се изучават причините, условията и начините на извършване на нарушенията, престъпленията и кръгът на участниците. Характерно за тях е, че се дават лично от виновните (заподозрените) лица, като при нарушения са предвидени имуществена и дисциплинарна отговорност. Такива обяснения се вземат и при наличието на предпоставки за наказателна отговорност, при накръняване на имуществените и финансови интереси на организацията (държавата). Контролният орган не участва в даването на обясненията от виновните лица, като за целта дава най-общи указания за написването им. Съдържанието на самото писмено обяснение е дело на лицето извършило нарушението. То трябва добросъвестно да изложи фактите, обстоятелствата и подбудите за извършеното нарушение.

Разпит

Разновидност на писмените обяснения е разпитът на виновното лице от контролния орган. Желателно е контролният орган сам да проведе разпита, тъй като той най-добре познава обстановката и фактите до момента, а по време на разпита те могат да се потвърдят или отхвърлят. Когато контролният орган няма необходимата подготовка или възможности, разпитът следва да се проведе от органите на дознанието. Основната цел е да се разкрие обективната истина за извършеното нарушение или нанесени щети.

Положителен резултат от разпита на едно лице може да се постигне само, ако контролният орган е разработил добър модел на своето поведение. Разработва се тактиката на разпита, която следва *определена технология* и обхваща няколко елемента: подготовка на въпросите, формиране на поведение от контролния орган, резултат от разпита и документиране на показанията.

2.11. Претърсване и обиск

Претърсването и обиска са способи главно на полицията и правораздаването. Тези способи намират приложение и в практиката на данъчните и митническите

власти, когато се налага събиране на доказателствени средства по нарушения с престъпен характер.

Претърсването и обиска са самостоятелни способности, но най-често те са взаимно свързани - единият предполага използването на другия.

Претърсването е функция на специализиран орган за контрол и за да го осъществи, той трябва да има съответните документи от съда или от прокурор - надлежно оформено решение. По принцип претърсването се извършва през деня и в присъствието на свидетел (поемно лице). Осигуряването на свидетел е важна част от процедурата, тъй като нейното неспазване прави усилията ненужни, а набраната информация неправомерна, излишна и без доказателствена сила. Претърсването в отделни случаи е свързано с взаимодействието и с други контролни органи или органи на властта и правовия ред. Когато се налага претърсване на чуждестранни субекти (офиси, транспортни средства и други) се налага участието на прокурор, полицейски инспектор и представител на съответната държава или организация със съответните правомощия. Когато има отказ, закона позволява при спазване на съответните процедури за насилствено (принудително) навлизане в контролирания обект. Забранено е да се изнасят публично данни, касаещи личния живот на претърсваното лице.

Обискът може да се използва от всички органи на финансовия контрол. Най-голямо приложение намира в работата на данъчните, митническите, правораздавателните и органите на дознанието. Той може да има самостоятелно приложение или да е под формата на част от претърсването. До обиск се претърсва, когато се породни съмнение, че има укриване на доказателствени средства в присъстващите лица.

Обискването е съпроводено с някои конкретни изисквания към контролните органи. То трябва да се извършва от лица от същия пол, от който е лицето, което ще бъде подложено на обиск. Обиска се извършва в присъствието на свидетели, които трябва да бъдат от същия пол. Обискът се извършва лично от контролния орган, като се обискат дрехите и вещите. Обискът се извършва от опитни лица с необходимите знания, опит и компетенции, като спазва необходимата процедура и технология.

Резултатите от обиска и претърсването се оформят в протокол, в които се посочва датата, мястото, името и длъжността на лицето извършило проверката и имената и адресите на свидетелите. Подробно се описват намерените вещи, пари и ценности, намерени по време на обиска или претърсването, които могат да служат като доказателства или допълнителна информация към общата преписка.

Развитието на обществените отношения, пораждаат нови процеси и явления, които противоречат на законодателството и нормативната уредба на страната. Тези промени налагат усъвършенстване на методите за контрол и необходимостта от нови знания, умения и навици на контролните органи.

Литература:

1. Арабаджийски, Н., Основи на публичната администрация, Специална част, София, 2005 г.
2. Бакалов, Й., Теоретичен модел на политика за сигурност и граждански контрол на Република България, С., 2011 г.

3. Балабанова, Хр., Административен контрол, В., 2004 г.
4. Гарнизов, В., Третият сектор в България: статистика, тенденции, събития. В: „Инициатива за подкрепа на гражданското общество в България”, Асоциация АКСЕС, С., 2003 г.
5. Гражданският контрол в Република България. Принципи, параметри, практики. Асоциация АКСЕС и издателство „Отворено общество”, С., 1999 г.
6. Динев, М., Контрол в социалното управление, Изд. „Тракия М”, С., 1999 г.
7. Иванов, Х., Гражданското общество и концепции за граждански контрол, С., 2002 г.
8. Йончев Д., Слатински, Н., Трифонов, Т. и др. Демократичното общество и гражданския контрол върху системата на национална сигурност. Сравнителен анализ и културни особености, С., 1997 г.
9. Къндева, Е., Публична администрация, С., 2007 г.
10. Рачев В., Аврамов, О., Кръстев, И., Национална сигурност и демократизация на гражданско-военните отношения в България, изд. „Албатрос”, С., 1976 г.
11. Сачев, Е., Културното наследство и националната сигурност, С., 2005 г.
12. Сачев, Е., Цивилизация и социокултурноисторическа сигурност, С., 2010 г.
13. Стойкович, В., Идентичност и толерантност, Сп. „Демократически преглед”, 1999 г., с. 20-25.
14. Томов, Й., Теория на контрола и одита, Изд. „Ценов”, Св., 2002 г.
15. Фотев, Г., Гражданското общество, С., 2002 г.

СЪЩНОСТ И СВОЙСТВА НА ОСНОВНИТЕ МЕТОДИ ЗА КОНТРОЛ

Христо А. Христов

THE CONTENT AND FEATURES OF BASIC CONTROL METHODS

Hristo A. Hristov

Abstract: *The control is one of the basic activities done by public organizations and the institutions of security sector in the Republic of Bulgaria. In relation to this the report examines the content and the features of basic control methods*

Keywords: *Sector of security, control methods, analysis, synthesis, foresight, deductive and inductive methods, research, survey, investigation, modeling and expert judgment.*

Контролът е основна дейност осъществявана от организациите на публичния сектор и институциите от сектора за сигурност в Република България. В тази връзка доклада изследва същността и свойствата на основните методи за контрол.

Метод за контрол - съвкупност от научно-теоретични и практически познания и умения, използвани от органите на контрол, за получаване на неизвестна до момента контролна информация за обекта.

Това може да е нова информация, а също така и информация, потвърждаваща дадено състояние или разкриваща отклонения от предварително определена норма на поведение на обектите. Чрез метода се разкриват закономерностите в развитието на явленията и процесите, търси се нещо ново, което не е известно до момента, което е ново за самия субект на контрол.

Докато методът за контрол дава нови широки знания за обектите, то за разлика от него, *способът* се използва за получаване на определена информация. Той се отличава с конкретност и целенасоченост и може да се използва само в определени случаи. Ето защо способите могат да се разглеждат като практически подходи за изучаване на конкретни процеси и явления, обект на контрола.

Изключително полезно за работата на контролните органи е да се познава не само отделния метод и способ, но и резултатите от тяхното комбинирано използване при изучаване на обектите и процесите в хода на контролната дейност. Един метод може да намери своята практическа приложимост при комбинирането на няколко способа.

Съществено значение за характеризиране на метода за контрол има разкриването на неговите свойства. **Основни свойства**, които характеризират един метод за контрол са:

- **Разбираемост на метода.** Методът за контрол трябва лесно да се възприема от субекта на контрол. Свойството "ясен метод" мотивира субекта да го използва в неговата практика. Метод, който трудно се осъзнава, няма приложимост и не се използва в контрола.

▪ **Целенасоченост.** Явленията и процесите, които съставят материалния свят, имат свои характеристики и особености, развиват се във времето по свой начин и стават обект на контрола. Тяхното изучаване може да стане чрез използването на определени подходи и знания, което предполага използването на такъв метод, който ще позволи постигането на поставената цел при най-малък разход на време и средства. Целенасоченост на метода за неговото прилагане изисква неговото изучаване и познаване. Целенасочеността следователно е тясно свързана с конкретността на приложение, което показва, че методът има известни ограничителни рамки, в които може да се използва.

▪ **Надеждност.** Надеждността може да се разглежда като осмислено желание за постигане на очакван резултат. Субектът на контрол използва определени подходи, процедури и тактика, за да постигне очаквания резултат, следствие от отклоненията и нарушенията в мениджмънта и законността. От тази позиция се подбира и метода, който ще се използва. Избира се най-надеждния метод, който осигурява увереност на субекта, че ще постигне целта.

▪ **Резултатност.** Чрез нея се изразява количествена, качествена и стойностна характеристика на постигнатото. Тя е следствие от изпълнението на поставената цел. Резултатът може да бъде положителен или отрицателен. Резултатът е положителен, когато се потвърди издигната версия и изпълни поставената цел. Резултатът е отрицателен, когато не са изпълнени целите и се налага създаването на нова версия, с нова цел и нови разходи на време, енергия и средства. Следователно резултатността е качествен показател и изразява ефективността, икономичността и ефикасността от контролната дейност.

▪ **Икономичност.** Това свойство на метода за контрол намира израз в съкращаване на разходите, които са планирани чрез план - сметката за контролната дейност на един обект или процес. Икономичност е реализирана тогава, когато е изпълнена целта в рамките определения бюджет.

2.2. Общи методи за контрол

Научната теория е създала множество методи за контрол. За нуждите на практиката приложение намира този метод или онази комбинация от методи, с която се постига поставената цел при най-малък разход на средства, време и ресурси.

Всеки метод на познавателния процес може да намери приложение в областта на контрола, но широко практическо приложение са намерили диалектическият метод, анализа, синтеза, дедукцията, индукцията, прогнозирането и др.

А. Диалектически метод. Той намира широко приложно поле, тъй като изучава процесите и явленията - обект на контрола, в динамика и в развитие. Това позволява на контролните органи да установят какви изменения са настъпили на развитието във времето и има ли отрицателни тенденции или симптоми. Въз основа на този метод може да се прогнозира очакваното състояние на обектите.

Освен в динамика, контролираният обект може да бъде изучаван и в статика. Изучаването на процесите и явленията в статика характеризират обекта в неговото моментно състояние, което е пречка за установяване на причините допринесли за промените (положителни или отрицателни). Тъй като във всеки следващ момент това състояние ще се променя, това изменение е основната предпоставка за продължаване на контролния процес (чрез диалектиическият метод), за да се обхване цялостното развитие на явленията и процесите.

Б. Анализ. В практиката се прилага сравнителен, факторен, стойностен и други видове анализ, в зависимост от нуждата на субекта на контрол. Той стои в основата на последващия контрол, когато трябва да се изучават крайните резултати и факторите, които са повлияли върху дейността на обектите.

Методът се отличава с точност и създава възможност да се установи не само наличието на отклонение, но и неговата стойност. Базира се на цифровия материал набран от първичните документи, счетоводните отчети и баланси и др.

Факторен анализ - процес на селектиране, сравнение и оценка на информация с цел установяване на съществени връзки, взаимоотношения и тенденции в дейността на контролирания обект.

Факторният анализ представлява методика за изучаване и измерване въздействието на факторите върху величината на резултативните показатели на определен обект.

Под фактор обикновено се има предвид:

- активно действащи сили, предизвикващи положителни или отрицателни изменения в състоянието на изследвания обект и на показателите, които го отразяват, т.е. причините за тези изменения;
- условия, необходими за протичане на различните процеси;
- самостоятелни структурни елементи в системата от причинно-следствени връзки на резултативното явление.

Основни задачи на факторния анализ:

- Подбор на факторите, които влияят върху резултативните показатели.
- Класифициране и систематизиране на същите фактори.
- Определяне формите на зависимост между факторите и резултативния показател.
- Моделиране на взаимовръзките между резултативните и факторните показатели.
- Изчисляване влиянието на факторите и оценяване ролята на всеки един от тях в изменението на величината на резултативния показател на контролирания обект.

Количествен анализ. Насочен е към неотчетения, "изкуствен" излишък. В теорията и практиката този анализ е известен като количествен анализ при стойностно отчитане на стоките, което показва, че той е насочен към изучаване на излишъци, формирани в различни сфери. Излишъците се създават чрез манипулации и измами и представляват като явление обществена опасност. И в сферата на производството и в сферата на обръщението създават условия за ниска конкурентност и нелоялност между пазарните субекти.

В зависимост от обхвата, количественият анализ може да бъде пълен или частичен. *Пълен* количествен анализ се извършва тогава, когато чрез него се обхваща движението на всички материални запаси в анализирания обект и период. Чрез *частичния* количествен анализ се обхваща част от материалните запаси - отделна група или отделен вид.

В. Синтез. Той се намира в тясна връзка с анализа, като целта на този метод е да установи отклонението в сумарно изражение. Чрез него отделните части на контролираните обекти се изучават в единство и взаимодействие. Той дава информация както за цялото, така и за структурата на отделните му съставни части. За целта контролните органи съставят таблици, които отразяват отклоненията от нормата и измеренията на отделните фактори, повлияли върху това изменение.

Г. Дедуктивен метод

При дедуктивния метод принципният подход е от общото към конкретното. Той насочва контролното въздействие към оценка на резултатите от поведението на човека, за да се изследват мотивите за него. Изследването на всички резултати и всяка мотивация на поведение не е самоцел, а организирано насочване на контрола към групиране на типични случаи на поведение, към задълбочено установяване на закономерния резултат от определено поведение и характеризиране на мотивите в тяхната индивидуална и комплексна форма на проява. Този своеобразен подход на моделиране на личностните поведения има за цел да определи границите, критичните точки в поведението, които винаги водят до съществени отклонения, затормозяват общото развитие. Отличното познаване на признаците на поведение на характерните групи мотиви, които могат да се контролират, създава условия за точна и ненапращваща проява на контролната функция.

Дедуктивният метод съдейства да се изследват неформални норми и правила за поведение на индивида в дадения колектив. Нормативно изградените взаимоотношения (чрез закони, наредби, правилници и др.) сравнително лесно се контролират. Но това е неимоверно трудно при неформалните норми и правила за поведение на личността в колектива. Безспорно има условия да нарастват формализираните норми за поведение, но не това е целта на социалния контрол.

Д. Индуктивен метод

Чрез индуктивния метод последователно се изследват мотивите, техните специфични особености и форми на проява, поведението, което поражда всеки мотив или комплекс от мотиви. Доброто познаване на дедуктивния метод в контрола улеснява подхода към индуктивния метод, защото тук отново се търси закономерното, повтарящото се, онова, което насочва личността към колективното действие и решение.

Постиженията в индуктивния метод също са предпоставка за развитието и усъвършенстването му. При индуктивния метод се създава основата на мотивацията в поведението на личността и в този смисъл е възможно да се приложи за конкретно изследване на всяко личностно поведение.

Е. Прогнозиране

Прогнозирането е обосновано предвиждане на възможните варианти за развитие на контролиран обект и вероятността те да се реализират.

При прогнозирането се установяват закономерностите в развитието, проблемните въпроси, като се определят възможните отклонения от утвърдените показатели и норми. Въз основа на този метод се изграждат системи за стратегически контрол, чрез които се извършва оценка на бъдещото развитие на обектите. При тях контролът е на входа на обекта, в резултат на което се постига превантивност на дейността. Въз основа на очертаващите се закономерности в развитието на явленията и процесите и при зададена норма, субектът за контрол предвижда момента и къде точно ще се появят отклоненията. Въз основа на получената информация се вземат решения за предотвратяване на отклоненията.

Методи за прогнозиране: Методи, основаващи се на тенденции; Методи, които се основават на причинно-следствени връзки; Методи, които се основават на отразяването на комплекс от връзки между фактори и прогнозираните величини; Методи, основаващи се на специфични зависимости; Методи, основаващи се на използването на експерти; Нормативни методи. Ориентирани са към определяне на

цели. Към тях могат да бъдат отнесени „дървото на целите“, „морфологичният анализ“ и др.

2.3. Специфични методи за контрол

Тези методи са класифицирани според специфичните особености на обекта и субекта на контрол. Групата на специфичните методи включва:

обследване, проучване, разследване, експертна оценка (експертиза), моделиране и др.

2.3.1. Обследване

Обследването е метод, който съдейства да се изследват всички, но главно съществени страни на едно или няколко явления или процеси. При обследването има налице както комплексно развиващи се процеси, обект на контрола, така и комплексно комплектуван субект на въздействие. Обследването има характер на „масов“ метод, в неговата реализация участват множество контролни органи.

Независимо, че чрез обследването се обхваща цялостната дейност на обекта, то няма изчерпателен характер. В основата на неговото провеждане стоят онези параметри, които определят облика на обекта, които дават представа за резултата от неговото развитие. Такива параметри могат да бъдат основните показатели за резултатите от дейността на обекта или задачите, които е трябвало да бъдат изпълнени. Резултатът от обследването се оформя в служебен доклад, съставен в два едно-образни екземпляра. Той се извежда в изходящ дневник на обекта. Първият екземпляр се изпраща на този, който е издал заповедта за обследването, а втория остава в самия обект. Данните от обследването могат да послужат за възбуждане на определени контролни действия.

2.3.2. Проучване

Проучването като метод за контрол е свързано винаги с определена необходимост. Осъществява се въз основа на писмена заповед или разпореждане от оторизирана институция за възлагане на контрол. При него винаги се определя обектът и целта на проучването, другите методи, които ще бъдат използвани в комбинация с проучването, както и необходимите ресурси – материални, човешки, финансови и времеви. Много често проучването допълва наблюдението. Може да се проучи какво е поведението на целия обект, на негови поделения или отделни ръководители. Обект на проучването може да бъде минала дейност, моментно състояние или бъдещо развитие. Важно условие при проучването е то да се основава на най-новите достижения на човешкото познание в дадената област.

Следователно, то трябва да се извършва от контролни органи, притежаващи съответната теоретическа и практическа подготовка по контрол и другите научни направления, които ще имат отношение към целта на проучването. При необходимост може да се формира комплексен колектив от взаимно допълващи се специалисти и експерти за извършване на проучването.

2.3.3. Разследване

Разследването се използва за установяване съответствие между действията на служебните (контролираните) лица, изискванията на законовата уредба и нормативните актове, и резултати получени от тези действия.

То е способ, който се отличава с конкретност и целенасоченост. Използва при определени обстоятелства. Такива обстоятелства могат да бъдат установяването на щета, престъпление и други поводи, възникнали в резултат на осъществени контролни действия.

Разследването може да се разглежда и като процес, състоящ се от различни елементи, подредени в определена последователност.

2.3.4. Експертна оценка (експертиза)

Експертната оценка се прилага при задачи с висока степен на сложност, които трудно могат да бъдат решени с други методи. Главната цел на експертното оценяване е по-лесно да се преодолява високата степен на неопределеност и на риск, характерни за целия комплекс от фактори, които се анализират при диагностиката на сложни обекти.

Експертният метод е качествен. Той се основава на интуитивно-логически съждения на експерти за състоянието и развитието на определен обект или процес. Оценките се изграждат върху наличната информация, опита и знанията на специалистите. Този метод се използва в анализа поради възможностите, които предоставя за преодоляване на неопределеността, свързана с дефицит на количествена или конкретна фактическа информация.

Експертизата се назначава от оправомощен орган, като се съгласува с ръководителя на обекта. Резултатът се оформя в експертно заключение, в което по недвусмислен начин се отразява установеният резултат по време на експертизата.

За нуждите на контрола се използват графологична, дактилоскопична, ветеринарна, медицинска, техническа, счетоводна и други видове експертизи. Всяка от посочените има точно определен обект и предмет за контрол.

2.3.5. Моделиране

Моделът е естествен или изкуствен обект със свойства (форма, структура, начин на функциониране и т.н.), близки до оригинала, който искаме да изследваме.

А. Цели на моделирането

- а) да се разбере същността на изучавания обект;
- б) да се научи да се управлява обектът и да се определят най-добрите начини за управление;
- в) да се прогнозира преките и косвени последствия;
- г) да се решат приложените задачи.

Б. Видове моделиране

Съществуват няколко вида моделиране, които могат да се групират в две основни групи:

- материално - веществено моделиране - моделът е реализиран като материален обект (система, опитна уредба, устройство, машина и т.н.);
- абстрактно - логическо моделиране - моделите се представят чрез средствата на математиката.

Според състоянието на моделираните обекти на контрола във времето моделите са: модел на фактическото състояние, модел на възможното състояние и модел на желаното състояние. Тези разновидности съответстват на потребността на социалния контрол да изследва събитията в тяхното минало, настояще и бъдеще, да търси и улавя, да измерва и оценява тенденции и закономерности в своя обект.

В научните разработки за контрола са известни още и т.нар. модели на проблемните ситуации. Те се създават при наличие на отклонения във фактическото от

зададеното състояние и утвърдена концепция за изменения чрез определен набор от мероприятия. Естествено е да се предполага, че и тук разнообразието в подхода е необходимост, за да се изследват възможните варианти на въздействие, да се създадат нови, най-подходящи модели за решения, изобщо в лабиринта от налични отклонения да се избере най-точното решение към желаното и очакваното състояние на обекта.

ЛИТЕРАТУРА:

1. Арабаджийски, Н., Основи на публичната администрация, Специална част, София, 2005 г.
2. Бакалов, Й., Теоретичен модел на политика за сигурност и граждански контрол на Република България, С., 2011 г.
3. Балабанова, Хр., Административен контрол, В., 2004 г.
4. Гарнизов, В., Третият сектор в България: статистика, тенденции, събития. В: „Инициатива за подкрепа на гражданското общество в България”, Асоциация АКСЕС, С., 2003 г.
5. Гражданският контрол в Република България. Принципи, параметри, практики. Асоциация АКСЕС и издателство „Отворено общество”, С., 1999 г.
6. Иванов, Х., Гражданското общество и концепции за граждански контрол, С., 2002 г.
7. Йончев Д., Слатински, Н., Трифонов, Т. и др. Демократичното общество и гражданския контрол върху системата на национална сигурност. Сравнителен анализ и културни особености, С., 1997 г.
8. Къндева, Е., Публична администрация, С., 2007 г.
9. Сачев, Е., Културното наследство и националната сигурност, С., 2005 г.
10. Сачев, Е., Цивилизация и социокултурноисторическа сигурност, С., 2010 г.
11. Стойкович, В., Идентичност и толерантност, Сп. „Демократически преглед”, 1999 г., с. 20-25.
12. Томов, Й., Теория на контрола и одита, Изд. „Ценов”, Св., 2002 г.
13. Фотев, Г., Гражданското общество, С., 2002 г.

МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ 2017

СБОРНИК ДОКЛАДИ

Издание първо. Тираж 25

Предпечатна подготовка във Факултет “Артилерия, ПВО и КИС” - Шумен