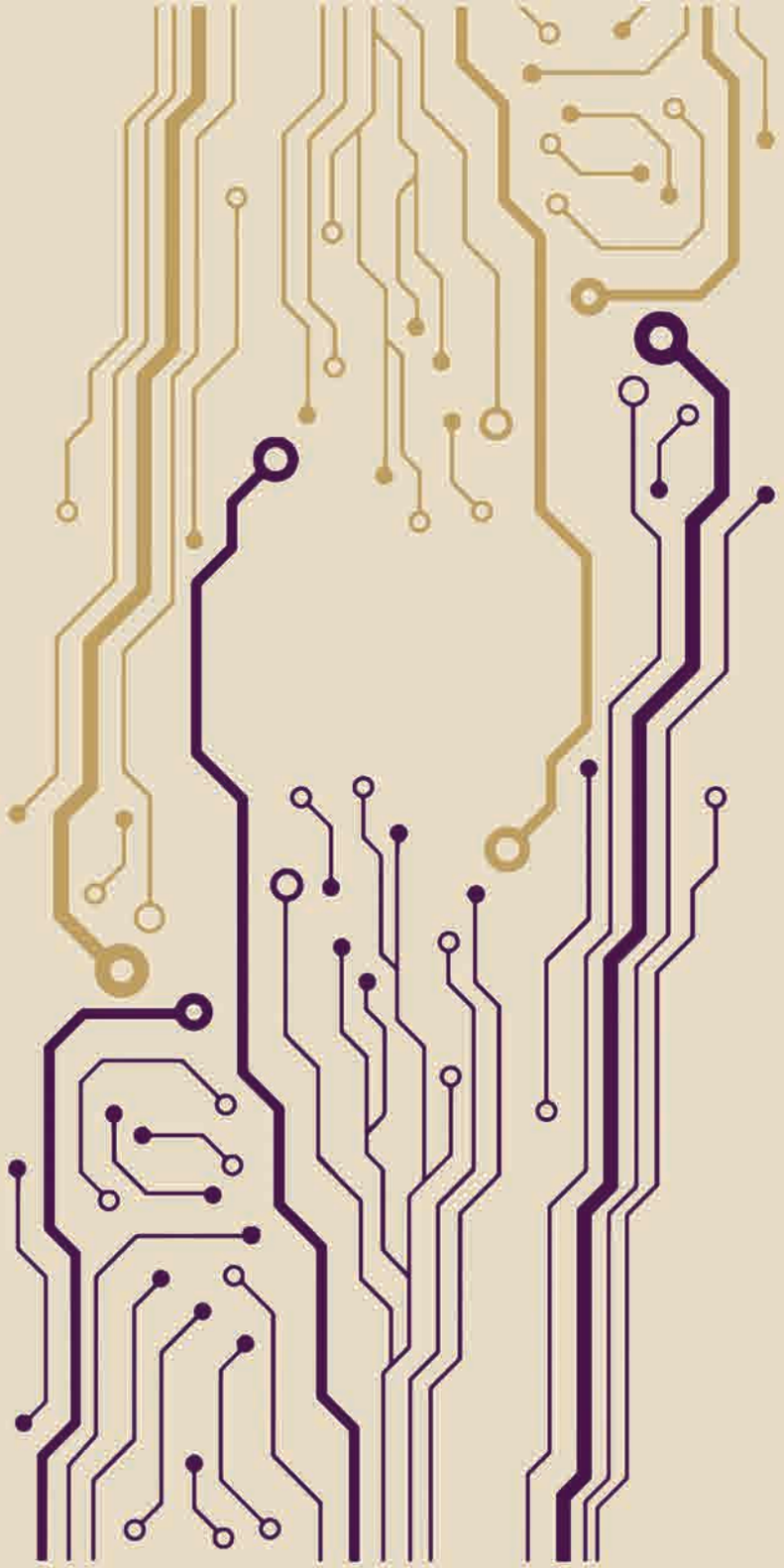

ГОДИШНИК

НА ШУМЕНСКИЯТ УНИВЕРСИТЕТ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

ТЕХНИЧЕСКИ НАУКИ

Т. VIII Е

ANNUAL

OF KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN

T. VIII E

FACULTY OF TECHNICAL SCIENCES

Универистетско издателство
“Епископ Константин Преславски“ 2018

ANNUAL

OF

KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN

VOL. VIII E

FACULTY OF TECHNICAL SCIENCES

Konstantin Preslavsky University Press 2018

ISSN 1311-834X

Content

ANALYSIS ON REASONS FOR APPLIED FINANCIAL CORRECTIONS CONNECTED WITH PUBLIC PROCUREMENTS FROM BENEFICIERIES WHO HAVE SIGNED A CONTRACT FOR A GRANT FINANCIAL ASSISTANCE WITH AGRICULTURE STATE FUND UNDER RURAL DEVELOPMENT PROGRAMME 2014-2020

Hristo A. Hristov

ABSTRACT: *The current report reflects the results of controls carried out by Agriculture state fund in accordance with procedure for performing prior evaluation and ex-post controls on public procurement procedures for approved investment costs, entirely or partially financed by the European Agricultural Fund for Rural Development.*

KEYWORDS: *Procurement, tender, Public Procurement Act, irregularities, experts, non-discrimination, award procedure, errors, public contract, the European Agricultural Fund for Rural Development, Agricultural State Fund.*

1. Introduction

The current report reflects the results of controls carried out by the Agriculture state fund in accordance with procedure for performing prior evaluation and ex-post controls on public procurement procedures for approved investment costs, entirely or partially financed by the European Agricultural Fund for Rural Development.

The most frequent public procurement irregularities can be grouped in the following way:

- Irregularities related to the preparation and opening of public tender procedures;
- Irregularities associated with conducting public procurement procedures;
- Irregularities in the performance of public procurement contracts [1], [18], [19], [20], [21], [22].

2. Errors related to preparation and opening of the procedure for awarding a public contract.

Most important is the group of mistakes that are made in connection with the preparation of the public procurement award and its announcement, that is to say, when formulating its subject matter and the choice of the order in which it will be conducted, when formulating the selection and award criteria, the technical specifications and the assessment methodology, as well as when the contract notice is sent to the respective publications institutions within the statutory time limits [2], [3], [4], [5], [6], [7].

1.There are identified cases where the grantor has not conducted the award procedure of a public contract which the law has prescribed.

In some cases, the contracting entities do not carry out the statutory procurement procedures, even though there are grounds provided by PPL.

In other cases, negotiated procedures are incorrectly executed, although there are preconditions for open procedure under PPL. The reason for that is misinterpretation and wrong implementation by contracting authorities of Art. 84, Art. 90 of Public Procurement Law (PPL) or of Art. 53, part. 1 of Ordinance for Award of Small Public Procurement Contracts (OASPP, repealed) in connection with Art. 5, para. 1, item 2 of Public Procurement Act.

2. Looking at the practice of Agricultural State Fund, breaches with the greatest financial consequences for the beneficiaries are those related to the prohibition under Art. 25, Paragraph 5 of Public Procurement Act, namely the documentation for participation does not lay down conditions that give priority or unjustifiably restrict the participation of individuals in the procedure. In most cases, the error is related to the formulation of selection criteria for the participants or to the submitted documents that are evidence for selection criteria [8], [9], [10], [11], [12], [13], [14].

The selection criterion is related to the financial and economic situation of the participants, their technical capabilities and their professional qualification. The selection criteria should be consistent with the subject, character, value, quantity and volume of the public procurement in order to be lawful and to ensure the principle of equality and non-discrimination.

2.1. In connection with the definition of requirements for financial and economic participants' status there are the following unlawful practices: / mistakes before amendments in PPA in force from 2014, July /

- Regarding the total turnover of the participants - it is not in line with the forecasted value of the procurement;
- Concerning the specific turnover of the participants - the same does not comply with the estimated value of the order; the activities - sources of turnover - are not related to the subject of the public procurement - for example, the contracting authority requires the specific turnover to be calculated only based on activities that are funded with funds from the

European Union or activities carried out on the territory of the Republic of Bulgaria, and for a specific type of contracting entities (eg. state or municipal administration); the specific turnover is required to represent not less than 80% of the total turnover of the participant, etc [40], [41], [42], [43].

- Regarding the requirement for free available financial resource - a certain source of free resource - for example, the contracting authority requires for the funds to be on credit, excluding the possibility of bank deposit or means at hand (provided by other persons - non-financial institutions); excessive amount of free financial resources - it is not in accordance with the order in which the payments for activities of public procurement should be made;

2.2. The grantors make mistakes in determining requirements for the technical capabilities of the participants and, in this context, the following unlawful practices are identified in the procedures of the Agriculture State Fund.

Concerning the participants' experience - the requirement for time to gain experience does not comply with Art. 51, para. 1, item 1 and item 2 of the PPA – the grantors define a shorter or longer period of experience acquisition without complying with the fact that it is legally established at 3 years for supply and service contracts and 5 years for construction contracts; the type of experience does not correspond to the subject and nature of the public procurement - the required experience is too specific or too general (for example: when the tender is for repair works in a school - changing of the joinery, repair of toilets and replacement of floor coverings - the grantor requires experience concerning similar activities in educational and health institutions); requirement for a certain number of completed contracts showing required experience in the subject matter - the contracting entities require participants to demonstrate that they have completed ten or fifteen contracts, similar to the public procurement (number of executed contracts doesn’t necessary fulfill the requirement for the participant to prove past qualitative performances to the procurement activities) [15], [16], [17], [18].

Concerning the ownership of the technical equipment for implementation of the contract - the contracting authorities require the participants to prove that equipment is their own or, in relation to the equipment, a specific type of contract has been concluded with the owner, ignoring art. 51a of the PPA which gives an opportunity for participants in the order to use the resources of other natural persons or legal entities. If the participants prove in an appropriate manner that they have the opportunity to use the foreign resources, the contracting authorities will be obliged to allow them to participate in the procedure.

• The requirements for completed contracts are set contrary to last amendments in Article 51 of PPA.

2.3. In some cases, the requirements for the professional qualification of the participants are formulated in contradiction with the prohibition under Art. 25, paragraph 5 of the PPL:

• Regarding the duration of the experts' experience - the contracting authorities formulate experience requirements for key experts whose duration does not comply with normative requirements for the implementation of the certain activity, or with customary practice in the relevant sphere;

• Regarding the essence of the required experience of the experts - the contracting authorities place requirements to the experts for experience in projects, funded by the EU, although the specific activities that experts will do are built on the skills, standards and rules applicable in relevant sectors, irrespective of the financial source of the order;

• Regarding the number of experts – the contracting authorities require the participants to prove that they had employed a certain number of employees on a contractual basis for the previous one or three years- there is no justification for the number of employees regarding construction contracts exceeding to great extent the legal minimum required for the registration of economic operators in Central Professional Builders Register for the relevant category construction works [40], [41], [42], [43];

2.4. The principle of equal treatment and non-discrimination requires the conditions of the order to be the same for all types of participants - both natural and legal persons and associations of such persons who are not registered as legal entities. That's why it is unlawful formulation of other different requirements regarding associations of participants that are not registered as a legal entity. In practice The Agriculture state fund has identified specific requirements for participants in cooperative unions - for example, requirements to economic, financial and technical capabilities refer to each member of the union; wholly or 80 % of total / specific turnover to be realized by one of the participants in the unification (leading party); the experience has been fully acquired by one of the participants in unification etc [19], [20], [21], [22], [23], [24], [25], [26], [27], [28].

2.5. There are essential requirements regarding the observance of the principles under Art. 2 of the PPL formulated by the contracting entities, relevant to the personality of participants - their legal capacity and in particular the possession of licenses or registration in certain professional registers. Most often in practice of Agricultural State Fund there are unsubstantiated overruns for construction contracts concerning the requirement for registration in the Central Professional Register of Builders - for example, the issued building permit is for construction of a second

category, and the participants are required to be registered in the Central Professional Register of Builders for the first category of construction works.

2.6. A key set of conditions that the assignor formulates when awards a contract are those related to the technical specifications. Regarding the outcome of the procedure it is also important that these technical specifications provide equal access to the contract and do not place unjustified barriers to competition under Art. 32, paragraph 1 of PPL. The most common unlawful practice related to technical specifications is the use of specific brands and models in the preparation of

Quantitative bills for construction or services without the words "or equivalent" - for example, a specific primer, grass covering or a brand of aerated concrete blocks is mentioned to be used or there is specification of a particular type of system through using a trademark, etc.

3. The other set of requirements that are significant for the outcome of the award procedure of a public contract, are those relating to the assessment criterion. Employers are required to select an evaluation criterion "The most economically advantageous tender" in accordance with formulation of an evaluation methodology that should contain accurate and clear parameters for each evaluation indicators as well as determination of the complex assessment according to Art. 28, para. 2 of the Public Procurement Act. According to practice of Agricultural State Fund the following examples of infringements can be given:

- Regarding the type of the evaluation indicators - under the assessment criterion "economic most advantageous tender", the assignor has formulated assessment indicators that aren't directly related to the subject of the public procurement and stipulate evaluation of the participants' suitability - for example, what is appreciated is the participants' experience or their achieved turnover or professional qualification of the participant's team that is proposed to execute the order. The listed circumstances are related to the financial and economic status of the participants, their technical capabilities and professional qualification and they are criteria for the selection of participants.
- Concerning the content of methodology for evaluation of the tender - the order described for determining the estimates for each indicator and determining the complex assessment is not accurate and clear, which is contrary to Art. 28, para. 2 of the Public Procurement Act. In this way conditions for unequal treatment of the participants are created. In such evaluation methodology the assignor determines only the relative weight of the indicators (for example, 40 points per indicator "execution time of the order "), without specifying the order for awarding the maximum and minimum of points.

• Another unlawful practice established by the Agricultural State Fund is to provide points (even 0) in the methodology for evaluation for tenders, which do not meet the requirements of the contracting authority. According to Art. 69, para. 1, item 3 from PPL such proposals should be removed.

• A practice which is contrary to the PPL is using the so-called "Methodology of the average dimensions " under which maximum points are awarded to the proposal that is closest to the average one within procedure proposals.

4. When public procurement procedures are opened and announced the authority body has set up a group of obligations of the contracting authority that are aimed at providing insurance of the principle of publicity and transparency under Art. 2, para. 1, item 1 of the Public Procurement Act – obligations related to time limit for receipt of tenders, the bodies that should be announced about the procedure and the content of the contract notice. In practice the following unlawful practices are identified by the Agricultural State Fund:

• Regarding the time limit for receipt of the tenders - the assignor has specified an unlawful shorter time limit for receipt of bids with or without unjustified reference to any of the grounds for shortening the term under Art. 64 of the Public Procurement Act. For example: No prior notice was sent with the required information about the public procurement contract or the requirement for providing access in Internet to entire documentation for the participation in the procedure is not observed and there is no internet address in the notice where it can be found.

• Concerning the announcement of the order - the assignor has not sent public procurement notice to the Official European Union Journal, even though the contract has an estimated value that exceeds European thresholds;

• Concerning the content of the public procurement announcement - the contracting authorities often do not specify all the selection criteria and all documents, which prove their performance. In the documentation for participation there are other additional requirements for participants and their suitability and / or documents, which should be submitted in the tender. This violates Art. 25, para. 2, item 6 of the PPL, which requires a comprehensive list of the criteria and the relevant documents. The principle of publicity and transparency under Art. 2, para. 1, item 1 of the Public Procurement Act is also broken;

• Another typical error in this group is the lack of rating indicators of tenders in the contract notice. According to Art. 25, para. 2, item 10 of the PPA the contracting authorities are obliged to indicate the criterion of bids'

evaluation and benchmarks with their relative weight in the announcement if the chosen criterion is "the most economically advantageous tender";

- In some cases, there are differences in the requirements contained in the contract notice and in the rest of the contract documents - for example, in the notice the requirement is that the participant should have a total turnover BGN 2 million and the participation documentation indicates that the total turnover should be BGN 3 million. Such practice creates conditions for unequal treatment of participants.

3. Errors in conducting the procurement procedure

The Commission that conducts the procedure and its activities is of key importance for the results of its conduct. In the course of its activities exclusively important issues are decided - which players should be removed, what should be the ranking of the participants, who will be the contractor. Errors allowed by commission lead to either unreasonable removal of participants or to their unjustified admission to participation. Both types of errors represent breach of the principle of equal treatment and non-discrimination under Art. 2, para. 1, item 3 of the Public Procurement Act. The reasons that cause these errors can be divided into two groups - the first: reasons related to misinterpretation of the applicable legislation, and the second: the reasons for misinterpretation of the documents contained in the tender [28], [29], [30], [31], [32], [33], [34], [35], [36], [40], [41], [42], [43].

1. Errors relating to misinterpretation of the applicable legislation - we have identified a case in which the commission has admitted a number of procedural errors: there is no public hearing for opening the price offers and the same have not been signed by the members of the Commission, the members of the support body have also failed to declare the provisions of the law circumstances (Article 35 of the PPA).

2. Errors relating to misinterpretation of the tender itself - in this group there are cases of unjustified admission and removal of participants (although according to the submitted documents, the participant does not respond to the contracting authority's requirements, the commission did not propose to remove it and / or the participant meets the conditions and requirements of the contracting authority, but it is unlawful removed from the procedure) and removal of participants for default of non - essential requirements of the assignor (for example, missing the number of pages, no signatures on all pages of the offer, bid is placed in a box instead of an envelope, the envelope with the price offer is marked with an inscription "Price" instead of "Offered price", etc.).

4. Errors in concluding and implementing public procurement contracts [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43].

The conclusion and implementation of the public procurement contract is also the focus of controls of Agricultural State Fund. In order to confirm the legality of the expenditure the content of the contract and its compliance with the procurement conditions set out in the opening of the procedure is analyzed as well as the proposals on the basis of which the participant is chosen to perform the order.

The most common errors can be considered conditionally in two groups:

1. Errors relating to the amendment of the conditions for the award and performance of the contract before the conclusion of the contract - there are cases in which the concluded contract for a public contract does not meet either the draft contract contained in the documentation for participation, or the proposals on the basis of which the participant is chosen to execute the order (for example, the draft contract does not include advance payment, but there is a clause for advance payment in the contract; in the concluded contract the amount of the advance payment is increased; the activities of the subject of the contract aren't in line with those set out in the documentation for participation, including the draft contract, without changing the price of the contract). There are cases where prior to the conclusion of the contract, the contract has been amended in several directions at the same time, compared to the project contained in the documentation for participation, eg: the number of additional experts required to implement a specific stage of the contract is changed; the terms of limitation of the stages are changed; the payment conditions for certain employees are changed; additional penalty clauses due by the assignor have been introduced, etc [29], [30], [31].

2. Errors related to the amendment of the public procurement contract – there are practices that amend the contracts and this contradicts to the prohibition on these amendments under Art. 43, para. 1 of the PPA:

✓ Concerning the term for the contracts' execution – according to public procurement construction contracts the contractors allow the change in the time in contract when the project was stopped because of winter conditions. The occurrence of these conditions is not an unforeseen circumstance within the meaning of applicable legislation. Therefore, the reference to Art. 43, para. 2, item 1, a. of the PPA, which allows an exception to the amendment ban, is unlawful.

✓ As regards the subject of the public procurement contract - the award of additional construction or services in cases where there are no unforeseen circumstances is also considered as unlawful amendment of the contract.

3. Conclusion

A number of other omissions have been identified in conducting award procedures of public procurement, which are often of a formal nature. In specific verified cases these weaknesses did not seriously affect the principles for awarding the public procurement and therefore their impact on the financial interests of the EU and the fundamental freedoms of individuals is too uncertain and indirectly emphasized in order to justify the imposition of financial corrections. However, we pay attention to beneficiaries as contracting authorities are required to strictly observe the provisions of the PPL and in the other procedures listed below violations could have a financial effect. Examples of such omissions are:

- ✓ Requiring for participants to submit a document without relevant selection criterion;
- ✓ Lack of deadline for work of the tender evaluation committee;
- ✓ Delay in issuing a decision to announce a ranking and contractor;
- ✓ Delay in sending the order assignment information;
- ✓ Errors in applying the regime for collecting three offers under Art. 2 of the Ordinance for the award of small public procurement (abrogated), etc.

REFERENCES:

1. Special Report of European Court of Auditors № 22/2014: Achieving savings: costs' control under EU financed rural development project grants.
2. Special Report of European Court of Auditors № 23/2014: Errors in disbursement of funds for rural development projects: what are the causes and what measures are taken ?
3. Special Report of European Court of Auditors № 10/2015: Making more efforts to problems with expenditure for public procurement in EU concerning cohesion.
4. Special Report of European Court of Auditors № 12/2015: „Weak management''.
5. Regulation (EU) No 1305/2013 of the European Parliament and of the Council on support for rural development by the European Agricultural Fund for Rural Development (EAFRD).
6. Directive 2014/24/EU of the European parliament and of the Council on public procurement.
7. Guidance of European commission for member states on public procurement and rural development
8. European commission, EGESIF 14-0030 of 29/9/2014 – Guidance for specialists on public procurement on avoiding the most common mistakes in projects funded by the European structural and investment funds.
9. Commission regulation (EU) № 65/2011 27 January 2011 laying down detailed rules for the implementation of Council Regulation (EC) No 1698/2005, as regards the implementation of control procedures as well as cross-compliance in respect of rural development support measures.

10. Council regulation (EC) № 1698/2005 of 20 September 2005 on support for rural development by the European Agricultural Fund for Rural Development (EAFRD).
11. Andreeva G., Andreev A. Survey and analysis of intercultural communication in Bulgaria and abroad. Journal "Scientific and applied research", USA, vol.3, p.89-97, 2013.
12. Andreeva I., Andreeva G., Andreev A. Conceptual models of retirement and promotion employment of older people in Bulgaria. Journal "Science, education, innovation", USA, vol.1, p.137-143, 2013.
13. Andreeva G., Andreev A. Model of intercultural communication in group language learning in military environment. Journal " Science, education, innovation ", USA, vol.1, p.133-136, 2013.
14. Ivanov, M., Intelligence Infrastructure, Sofia, Profisec, 2012, p. 215, ISBN 978-954-32927-1-8.
15. Ivanov, M., Nazism and Islam, MATTECH 2018, Shumen, St. Konstantin Preslavskiy University Publishing House, 2018, ISBN 1314-3921.
16. Ivanov, M., Army and Police - Diffusion of Functions and Tasks, Fourth National Conference with International Participation "Metal Science, Hydro- and Aerodynamics and National Security 2014", Sofia, 2014, ISBN 1313-8308.
17. Савов, И., Рискове и заплахи за сигурността в Черноморския регион, Международна конференция „Проблеми на сигурността в черноморския регион", ВУСИ, септември 2017 г., ISBN 978-619-7343-09-0, с. 7-18.
18. Savov, I. Some aspects of legislative system of the institutes migration and readmission in the European Union, International conference - Law and Security in migration process and the consequences of the migration crises, Nikola Tesla University, Beograd, 2017, ISBN 978-86-6113-046-5, p. 265-277.
19. Савов, И. Структури и организации в Република България свързани с миграцията, Годишник, том XIV, 2017, ВУСИ, ISSN 2367-8798, с. 14-21.
20. Савов, И., Борисов, Т., A look on the nature of agreements for the application of the readmission institute, International conference – European integration, Nikola Tesla University, 2018, Beograd, ISBN 978-86-6113-050-2, p. 45-56.
21. Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Русе, 2017, с.19-27, http://jei.uni-ruse.bg/Issue-2016/02.%20Zagorcheva%20-%20Pavlov.pdf.
22. Zagorcheva, D., Stages in the systems for financial management and control in the Bulgaria's public sector, The XIV International Scientific Conference Information Technologies and Management, 2016, Riga, Latvia.
23. Загорчева, Д, Велчева, Й., Бюджетната децентрализация като фактор за едновременно развитие на общините и индустриалния бизнес, Народностопански архив, година LXX, книга 3 – 2017, ISSN 0323-9004, стр. p.46-59, https://www.uni-svishtov.bg/NSArhiv/title.asp?title=981.
24. Boyanov, P., Educational exploiting the information resources and invading the security mechanisms of the operating system windows 7 with the exploit Eternalblue and Backdoor Doublepulsar, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 14, 2018, pp. 34-41, available at: http://www.rst-tto.com/publication.html.
25. Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University

Press, ISSN 1314-6289, Vol.3, 2013, pp. 114-124, available at: http://www.rst-tto.com/publication.html.
26. Solakov, T., The Bulgarian state and the religious organizations in the period after 1989, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press“, ISSN 1311-834X, Vol. VI E, 2017, pp. 107-119.
27. Solakov, T., Religious fundamentalism and extremism, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press“, ISSN 1311-834X, Vol. VI E, 2017, pp. 120-132.
28. Solakov, T., Radicalism and stages of radicalization, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press“, ISSN 1311-834X, Vol. VI E, 2017, pp. 133-140.
29. Velikov, I., Humanitarian aspects of protection of information, MATTEX 2018 Conference proceedings, Konstantin Preslavsky University of Shumen, ISSN 1314-3921, Shumen, Vol. 2, part 1, 2018, pp. 3-10.
30. Досев, Н., Създаване на склад от данни за определяне на риска за информационната сигурност на корпорацията, Научна конференция с международно участие на тема „Киберсигурността в информационното общество”, Факултет "А, ПВО и КИС", Шумен 2017 г.
31. Досев, Н., Създаване на модел на система за ранно предвиждане рисковете за информационната сигурност на корпорацията, Научна конференция MATTEX на ШУ „Еп. К. Преславски“, гр. Шумен, 2016 г.
32. Досев, Н., Обезпечаване сигурността на достъпа до интегриран склад от данни, Международна научна конференция 2016, Факултет „А, ПВО и КИС“ гр. Шумен, 2016.
33. Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.
34. Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.
35. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).
36. О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.
37. Василева, Р., Русева, В., Корупцията в сферата на държавната администрация, Сборник научни трудове от научна конференция с международно участие „MATTEX 2018“, ШУ "Епископ Константин Преславски", 25-27 октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
38. Василева, Р., Русева, В., „Корупцията - обществен феномен в България“, Сборник научни трудове от научна конференция с международно участие „MATTEX 2018“, ШУ "Епископ Константин Преславски", 25-27октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
39. Василева, Р., Анализ на органите и структурата на местното самоуправление", Годишната университетска научна конференция, 14-15 юни 2018 г., гр. Велико Търново, ISSN:1314-1937 (print), 2367-7481 (online).

40. Dimitrova, N., 2014: The motivation for effective study of technical and technological information assimilation. International Scientific Online Journal – ISSN 2367-5721 Issue 4, December 2014, www.sociobrains.com, pp 94-99.
41. Dimitrova, N., 2015: Operationalize the aims of technological education International Scientific Online Journal. Issue 16, December 2015, www.sociobrains.com pp. 48 – 53.
42. Dimitrova, N., 2014: Role of informatization in technological education and information culture of students International Scientific Online Journal, Issue 2, October 2014, www.sociobrains.com pp. 26-30.
43. Димитрова, Н. Приносът на технологичното обучение за съхраняване на българските национални традиции. – Годишник на Шуменския университет „Епископ Константин Преславски", Т. XX D, Научни трудове от конференция „Иновации в образованието", 30 септември – 02 октомври 2016, Педагогически факултет, Шумен, Епископ Константин Преславски, 2016, 686 – 690.

Author's name: assoc. prof. eng. Hristo A. Hristov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems"
E-mail: hristov63@abv.bg

ISLAMIC ASSOCIATIONS, ORGANIZATIONS AND MOVEMENTS DEVELOPING OR USED TO DEVELOP ACTIVITY IN THE REPUBLIC OF BULGARIA

Hristo A. Hristov

ABSTRACT: *Attempts and processes have been observed to disseminate radical Islamic ideas among the Muslim population under the cover of missionary activities of various Muslim organizations. In connection with the above, it is necessary to study the activity of the existing Islamic associations, organizations and movements on the territory of the Republic of Bulgaria.*

KEYWORDS: *Islamic associations, radicalism, extremism, enmity, intolerance, re-Islamization, the Muslim community, minorities, risky groups, national affiliation and national identity*

1. Introduction

Considering the essence of modern religious cults the following fact shouldn't be ignored that striving for developing active religious and missionary activity they often infringe the text of the constitution of Republic of Bulgaria which abidance guarantees national security, rights and freedoms of citizens and their life. The basic law in the Republic of Bulgaria doesn't set the concrete religious organizations as anti-constitutional. The constitution doesn't have such a task but it strictly defines the signs that categorize the particular religious community as anti-constitutional determining the necessity of their understanding which corresponds to national security of Republic of Bulgaria [1], [18], [19], [20], [21], [22].

2. Islamic associations

The most active international Islamic associations, fundamentalist organizations and movements developing (or used to develop) activities in our country are [2], [3], [4], [5], [6], [7], [8], [9], [10]:

- *Association „Union for Islamic development and culture''* – legal entity, non-governmental organization

The organization „Union for Islamic development and culture'' is registered on 14th of October, 2004 with verdict № 1078 of Regional court – Smolyan, Register 55, Account type 8, Volume 278, Page 28 with address Smolyan city, boulevard „Bulgaria''№ 66. The participants in association's management are Arif Kemil Abdulah, Ismet Iseinov Rashidov, Mehmed Ahmedov Aptovski, Mehmed Ahmedov Gluhov, Milen Ruzhenov

Zhurnalov, Mustafa Fehmi Mehmed, Nihat Nuriev Ademov, Selvi Shabanov Shakirov, Fatime Ali Hajraddin Rashidova, Hamdi Hilmiev Mollov [1]. Most establishers are at age between 23 and 30. The goal of the formation was presented as strive for increasing religious literacy of Islamic followers in the country. Besides the establishers outline the charitable work which associations will develop [2].

According to the statute of the association the management bodies are General Assembly, Chairman, deputy Chairperson, Management board and operational bureau. Each Muslim who has attained the age of 18 can apply for membership in the union and be admitted if he has recommendations from at least three members of the association and written consent of management board for his membership [3].

The chairman of the association is Arif Abdulah who studied 10 years in Jordan and he is a master of Qur'an's interpretation, his deputy is Selvi Shekirov and a secretary – Ismet Rashidov – both bachelors in Qur'an's basis in private university in Zarka city, Jordan [4].

The organization has a site where the cognizance of the union for Islamic development is a crescent which two ends are connected through stars and the formed circle is the terrestrial globe. The suggestion is more than clear. The goals that are set by the Union for Islamic development are related to „Building real Islamic personality among Muslims'', „Making religion compulsory in school'', „Saving identity of Muslims'' etc. The inscription in site is interesting „There is no god except Allah and Muhammad is the messenger of God" [5].

More scandalous are theses of Arif Abdullah that the Muslims are oppressed and the Muslim ethnos is assimilated. Claiming that the Muslims in Bulgaria are oppressed is far from true because the movement for rights and freedoms has two mandates in country management and the assertion that there is Islamic ethnos that is assimilated is pure fundamentalism because religious identity has nothing in common with nationality [6].

The daughter of regional ex-Mufti of Sofia Fatime Ali Hayraddin is in board of directors of popular non-governmental organization Association „Union for Islamic development and culture'' which headquarters is in Smolyan city and she causes a scandal with her requests for Muslim women to wear kerchiefs on public places like schools and state institutions. According to company register DAXY the union is registered in October, 2004 in Smolyan and youngsters born between 1974 and 1983 takes part in its management. Hayreddin provides financing of Islamic organization through her close relationship with Syrian building contractor Mohamed Jeniyat [7].

In 2007 a scandal broke out in Smolyan. The organization ,,Union for Islamic development and culture'' submitted a complaint in the Commission for protection against discrimination against the director of the Vocational School of economics in town because the director discriminated two students as she didn't permit wearing kerchiefs in school. A little later there was a scandal with football club ,,Rudozem 2005'' because there was a Muslim crescent on players' T-shirts. It turned out that the sponsor of the team was the same Union for Islamic development [8].

In number 19/13.03.2009 of Bulgarian official gazette there was an announced invitation to creditors of association ,,Union for Islamic development and culture'' from Arif Kemil Abdulah – a liquidator of association in connection with announcement of dissolution of association through liquidation in civil case № 155/2007. On the basis of Article 267 of Commercial Law Arif Kemil Abdulah invited creditors of the association to submit their claims [9].

- *Association ,,Union of Muslims in Bulgaria''*

The association is registered in 27th of June, 2006 with verdict № 1 of Sofia city court, Register 55, Account type 13243, Volume 22, Page 135 and the registration address is Sofia city, residential complex ,,Oborishte'', street ,,Struma'' № 2, floor 2, ap.3. The members of board of directors are Ali Hjusein Hayraddin, Aniola Kirilova Dimova, Kamen Dimitrov Genadiev, Mjumjun Ismail, Mohamed Usajd Jenijat, Salih Ramadan Arshinski and Fatme Alieva Ahmedova. The union is registered as operating in publishing, translation and consultancy work related to activities and goals [10]. Arab dollars are behind the funding of the ,,Union of Muslims in Bulgaria'' created in Velingrad [11], [49], [50], [51], [52].

The union is established completely incognito by media and social activists in native town of present main Mufti Mustafa Alish Hadji. 50 people were on its establishment; 55 people were invited [12]. To apply for membership in the Union of Muslims it is required to get recommendations from three members of the organization [13].

The headquarters of the Union of Muslims in Bulgaria is Velingrad. The organization sets a goal ,,to revitalize Islamic and return Pomaks to their faith''. The chairman of this union is regional ex-Mufti of Sofia Ali Hairaddin. Here as it's expected there is an Arab relation. One of the establishers is Syrian Mohamed Jeniyat – manager of the company ,,Aladin – building''. There is one more interesting relation as regards this new-coming union of Muslims in Bulgaria. The daughter of chairman Ali Hajraddin – Fatme is in Board of directors of organization for Islamic development. Her actions have been already pointed out in regard to scandals with kerchiefs

and equipments of football team „Rudozem'' with crescent on players' T-shirt [14], [46], [47], [48].

Ali Hayradin is ex-Mufti of Sofia, a mouth-piece of Arab Islamic in Bulgaria as for this aim he actively assist to send students in Saudi Arabia where this movement is manifested. His reel on Arab Islam that is different from preached Turkish Islam in Bulgaria is probably the reason for his suspension of Mufti position year ago. The official version is changes in Mufti structure. Since years Hajredin has had ambitions to enter politics and become spiritual leader of Pomaks. The last year he undertook with islamification of Bulgarian gypsies. The territory he had chosen for this is Samokov, Ihtiman, Montana, Dolni and Gorni Tsibar. All this stresses the Muslims in Bulgaria. They claim that schism occurred among them because of the different interpretation of Qur'an. Even the rituals are different those who had teached and returned from Saudi Arabia had conflict with their families. Arab emissaries paid Muslim women 200 levs to wear kerchiefs [11], [12], [13], [14], [15], [16], [17], [18], [41], [42], [43], [44], [45].

- *Association with public useful activity „Federation Justice – Bulgaria''* – registered on 15th of May, 2007 by Sofia city court with verdict № 1 recorded in Register 55, Account type 13931, Volume 295, Page 45 in company case 7323/ 2007.

The headquarters of the association is with address Sofia city, residential complex „Krasno selo'', boulevard „Hristo Botev''№ 21, floor 2, ap.4. When it was established in the program of association the following is written: „Development and strengthening of the Muslim community, recognition of Turkish minority in Bulgaria and making Bulgaria two-national country; Turkish should be announced as second official language in the country''. Association „Federation Justice – Bulgaria'' is operating through organization of press-conferences, seminars, symposiums, discussions and other similar initiatives while they are in conformity with goals of the association; publishing work; helping education and qualification of association's members, each other legitimate activity that fits with association's aims [16], [19], [20], [21], [35], [36], [37], [49], [50], [51], [52].

- *Unregistered association „National Turkish association''*

In 2006 50 representatives of Turkish ethnos in Bulgaria created National Turkish association on peak Buzludja. The businessman from Kazanlak – Menderes Kungjun was chosen for leader of the formation. National Turkish association accepted its own symbols. The flag was black horse on green background and inscription was National Turkish Association Bulgaria. The formation had a motto „Rights are not given, you should fight for them'' [17]. The non-governmental organization is supposed to manage

by 5-membered board of directors as two of its members are foreign citizens. Five representatives of Turkish human rights non-governmental organization „Bahat'' attended the establishment of new formation. The national Turkish association adopted 10 aims and tasks that it would work for. They are development and affirmation of citizen society among Turkish Muslim community in Bulgaria as well as support of social integration of Turkish population in Bulgaria. Protection of individual human rights and Turkish minority in Bulgaria as well as development of political pluralism are other purposes of new formation [18].

Other basic goals of association are: development and affirmation of citizen society among Turkish-Muslim community; protection of individual human rights and those ones of Turkish community; counteraction through peaceful means against aggressive actions of ethno-national formations and national chauvinistic and racist propaganda against Turkish Muslim community as well as development of political pluralism in order to democratize and unbundle Turkish community [19].

Under declaration of establishers of National Turkish association announced in media the headquarters of association will be in Plovdiv and branches of organization will be created in Kardjali, Razgrad, Targovishte, Shumen and Kazanlak [20]. The General Assembly and Board of directors are management bodies with chairman Menderes Kungjun [21].

The registration form is received in court on 12th of July, 2006 in Regional court-Plovdiv that denies registration because under Article 12(2) of Bulgarian constitution associations of citizens must not set political purposes. According to motives in verdict for registration denial of „National Turkish association'' a part of declared and adopted goals of association by Constituent Assembly has a political direction. It concerns „development of political pluralism in order to democratize and unbundle Turkish community''. Such goals correspond to registration under Law of political parties and the competent court is another one which is supposed to judge the conformity of the statute and set goals as regards Constitution of Bulgaria [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [35], [36], [37].

Islamic organizations: - Organization „Islamic protection'' is created in 1996 in region of Jakoruda. It is illegal. Throughout press announcement it announces the basic part of its statute: creating Muslim autonomous district in West Rhodopes, own radio and television, local police and Islamic schools, violent actions to overthrow the government and court for those who repress Muslims. It is supposed that its establisher is Syrian citizen who lives on the territory of Republic of Bulgaria [23], [32], [33], [34], [35].

ISLAMIC MOVEMENTS: - Movement of Sufis – seclusion mystic movement that rejects all secular. By way of Turkey Sufis try to penetrate

into Bulgaria. Its missionaries preach in Sheriff Khalil Pasha Mosque in Shumen [24], [35], [36], [37], [49], [50], [51], [52].

In region of West Rhodopes the Sufis play educational role as they strive to attract new adherents and followers of Islamic religion through organizing of free educational courses, offering study grants and full financing of education in Saudi Arabia and Jordan and free spreading of holy book of Quran among Muslim population. The pragmatically adopted approach is used ,,Read Quran and diffuse ideas among rests''[1], [2], [3], [4], [5], [6], [7], [9], [10], [15], [17], [22], [38], [39], [40].

3. Conclusion

In conclusion it must be said that the activity of Islamic fundamentalist organizations is directed to:

- Activizing the activity on the territory of Republic of Bulgaria. Islamic leaders know that older Muslims in our country are bearer of so-called popular Islam which forms and doctrines are different from fundamentalists to some extent. On the other hand they ascertain that young Muslims in Bulgaria don't know the canons of Quran and fundamentalists make efforts to cover exactly them as they preach their ideology.

Their emissaries attend regions with Muslim population and make lists of youths who study Islam and then send them to train for spiritual employees in Sudan, Egypt and other Arab countries. Courses are organized as the situation is examined in advance and suitable places are chosen in mountain and recreational places where there is strong control and no external visitors are allowed. Teachers require the student to observe the basic rules including the compulsory five preaches per day. They act unfeignedly as they rely that the authorities in Bulgaria are engaged with the problem with nowadays Christian and east religious sects and their activity stays unnoticed and uncontrolled by the country.

- Union of all Muslims in Bulgaria on the basis of Islam as common religion. Islamic fundamentalist organizations that have great finances give money to restore old mosques and build new ones.

The aim is to function Muslim rite temples in all big Bulgarian cities and towns on obvious place; financial support to train new cadres for religious and secular schools. In Egypt, Saudi Arabia, Syria, Iran and Turkey our citizens are trained to teach in universities and high schools that function in Bulgaria.

The preparation of secular teachers is under separate conditions. Youths from these circles that have shown good results in high schools in our country are sent to study radio-television journalism i.e. preparation of professional cadres who can influence directly on social consciousness

mainly of Muslims. Islamic fundamentalist organizations strive to create their own cultures in Bulgaria.

REFERENCES:

1. Information legal product „CIELA INFO''
2. V., Joncheva, 07.08.2008г., Illegal sects act under cover of fondations, Muslim organizations in Bulgaria preach radical Islam, Retrieved from: Novinar, http://novinar.bg/
3. Will Rodopi become tight for Bulgarians ?, 14.10.2006г., Retrieved from: newspaper „Now'', http://www.segabg.com/article.php?id=292299
4. News.Plovdiv24.bg„ 14.10.2006г., http://news.plovdiv24.bg/19845.html
5. http://www.segabg.com/article.php?id=292299
6. http://pomaks.blogspot.bg/2007_03_01_archive.html
7. The cost of faith or how much the sects were paying! The Rhodopes cost the pastor's fuel, school heads or half-moon t-shirts?, http://rodopi24.blogspot.com/2015/04/blog-post_145.html.
8. http://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=16926 (Offical gazette, number 19, 13.03.2009).
9. http://www.bgns.net/site/smf/index.php/topic,2195.0.html.
10. Pomaks, http://pomaks.blogspot.bg/ 2007_03_01_archive.html.
11. http://pomaks.blogspot.bg/2007_03_01_archive.html.
12. Iren, Delcheva, Ali recruited Amazons with charm for Islam, newspaper „Standard'', number 5073.
13. /http://www.bghelp.co.uk/forums/printthread.php?&t=9383.
14. http://forum.vestnikataka.bg/index.php?topic=1612.0.
15. http://www.omda.bg/public/bulg/news/Bulgaria/Kungyun.htm.
16. http://www.omda.bg/public/bulg/news/dps/Turska%20namesa%20v%20Bg%202.htm
17. Agency Focus, Association „National Turkish association'' of Menderes Kungjun, http://www.ndt1.com/article.php/20061115125427346.
18. Radical Islam in Bulgaria, 17.03.2009, http://news.bg/comments/radikalniyat-islyam-v-balgariya.html.
19. V., Hristov,(2012), The symbiosis of "religion and ultimate nationalism", favorable prerequisite for triggering negative processes in the Western Rhodopesp Scientific almanac of Varna Free University "Chernorizet Hrabar", Book 19, page 198.
20. Andreev A. Any aspects of security what concept. NMU- Shumen, Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.
21. Andreev A. The environment of security and influence national security and national interests. NMU- Shumen. Scientific Conference "Problems of national security", 2009, ISSN 1314-0647).
22. Andreeva G., Andreev A. Survey and analysis of intercultural communication in Bulgaria and abroad. Journal Scientific and applied research, USA, vol.3, p.89-97, 2013.
23. Velikov, I., Humanitarian aspects of protection of information, MATTEX 2018 Conference proceedings, Konstantin Preslavsky University of Shumen, ISSN 1314-3921, Shumen, Vol. 2, part 1, 2018, pp. 3-10.
24. Ivanov, M., Intelligence Infrastructure, Sofia, Profisec, 2012, p. 215, ISBN 978-954-32927-1-8.

25. Ivanov, M., Nazism and Islam, MATTECH 2018, Shumen, St. Konstantin Preslavsky University Publishing House, 2018, ISBN 1314-3921.
26. Ivanov, M., Army and Police - Diffusion of Functions and Tasks, Fourth National Conference with International Participation "Metal Science, Hydro- and Aerodynamics and National Security 2014", Sofia, 2014, ISBN 1313-8308.
27. Савов, И., Рискове и заплахи за сигурността в Черноморския регион, Международна конференция „Проблеми на сигурността в черноморския регион", ВУСИ, септември 2017 г., ISBN 978-619-7343-09-0, с. 7-18.
28. Savov, I. Some aspects of legislative system of the institutes migration and readmission in the European Union, International conference - Law and Security in migration process and the consequences of the migration crises, Nikola Tesla University, Beograd, 2017, ISBN 978-86-6113-046-5, p. 265-277.
29. Савов, И. Структури и организации в Република България свързани с миграцията, Годишник, том XIV, 2017, ВУСИ, ISSN 2367-8798, с. 14-21.
30. Савов, И., Борисов, Т., A look on the nature of agreements for the application of the readmission institute, International conference – European integration, Nikola Tesla University, 2018, Beograd, ISBN 978-86-6113-050-2, p. 45-56.
31. Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Pyce, 2017, c.19-27, http://jei.uni-ruse.bg/Issue-2016/02.%20Zagorcheva%20-%20Pavlov.pdf.
32. Zagorcheva, D., Stages in the systems for financial management and control in the Bulgaria's public sector, The XIV International Scientific Conference Information Technologies and Management, 2016, Riga, Latvia.
33. Загорчева, Д, Велчева, Й., Бюджетната децентрализация като фактор за едновременно развитие на общините и индустриалния бизнес, Народностопански архив, година LXX, книга 3 – 2017, ISSN 0323-9004, стр. p.46-59, https://www.uni-svishtov.bg/NSArhiv/title.asp?title=981.
34. Boyanov, P., Educational exploiting the information resources and invading the security mechanisms of the operating system windows 7 with the exploit Eternalblue and Backdoor Doublepulsar, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 14, 2018, pp. 34-41, available at: http://www.rst-tto.com/publication.html.
35. Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, Vol.3, 2013, pp. 114-124, available at: http://www.rst-tto.com/publication.html.
36. Solakov, T., The Bulgarian state and the religious organizations in the period after 1989, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press", ISSN 1311-834X, Vol. VI E, 2017, pp. 107-119.
37. Solakov, T., Religious fundamentalism and extremism, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press", ISSN 1311-834X, Vol. VI E, 2017, pp. 120-132.
38. Solakov, T., Radicalism and stages of radicalization, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press", ISSN 1311-834X, Vol. VI E, 2017, pp. 133-140.

39. Досев, Н., Създаване на склад от данни за определяне на риска за информационната сигурност на корпорацията, Научна конференция с международно участие на тема „Киберсигурността в информационното общество”, Факултет "А, ПВО и КИС", Шумен 2017 г.
40. Досев, Н., Създаване на модел на система за ранно предвиждане рисковете за информационната сигурност на корпорацията, Научна конференция MATTEX на ШУ „Еп. К. Преславски“, гр. Шумен, 2016 г.
41. Досев, Н., Обезпечаване сигурността на достъпа до интегриран склад от данни, Международна научна конференция 2016, Факултет „А, ПВО и КИС“ гр. Шумен, 2016.
42. Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.
43. Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.
44. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).
45. О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.
46. Василева, Р., Русева, В., Корупцията в сферата на държавната администрация, Сборник научни трудове от научна конференция с международно участие „MATTEX 2018“, ШУ "Епископ Константин Преславски", 25-27 октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
47. Василева, Р., Русева, В., „Корупцията - обществен феномен в България“, Сборник научни трудове от научна конференция с международно участие „MATTEX 2018“, ШУ "Епископ Константин Преславски", 25-27октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
48. Василева, Р., Анализ на органите и структурата на местното самоуправление", Годишната университетска научна конференция, 14-15 юни 2018 г., гр. Велико Търново, ISSN:1314-1937 (print), 2367-7481 (online).
49. Dimitrova, N., 2014: The motivation for effective study of technical and technological information assimilation. International Scientific Online Journal – ISSN 2367-5721 Issue 4, December 2014, www.sociobrains.com, pp 94-99.
50. Dimitrova, N., 2015: Operationalize the aims of technological education International Scientific Online Journal. Issue 16, December 2015, www.sociobrains.com pp. 48 – 53.
51. Dimitrova, N., 2014: Role of informatization in technological education and information culture of students International Scientific Online Journal, Issue 2, October 2014, www.sociobrains.com pp. 26-30.
52. Димитрова, Н. Приносът на технологичното обучение за съхраняване на българските национални традиции. – Годишник на Шуменския университет „Епископ Константин Преславски”, Т. XX D, Научни трудове от конференция „Иновации в образованието”, 30 септември – 02 октомври 2016, Педагогически факултет, Шумен, Епископ Константин Преславски, 2016, 686 – 690.

Author's name: assoc. prof. eng. Hristo A. Hristov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems"
E-mail: hristov63@abv.bg

FEATURES IN THE ACTIVITY OF THE GENERAL DIRECTORATE "BORDER POLICE" – MINISTRY OF INTERIOR IN THE APPLICATION OF THE INSTITUTE READMISSION

Ilin Savov
Milko Berner

ABSTRACT: *The article give a view about the specifics and the role of the Border Police Directorate General at the Ministry of Interior of the Republic of Bulgaria in connection with the control of the migration processes. The activity of the individual structures in the Republic of Bulgaria participating in the implementation of the readmission institute is analyzed. The goals set in the interaction between the different organizations related to the migration processes in the country are assessed.*

KEYWORDS: *Migration, Ministry of Interior, General Directorate "Border Police", National security, Readmission*

Introduction

Readmission is an important tool for managing migration flows. It facilitates the return of persons residing unregulated in a country to the country of origin or transit and represents arrangements between the competent authorities, laying down the procedures to be followed. The review of Bulgarian and European legislation shows that, as regards Bulgarian citizens, the obligation of the Republic of Bulgaria to accept them through the readmission institute stems from Art. 35, para. 2 of the Constitution of the Republic of Bulgaria stating that "Every Bulgarian citizen has the right to return to the country". The process of moving citizens on their way to their home country should not be a problem due to the fact that each country has commitments to protect its citizens. The readmission agreements concluded in principle contain a clause according to which the requested party is committed to accepting its citizens, which in turn involves the transmission of travel documents without delay to the consular representative of the requested country.

Role of the General Directorate "Border Police" - Ministry of Interior in the control of migration processes

The Directorate-General "Border Police" - Ministry of Interior has set up the Border Control Directorate, which is the division "Border Surveillance" (BS). The established structural unit "Re-admission" to the

General Directorate - DGBP at the Ministry of Interior has created its name several times since its establishment. We will briefly follow the evolution of the readmission sector. In 1997, a Police Force Management and Planning Division was set up for the Police Force Protection Division, which carried out methodological guidance, planning and control of the police forces in the crossing of the state border guard from professional staff.

In May 2003, the RFMPD changed its name to "Acceptance and Transmission of Persons and Administrative Activity" and its obligation dropped some of the activities carried out, but new tasks were added. The sector is established in the newly established "Guard of the State Border" and begins to implement the organization, methodical management and control in the administrative service of both foreigners and Bulgarian citizens. With the entry into force of the new Law on the Ministry of the Interior, a number of structural changes were implemented on 1 May 2006, one of which is the renaming of a sector in the Re-admission sector, which in turn is responsible for the following main activities:

- Expert, control, methodological and coordinating activities concerning the enforcement of compulsory administrative measures under Aliens in the Republic of Bulgaria Act (Foreign Nationals Act) for foreigners who violate the border regime.

- Expert, control, methodological and coordinating activities concerning the work on imposing compulsory administrative measures under the Bulgarian Personal Documents Act of Bulgarian citizens who violated the legislation of a foreign state - until 2009;

- Preparation of expert opinions on the implementation, amendment and supplementation of the legal framework related to the LRAW, the Law on Labor and Social Security and the Law on Asylum and Refugees.

- Interaction with Migration Directorate, Bulgarian documents Directorate, State Agency for Refugees (SAR) at the Council of Ministers, State Agency for Child Protection (SACP), Agency for Social Assistance (ASA) at the Ministry of Labor and Social Policy.

- Maintain regular contacts with international and non-governmental organizations: the United Nations High Commissioner for Refugees (UNHCR); Bulgarian Helsinki Committee (BHC); The International Organization for Migration (IOM); The Bulgarian Red Cross (BRC) and others.

- Drawing up of draft instructions regulating the technological order for imposing and executing orders for imposing compulsory administrative measures on persons under the Aliens Act in the Republic of Bulgaria.

- Coordinates and controls the activity of reception, escorting, guarding and surrender of persons with forced coercive administrative measures (CAM).

- Prepares and provides the necessary reference and statistical information to the higher management levels.

- Involved with expert representatives in the work of inter-ministerial committees and carrying out internal, official and inspectorate inspections in the RDBF and their structural units.

- Implementation of readmission agreements / readmission agreements concluded between the Republic of Bulgaria and other countries as well as agreements concluded by the European Union.

- Preparation of expert opinions related to the implementation of specific bilateral readmission agreements and opinions on draft bilateral readmission agreements as well as draft protocol on their implementation.

- In connection with the implementation of Reception Agreements, they carry out translations and coordination procedures with the Border Checking and Operational-Investigation (BSS) departments. In this regard, it is important to note that the BCP is key to the functioning of the state's economic and socio-political system. It can be defined as an important part of the system for managing the balance between freedom of movement and the protection of internal security and the preservation of public order. Regarding the implementation of the readmission agreements, there is a regular cooperation with the police representatives at the embassies and with the references in the Consular Relations Directorate at the Ministry of Foreign Affairs[1].

After reviewing and analyzing the normative documents it is clear that as a result of the implementation of the Ordinance on the Responsibility and Coordination of the State Bodies[2], the DGD jointly with SAR - MS perform the following joint activities:

- carry out actions on the transfer of a foreign national from or to the Republic of Bulgaria pursuant to Council Regulation (EC) No 343/2003 of 18 February 2003 and Council Regulation (EC) No 1560/2003 of 18 February 2003;

[1] Rules of Procedure of the Ministry of Foreign Affairs. Prom., SG, no. 80 of 13.09.2013, in force since 13.09.2013 Adopted by Council of Ministers Decree No. 202 of 11.09.2013

[2] Ordinance on the Responsibility and Coordination of State Bodies Pursuing the Implementation of Council Regulation (EC) No 343/2003 of 18 February 2003, adopted by Council of Ministers Decree No. 332 of 28.12.2007, prom. 3 of 11.01.2008, as amended by Decree of the Council of Ministers No 301 / 10.11.2011.

- notify the State Agency for Refugees of a foreigner who has crossed the state border of the Republic of Bulgaria and has declared his wish to obtain a status under the LAR.

In this article, we will follow the process of a declared desire to provide protection by persons who have crossed the border according to the legal normative act in the Republic of Bulgaria. GARD officers detain foreigners crossing the border illegally for a maximum of 24 hours, respecting the rights of detainees subject to the following procedures:

- Identification of persons;

- The officers of GDF and Frontex conduct screening interviews to establish the nationality of individuals;

- Verification in the Automated Information System (AIS). Use of the "Search Activity - NISIS" handling alerts for categories of persons pursuant to Ordinance No 8121h-465 of 26 August 2014 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria.

- Collection, processing, and storing of fingerprints in the AFIS-BD - AFIS data maintenance and processing activities are performed by administrators and operators of the Automated Workplace System (ARM) located in the Territorial Units of DGBP - Ministry of Interior. Operators of the territorial units of the DGMF - MI shall carry out real-time inspections of persons violating the border regime of the Republic of Bulgaria or with imposed compulsory administrative measures, also bring in the AFIS-BD border subsystem fingerprints, photos and personal data of the checked persons. The persons representing AFIS information sites are described in detail in Order No. 8121h - 583 / 08.06.2016 of the Minister of the Interior on the Organizational and technological rules of AFIS automated dactyloscopic identification system.

- Registration in the EURODAC automated dactyloscopic identification system in category II under Regulation 603/2013 (detained for illegal crossing of an EU external border). According to Art. 6, para. 1 of Ordinance No I - 1911 / 20.11.2011 of the Minister of Interior on the organizational and technological rules of the automated dactyloscopic identification system "EURODAC" have the right to use the system:

1. the structures of the General Directorate "Border Police" - Ministry of Interior;

2. Directorate "Migration" - Ministry of Interior;

3. State Agency for Refugees at the Council of Ministers - ARM for the taking and transfer of dactyloscopic prints of the persons under Art. 2 to the national AFIS.

An application for protection in the Republic of Bulgaria is filled in with the help of an interpreter. The application shall be filed with a business card number and shall be sent in due time by e-mail, fax or by letter to the State Agency for Refugees. The procedures for obtaining protection in the Republic of Bulgaria are explained both through printed and informative materials in different languages provided by UNHCR, SAR - MS and the Bulgarian Helsinki Committee, as well as by the translator who supports the filling of the application. All persons who have filed applications for protection before the GDBP authorities shall be transmitted by means of a pass-through protocol to the employees of SAR. The original of the application for protection as well as any personal documents owned by the person concerned shall be attached to the passport. If a disease is detected in the first medical examination, a medical note shall be attached to the set of documents, reflecting the outcome of the review.

For foreigners detained in an attempt to illegally cross the state border of the Republic of Bulgaria or in the border zone, in order to prevent violations of the border regime, prevention and elimination of the harmful consequences thereof, administrative enforcement measures under the Aliens Act in the Republic of Bulgaria.

The persons shall be imposed CAM by the order of art. 41 "Return to the country of origin, country of transit or third country" and Art. 42h "Prohibition of entry into the Republic of Bulgaria" by the Foreign Nationals Act, until the removal of the obstacles to the implementation of the imposed measures (identity uncertainty, danger to absconding and prevention of return, creation of a return organization) the foreigners are transferred to Special Homes for temporary accommodation of Foreigners to the "Migration" Directorate-Ministry of Interior.

Of the data released by the GDBP in 2013, 3019 third-country nationals were detained in an attempt to unlawfully detained, more than 10 times compared to 2012 when 281 persons were detained. The most people detained at exit are nationals of Afghanistan - 843, Syria - 699, Algeria - 428, Morocco - 99 and Mali - 86.

It is characteristic that most of them were in the process of granting protection in Bulgaria, which is a violation of Art. 30 (6) and (7) of the Law on Asylum and Refugees (not to enter the border area of the Republic of Bulgaria without due authorization, not to leave the territory of the Republic of Bulgaria without the permission of the State Agency for Refugees).

During the period 01.01 - 31.05.2014, 840 attempted illegal crossings of third-country nationals were detected while in the period 01.01 - 31.05.2013 there were only 409. Of these 647 were found at external borders (264 for first five months of 2013). At the internal borders, 193 persons were

established (145 for the period 01.01 - 31.05.2013). Most are third-country nationals attempting to disrupt the Afghanistan border - 335, Syria - 274, Iraq - 31, Pakistan - 25, Mali - 23 and others.

At the exit of the state border of the Republic of Bulgaria for the period 01.01-31.10.2018 a total of 486 third-country nationals were detained 152 with AFIS, of whom 12 were minors.

From the beginning of 2018 to 31 October 2018, 266 third-country nationals were removed under the Readmission Agreements concluded at both bilateral and European level in the Republic of Bulgaria.

It is important to note that in 2010 a "Tripartite Memorandum of Understanding on the ways of co-operation and coordination in facilitating the access of persons seeking protection to the territory of the Republic of Bulgaria and the protection procedure in the country" was concluded between DG Border Police - Ministry of Interior, UNHCR Representation in the Republic of Bulgaria (UNHCR) and the Bulgarian Helsinki Committee (BHC), which plays its role in building the main mechanisms for coordination and cooperation in the implementation of the monitoring of the Bulgarian borders. Under the Memorandum, the parties to it form a Tripartite Task Force (TRG), which monitors its implementation, and meets during the year on current issues.

Representatives of other relevant institutions active in the field of migration and asylum may attend meetings of the tripartite group.

According to this Memorandum, reports are issued on a yearly basis which regulates the procedure for border surveillance on access to refugee territory.

In this article we will highlight some of the important goals of the memorandum, namely:

- monitoring to ensure the access of persons seeking international protection in the Republic of Bulgaria and observance of the principle of the protection of persons against forced refoulement from the border;

- Training of Border Police officers with the participation of SAR - MS and other non-governmental organizations - BRC and BHC, paying special attention to the issues of respecting human rights and police ethics in working with vulnerable groups - unaccompanied children, minors and persons with special needs;

- Provision by the Bulgarian Helsinki Committee (BHC) of translation and representation with a view to creating additional guarantees for the access of persons to specialized legal assistance;

- annually, a report on the border surveillance of the Republic of Bulgaria with regard to access to the territory and the protection procedure shall be prepared.

In 2014, the State Agency for Refugees to the Council of Ministers officially reported that it received 7851 inquiries from other EU Member States under the Dublin Regulation, of which only 174 back transfers of pending asylum seekers were actually made. However, the majority of the inquiries concerned requests for the status of concerned persons with protection granted in Bulgaria in the form of refugee or humanitarian status, for which a readmission procedure might be applicable. In 2015. 122 readmissions from a total of 1,000 return requests were made to the country. The top three countries returning readmission during the year were Serbia with 58 re-admitted to Bulgaria, Germany with 24 persons and Austria with 11 persons returned to the readmission agreements.

From the review of the Bulgarian and international legislation regarding the joint activities of the Republic of Bulgaria and international structures in connection with the solution of the threats and dangers of the increased migratory flow, it can be concluded that:

- the cooperation between the responsible Bulgarian authorities and the international organizations can be defined as one of the important national achievements regarding the rules on the right of access to the territory of the Republic of Bulgaria;

- synergies and coordination are essential for a fruitful partnership in joint actions to contribute to the effective implementation of the obligations of national authorities in the field of international protection;

- in view of the contemporary challenges to the national security of the Republic of Bulgaria in the activities of the border and migration authorities, there is a need for cooperation of NGOs on meeting the needs of vulnerable categories of persons under their jurisdiction and responsibility;

- the need to refine and extend the law relating to the principle of impunity for persons who declare that they are seeking international protection, and not only for the category of persons referred to in Art. 279, para. 5 of the Criminal Code of the Republic of Bulgaria, which states the following: "It is not punished the person who entered the country to enjoy the right to asylum in accordance with the Constitution";

- in carrying out its border guard and border control activities through the relevant state authorities, the Republic of Bulgaria should provide guarantees for full respect for fundamental human rights, including the possibility of protection from return and the right to apply for protection, despite the necessity of the intensified measures for prevention of access to the territory of the Republic of Bulgaria.

Conclusion

The need to tackle migration to the European Union predetermines a new approach. Member States must make use of the mechanisms at their disposal, making it necessary to combine internal and external policies in the best possible way. The right decisions can be made after close cooperation between countries, all EU institutions, international organizations, local authorities and countries outside the Union.

Nowadays, along with the implementation by states of well-known and long-standing procedures for the forced return of illegal migrants (expulsion, deportation, etc.), more and more countries are resorting to the use of the readmission institute, which has its advantages and distinctive features.

REFERENCES:

1. Ministry of the Interior Act.
2. Aliens Act in the Republic of Bulgaria
3. Penal Code of the Republic of Bulgaria
4. Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)
5. Annual Report on Border Surveillance in 2015 - Access to Territory and International Protection - Sofia, issued on 30.06.2016 by the Bulgarian Helsinki Committee, the Border Police General Directorate and the UNHCR Representation in the Republic of Bulgaria.
6. Annual Report on Border Surveillance in 2014 - Access to Territory and International Protection - Sofia, issued on 25.05.2015 by the Bulgarian Helsinki Committee, the Border Police Directorate General and the UNHCR Representation in the Republic of Bulgaria.
7. Rules of Procedure of the Ministry of Foreign Affairs. Prom., SG, no. 80 of 13.09.2013, in force since 13.09.2013 Adopted by Decree of the Council of Ministers No 202 of 11.09.2013.
8. Ordinance on the Responsibility and Coordination of State Bodies Pursuant to the Implementation of Council Regulation (EC) No 343/2003 of 18 February 2003, adopted by Council of Ministers Decree No. 332 of 28.12.2007, promulgated in State Gazette . 3 of 11.01.2008, as amended by Decree of the Council of Ministers No 301 / 10.11.2011.
9. Savov, I Reaction and Migration Processes of Foreigners in the Republic of Bulgaria, HSSE, 2017, ISBN 978-619-7343-05-2.

Author's name: prof. Ilin Savov, PhD
Workplace: Higher School of Security and Economics, Dean of Department „National security and public order"
E-mail: ilin_savov@abv.bg

Author's name: Milko Berner, PhD
Workplace: Deputy Minister at Ministry of Interior of Republic of Bulgaria
E-mail: alphachem@abv.bg

NON-LETHAL WEAPONS – AN OVERVIEW OF CURRENT TECHNOLOGIES

Milko Berner

ABSTRACT: *The Non-Lethal Weapons (NLWs) and associated technologies will have growing impact on the future war tactics, peace keeping operations, riot control, civil policing and entire law enforcement domain. The paper presents a brief review of the most promising, as per the author's opinion, NLWs. Different technologies is classified and principles of their action are described. Specific attention is given to applicability of different representatives of NLWs, their effectiveness, potential for future development and challenges towards their practical implementation. The main risks related to the use of considered weapon systems are also discussed. At the end some moral aspects of NLWs use are analysed.*

KEYWORDS*: Non-lethal weapons, Law-enforcement, Riot Control, Military, Security, Chemical Weapon Convention, Biological Weapon Convention.*

1. Introduction

In recent years, the employment of non-lethal weapons has proven increasingly effective in dealing with adversaries in different law enforcement and military scenarios. In these cases, the goal of law enforcement and military personnel is to employ an adequate level of force necessary to only control the situation during the confrontations. Avoidance of collateral damage is increasingly critical for humanitarian and public policy reasons. Normally the possibility of permanent injury or unintentional death increases as response level increases. In the same time, as the level of force applied increases, adversaries will often escalate their response thereby increasing the risk of injury to the law enforcement or military personnel. When NLW are involved in the course of military conflicts, besides incapacitation of adversary's personnel, their use may possibly target disabling of large quantity of enemy's hardware (equipment, vehicles, etc.), permanently or for prolonged period. In such scenarios, NLWs obtain some of the characteristics of strategic weapon. Many NLW do possess the potential for lethal effects against humans. Because of this, NLW are sometimes called less-than-lethal weapons.

2. Non-lethal weapons – main characteristics and types

In general NLW are devices, chemical or biological agents and combinations of them, whose effect on adversaries could be based on different principles. (Table 1)

In order to be considered as NLW, they should, as minimum, meet the following requirements:

- Level of effectiveness which guarantied fulfillment of assigned tasks.
- They should be consistent with established policies including laws, treaties, arms control agreements, or other legal obligations the government is committed to observe.
- They should be technologically and operationally feasible.
- They should have an acceptably low probability of being fatal or inflicting permanent disablement on personnel, and causing undesired damage to property and the environment.
- They should not be capable of being easily defeated by enemy countermeasures once their operational principles are known.

Table 1.

Action principle	NLW representatives
Utilisation of kinetic energy (Including acoustic energy)	- Low energy projectiles - Water cannons - Toroidal vortex emitters - Infrasound
Utilisation of electromagnetic radiation	- Blinding laser weapons - Noble gas radiators - Sound-flash munitions - Microwave projectors
Utilisation of electric energy	- Electric stunners - Conductive chaff cloud
Utilisation of chemical agents with different actione	- Lacrimators - Sternites - Malodorants - Super acids or super bases - Polymer degradation agents - Metal embrittlers - Filter-slugging agents - Fuel inhibition agents - Traction modification agents
Dazzling or obscuring effect	- Obscuring smokes - Obscuring coatings
Impact on the Central Nervous System	- Tranquilizing agents - Calmative agents - Strobing incapacitating Torches
Physical immobilisation	- Restraining nets - Adhesive foams
Utilisation of biological agents	- Bio-corrosive agents - Biological fuel-eaters

Below the currently existing and some of the most promising representatives of NLW are described and discussed.

Low energy projectiles include bullets, pellets, or ring airfoils that will not penetrate the skin but will deliver significant kinetic energy and momentum to the target. The projectiles will produce significant pain similar to a punch with a fist or a knuckle. The intent is to produce a noticeable and highly unpleasant, yet minimally damaging impact. Larger projectiles may be used to knock an individual off balance. Projectiles may be made of rubber, wet sponges, and bags with compressed chalk or polymer powder. They may be fired from rifles, shotguns, or grenades launchers. Obviously, the projectiles can cause serious injuries if they hit sensitive parts of the body.

Individuals reacting to the impacts may subject themselves to indirect injuries from falls.

It is easy to predict that inattentive use of low energy projectiles may cause fatalities or chronic injuries.

Water cannons use high-pressure water streams to knock out targeted individuals. The simplest implementation is fire hoses, although specialized pump and nozzle systems (nozzles which generates pulsating jets) can be used with greater accuracy at longer distances. Obviously if the water jet is powerful enough it may be capable of producing injuries and cause fatalities.

Toroidal vortex emitters are devices that create and direct toroidal vortex rings against distant targets. These rings are volumes of air that rotate about the azimuthal axis of the ring (in essence it is donut-shape volume of air). The azimuthal axis is oriented perpendicular to the ring's direction of motion.

Molecules of air are trapped within the vortex and propagate with it. Vortex rings can maintain their shape and character for many seconds to minutes after formation and can propagate distances of hundreds of meters. To certain extend they behave as solutions in the air. The primary function of a vortex projector is to deliver a pulse of energy and momentum to the target. A vortex ring can knock out an individual. Vortex rings can also be used as vectors to carry chemicals or small particles with them. Thus a vortex ring projector might be used to deliver a portion of riot control agent, calmative agent, or malodorant to a specific target from long distance.

Infrasound projectors are devices that create sound with frequencies below the range of human hearing (< 20 Hz) and direct it against desired targets. Infrasound resonates with the internal organs of the body to produce rapid discomfort, nausea, and loss of bladder control. Complete recovery takes seconds to minutes. At high enough intensity levels, it may resonate with other structures, causing them to undergo amplified vibration followed by damages or structural failure in severe cases. A large infrasound projector

could induce the equivalent of an earthquake in a structure causing walls to fail and the building to collapse. Contemporary infrasound generators consist of small open-ended combustion chambers that are alternately filled with fuel-air mix and ignited at rates of a few Hz. Specifically shaped tubes serve to direct and focus the sound waves at a target.

Blinding laser weapons are designed to temporarily blind humans and electro-optic systems and sensors. Temporary blinding of humans can be accomplished by flash blinding or veiling glare. Flash binding is an effect in which the visual receptors are saturated. An afterimage results whose intensity decays slowly with time. As long as the afterimage brightness exceeds ambient light levels, the exposed individual cannot distinguish objects in his environment. Flash blindness can last from second to many minutes, depending on ambient light levels. The laser light scattered in the eye produces a strong illumination over much of the retina. When this scattered illumination exceeds ambient illumination levels, the real images are veiled by the scattered light.

The effects of veiling glare disappear as soon as the laser beam illumination is removed. It is obvious that effect on human eye depends on intensity of laser radiation and the distance from the source. It is difficult to tune these two parameters properly on a field, such way to guarantee complete avoidance of permanent injuries. Hence operations with use of laser weapons should be planned in details and well in advance, considering restrictive factors.

Dazzling lasers could be vehicle mounted or handheld. One prototype which is currently under testing is so called personnel halting and stimulation response rifle or PHASR. (fig. 1) They are also pocket size laser torches with multitude collimated laser diodes forming spot wide enough to allow easy targeting.

Fig.1. PHASR

Sound-flash munitions are pyrotechnic devices (usually hand grenades) that produce intense sound (220 dB at 1 meter distance) and blindingly intense light. The combined sound and light saturate the human sensory system. Any individual within a few meters of a flash-bang explosion is stunned for periods up to six to eight seconds. As a rule the device is designed not to propel any fragments. There is some possibility of hearing and/or vision damage if the device explodes too close to an individual's head.

Sound-flash munitions have to be used by skilled personnel and with care because they are potent to cause fatalities and/or chronic injuries.

Noble gas radiators are similar to sound-flash grenades/munitions with the difference that the pyrotechnical charge is surrounded by pressurized noble gas jacket (argon or xenon).

When the charge is detonated in the confined atmosphere of a monatomic gas, the propagation of the resultant shock wave through the gas causes additional compression of the gas and adiabatic heating. This heats the gas to tens of thousands degrees Kelvin at the front of propagating shock wave and causes it to generate an intense emission (flash) of light containing virtually all wavelengths, and effectively blinding unprotected individuals and/or different types electro-optic devices. The device produces light at intensity several orders of magnitude greater than that of a conventional flare. The device produces a short pulse of electromagnetic energy having duration of the order of tens of microseconds, in a broad band of wavelengths from ultraviolet to infrared.

Noble gas radiators may be in the form of hand grenades, munitions for grenade launchers or artillery shells. A single artillery-delivered noble gas radiator could be used to flash blind on temporary base unprotected individuals within hundreds of meters from ground zero. Such munitions used in a suitable moment will provide valuable tactical advantage.

Noble gas radiators are potent to cause fatalities or chronic injuries if not used with care.

Microwave projectors can be used as anti-personnel weapons and as anti-equipment or anti-materiel weapons. There was an intensive research in this area, in many countries, last two decades. As a result, a gamut of weapon systems, with different purpose undergoes trough intensive testing. Devices may be mounted on vehicles or may be handheld; there are also microwave projectors which are in the form of artillery shells and air bombs. Microwave projectors may even be satellite-mounted. (Fig. 2)

Depending on the frequency, intensity, duration, and waveform emitted, microwaves can cause a variety of effects in humans and animals. They can cause either readily noticeable or very subtle overheating or fevers.

They can induce memory impairment. They can cause temporary neural stunning or even blackouts.

Sensitive electronics, communication equipment, electrical grids are also amongst the targets against which the microwave projectors are effective. Principle of action of these devices or munitions is related with inducing of current in the human body or in the structures/equipment. When intensity is low, microwaves penetrating in human body not more than parts of the millimeters deep, generating unbearable heat. More powerful emitters may affect other organs or brain of the target. In the C3 systems, electronic equipment, electrical grids or materials, high-power microwave projectors inducing foucault currents which damage them irreversible.

Depending on intensity and frequency of microwave radiation, this type of NLW may cause fatalities. In most of the cases recovery of the equipment is difficult or impossible.

So called plasma-generating pyrotechnical compositions or explosives also felt into this category of NLW. These are pyrotechnical compositions or explosives, which when burning, generate cloud of low temperature plasma (with temperature over 3000K) containing high concentration of free electrons and ions. In order to achieve high level of ionization of the burn products, the plasma-generating compositions and explosives should on the one side burn at high temperatures, and on the other to contain elements and compounds of elements with low ionization potential. The elements form I-st A group of the periodic table has the lowest ionization potential. It is most of all the elements cesium, rubidium, and potassium and their compounds that presents a practical interest. The ionization potentials of these elements are as follows: Cs – 3.893 eV; Rb – 4.176 eV; K – 4.339 eV.

The plasma generating pyrotechnical compositions may be used against enemy's equipment, for counteraction of the radiolocation intelligence means, for distant activation of planted IEDs and others.

For the effective counteraction of the enemy radiolocation devices, a concentration of electrons in the burn products is necessary to be in the range $10^{17} – 10^{19}$ e^-/g- ionized gas.

Fig.2. Active Denial System, used by US Army for crowd and perimeter control – a microwave NLW (wavelength 3.2 mm, frequency 95 GHz) which heating the epidermis of a target person to about 55°C.

Electric stunners produce high voltage shocks in the targeted individuals. The shock is sufficient in amperage to cause muscular blockage, but not ventricular fibrillation or death.

Stunners include so called tasers (guns which shoot twin needle-ended wires connected to a pulse forming system), cattle prods (batons with two closely spaced electrodes at one end connected to a pulse forming system), electrically charged fences, and shotguns propelling small electric stunners. (Fig. 3) Use of electric stunners may cause fatalities.

Fig.3. Taser's eXtended Range Electronic Projectile (XREP)

Conductive chaff cloud consists of long strands of carbon or metal fibres or long thin metal strips. When dispersed over an area, the chaff will drift into power lines or transformers shorting them out and producing power

outages. It is often impossible to restore power until all of the chaff has been cleaned away from the power equipment and the nearby areas.

This NLW may indirectly cause fatalities and injuries. It may render equipment completely unusable for long time.

Lacrimators are chemical agents that irritate the mucous membranes and produce intense tear production, eye pain and throat congestion. Common examples are the chemical agents o-chlorobenzilidene malononitrile – CS, phenacyl chloride - CN or Mace, dibenzoxazepine – CR or DBO, and capsaicin – OC or Pepper Oil.

In isolated cases lacrimators may cause fatalities. In case used lacrimators are not declared by the country as a standard riot control agent, their application may be considered as a violation of the Chemical Weapons Convention.

Sternites are chemical agents that irritate the respiratory tract. They produce violent sneezing, severe nausea and vomiting.

Common examples are the chemical warfare agents from the group of arsenicals: Diphenylchloroarsine - DA, Diphenylcyanoarsine - DC, and Adamsite - DM. They may be dispensed from pyrotechnic grenades, smoke generators and when dissolved in suitable solvent from aerial spray tanks. These are very effective at incapacitating agents. Complete recovery occurs within a few minutes to an hour, once exposure to the agent is halted. The high toxicity of the sternites has caused their limited use. Sternites may cause environmental damage due to presence of Arsenic in their molecule.

In most of the cases the use of Sternites as NLW will be considered as violation of Chemical Weapons Convention.

Malodorants are chemical with extremely strong and usually offensive odors. For example, Butyl mercaptan has the characteristic odor of skunk, Skatole has the odor of fecal matter, Cadaverine has the odor of rotten meat, and n-Butyric acid has the odor of vomit. Other representatives are: Cortil mercaptan; Isonitriles; Solenoids; Sodium telluride; Geosmin; Benzcyclopropane etc. Sprayed onto individuals, a malodor ant will make others to leave their presence in order to avoid the smell. Malodor ant can disrupt the command and control of all but highly disciplined units. Most individuals whose bodies or clothing are partly covered with malodor ants will attempt to leave the area and clean themselves up. Malodor ants can discourage troops to occupy or even cross a contaminated zone.

During second Iraqi campaign US Army used modified 155 mm artillery projectiles XM 1063, charged with Skatole. As per the reports, the artillery fire mission achieves “effect of visible demoralisation”.

Super acids and super bases are acids and bases that are stronger than typical concentrated sulphuric acid and sodium hydroxide.

Hydrogen fluoride and chlorine trifluoride are superacids. Another class of super acids is obtained by mixing of metal fluorides and hydrofluoric acid (an equal mixture of antimony pentafluoride and hydrofluoric acid, for instance). The metal fluoride forms a complex that binds fluoride ions much more strongly than hydrofluoric acid binds fluoride ions. The result is an activation of hydrofluoric acid to acidity orders of magnitude stronger than normal. Super acids can dissolve almost all metals and glasses. Only a few plastics such as Teflon are unaffected. Relatively small amounts sprayed on vehicles or equipment could render them unusable by etching windows and optical components or by weakening metal structures or destroying critical metal parts such as wiring.

Cesium hydroxide is an example of a super caustic. It readily dissolves glass. Methyl sodium is another super caustic.

Both super caustics and super acids may cause fatalities and chronic injuries. Recovery of injured personnel may last as long as several months. Hydrofluoric acid and other fluorine based superacids interact with calcium and magnesium in the body and may cause cardiac arrest when enter into the blood stream. Wounds larger than 160 cm^2 are lifethreatening.

Polymer degradation agents are chemicals designed to deteriorate the physical properties of the polymers. Examples of polymer degradation agents include Organic solvents, powerful oxidizers, compounds comprising elements with changeable valences, depolymerising agents, etc. Super-acids can also be included in this group.

In some cases these agents might be used to dissolve rubber or to create cracks in tires of the vehicles or in gaskets of a plane cockpit in order to compromise the impermeability. In other case agent might be used to alter the aging of the polymer, transforming it into a brittle material. If applied to polycarbonate cockpit or bulletproof shield, after certain period of time, the polymer will lose it mechanical strength and would not be able to withstand the aerodynamic stresses during the flight or bullet impact. Yet another agent might turn polymer lubricants into an adhesive or even abrasive.

Polymer degradation agents are capable to damage the equipment to extent of making it unusable or requiring long and expensive recovery. They may cause environmental damage in some cases.

Metal embrittlers are chemicals that when applied to metals will alter their latice structure in such a fashion as to cause it to become brittle. The embrittled metals will later fail under operating stresses. For example, a metal embrittlers applied to supports of a bridge could cause it to collapse when a convoy of vehicles or a railroad train passed over it. Hydrogen is a common agent of this type. The liquid metals, mercury and gallium, are also known to act as embrittler to certain structural alloys.

Filter-slugging agents are chemicals that can polymerize or otherwise adhere when they come in contact with the fine mesh structures of air filters. Sprayed as an aerosol around a vehicle with a running engine, the inhaled agent would soon completely block the air filter causing engine malfunction. Change of the filter or long lasting cleaning with appropriate solvents would be required to recover the vehicle.

Filter-slugging agents may cause chronic lungs injuries or even fatalities as such agents might act to block the finest respiratory passages, just as they block the filter pores.

Fuel inhibition agents are chemicals that change the combustion properties of fuels, making them burn more or less efficiently. The chemicals may be added to fuel supplies by sabotage group or to be ingested along with air for combustion. An efficiency-enhancing additive, such as ether, acetylene or isopropyl nitrate in air (below flash point), could make an engine run considerably faster, or subject it to uncontrollable detonation that would rapidly lead to wear and engine damage.

An efficiency reducing additive would result in less energy and power per unit fuel consumption. Vehicles with such additives could not carry their intended loads or travel at expected speeds. The ultimate in efficiency-reducing additives would render completely unusable.

Other additives might produce by-products that are detrimental to engine life. Sugar added to gasoline will produce rapid carbon deposition that will eventually prevent proper ignition. Yet another class of additives changes the viscosity of fuels so that they are improperly fed into the combustion chambers. Some fatty acids with high molecular masses as naphthenic and oleic acid, their metal salts and even wax added to gasoline, causing carburetors to stop working.

Traction modification agents are chemicals or mixtures that either reduce traction by lubrication or increase traction by adhesion.

Lubricants can be sprayed on roads (especially on the curves), ramps, staircases, etc., to make them unusable. Personnel and vehicles will not be able to gain sufficient traction to guarantee stability or to exert any effective action. Lubricants which present practical interest are some of quickly hydrolyzing halogen siloxanes and some of the commonly used oils and greases.

Adhesives can be placed on the same surfaces to slow down and possibly immobilize moving personnel or vehicles. Among the examples of such agents are tar, some epoxy or polyurethane resins and fast-acting cyanoacrylate adhesives.

Inattentive and impetuous application of traction modification agents may lead to indirect fatalities and injuries and may render equipment

unusable for long period of time. Use of lubricants and adhesives may cause also environmental damage.

Obscuring smokes reduce the ability of many optoelectronic systems to provide visual information about targets. Smoke may be used to hide actions that might appear provocative to assembled crowds or adversaries. Smoke may be used to protect troop movements and prevent or delay directed fire until troops reach to hand-to-hand combat ranges. Smoke screens are effective mean in police tactic as well.

In general white smokes are more effective in blocking the radiation from visible part of the spectrum, while black and metalized smokes are more effective against propagation of infrared radiation. Obscuring effect of the cloud depends highly on the size of smoke's particles. When average size of smoke's particles is commeasurable with wavelength of the passing radiation, then level of absorption is maximal.

Obscuring coatings are basically adhesive materials which when applied to the external apertures of sensors form a nontransparent film. Such way these materials block signals entering or leaving the apertures. Different type of fast draying paints in spray form can be used for this purpose. Heavy oils, lubricants and petrolatum can also be used. Metalized paints are effective against infrared electro-optical sensors and radars. If such paint is applied on the radar's radio transparent housing, the resulting coating will effectively reduce the performance of equipment. Effectiveness of the coatings depends on density/thickness of the layer, the concentration of metal particles, the type of used metal and the size and shape of metal particles.

Tranquilizing agents are commonly used to sedate dangerous wild animals so that they can be transported or cured. Logicaly these agents can be use on humans. Tranquilizers are administered by use of hypodermic needles or darts or by use of suitable lipophilic solvents. One such solvent is Dimethyl Sulfoxide (DMSO), which has incredible high skin resorption. Representatives of this category of agents with potential for field use are barbiturates and flunitrazepam (or benzodiazepine).

Use of tranquilizers may cause chronic injuries and fatalities (mainly indirect) and may be considered as a violation of Chemical Weapons Convention.

Calmative agents are pharmaceutical chemicals that have a sedative or hypnotic effect on exposed individuals. If a riotous crowd were sprayed with such agents, their levels of emotion and motivation could be reduced to the point that they would no longer be capable of acts of violence or unrest. Such agents are likely to be considered as incapacitating chemical agents and would be banned by the intent of the Chemical Weapons Convention.

Examples of such agents are scopolamine; fentanyl; haloperidol; spiperone; fluphenazine. Potentially isophlurane and halothane.

Obviously main difficulty related with field use of calmative agents is even distribution and dosing of the agent. Over dosage is dangerous and may cause fatalities.

Strobing incapacitating torches as tactical NLW are based on the so called Bucha Effect, named after Dr. Bucha, who discovered this phenomenon in the 50-s. In essence these NLW are color lights (normally red and blue) that blinking with frequencies near the frequency of brain waves. (Fig. 4) Disorientation appeared within seconds after exposure. The incapacitating effect is a result of an "after image" caused by an exposure to high-intensity short light signals. Resulting “after image” is a function of brightness, time duration and frequency of the irradiation. When frequency of the light cycles is high enough, the brain cannot adjust and getting disoriented. Due to strobing light the photoreceptors in the eyes are unable to reset, which affects target’s vision. Light pulses forces the brain's perception input to arrive in segments, thus creating after images as the brain work trying to complete the partial image created by the momentary exposure of the strobe. These after images compound with each light pulse, which increases perceptual disparity.

Individuals do not react to strobing incapacitating torches in a uniform way. In solitary instances strobing light may alter an epileptic fit, in other cases target individuals may demonstrate resistance and may not be affected.

Fig.4. Strobing incapacitating torch

Restraining nets may be projected by special guns, called netthrowers. They may be erected across roads to act as barriers. They may be dropped from elevated platforms. They may be towed by small boats or submersibles.

Gun projected nets will entangle and trip up running peoples. Barrier nets can stop moving vehicles by catching entire car or by fouling car's tires. (Fig. 5) Similar nets are used on military airfields or aircraft carriers to catch plains that miss to hook at landing. Marine nets can be used to foul propellers of large boats. Depending on the purpose restrain nets are made of aramid or cordura fabric and may be reinforced with steel treads.

Fig.5. Restraining net

Adhesive foams are dispersion of gases into a liquid or solid matrix. Sticky foam is made from resins that have strong adhesive properties and take long times to set. Once stuck to an object, it will not easily come off and one piece of foam tends to stick to another piece of foam. Spraying such foam on adversary personnel will quickly immobilize him. (Fig. 6)

Special solvents are required to remove the foam and restore mobility. In large quantities, sticky foams can prove lethal. If a target falls and thoroughly covers his breathing passages, he will eventually suffocate. Hard foams are similar to sticky foams except that they set more quickly (seconds to minutes). This kind of foam can be used to create barriers to personnel and vehicle mobility. It can also be used to immobilize dusts or liquids (such as NBC agents) and can be used to absorb significant amounts of explosive energy. Aqueous foams are foams based on water and can be easily produced in large quantities. Unless the foam is directly inhaled or ingested in large quantities, the foam is breathable. Aqueous foam can be used to carry irritants, malodor ants, or calmative agents. It can also be used to limit mobility either directly (speed through a foam is much less than without the foam) or by using it to conceal devices such as entanglement nets.

Use of foams cause damage to environment. Even aqueous foams present certain risk to environment. It will take significant amount of time and efforts to recover affected equipment and personnel or area.

Fig.6. Immobilisation by use of adhesive foam

Bio-corrosive agents are aerobic and anaerobic microorganisms which perform corrosive action due to their ability to use metals, their alloys or polymer products as food or due to the corrosive action of their metabolite products (lactic acid, acetic acid, sulphuric acid, hydrogen sulphide). Sulphate reducing bacteria, Acidithiobacillus thiooxidans, Ferrobacillus ferrooxidans are representatives of aerobic corrosion active microorganisms. Desulfovibrio and Desulfotomaculum are representatives of some of the common anaerobic corrosion active microorganisms.

Sulfate-reducing bacteria produce hydrogen sulphide and can cause hydrogen embrittlement of steel and other alloys. Steel reacts with hydrogen sulphide, forming metal sulphides and nascent hydrogen, part of which diffuses into metal lattice and causing reduction of mechanical strength of the specimen.

Microbial colonies and deposits can also form concentration cells and accelerate galvanic corrosion.

Purposeful contamination of certain critical elements of the infrastructure may significantly accelerate their corrosion. Among the targets are pipelines, underwater steel structures, metal elements of the infrastructure, vehicles (including their polymer elements) under long storage, elements of electrical grid and sensitive electronic.

The use of bio-corrosive agents may be considered as violation of Biological Weapons Convention.

Fuel-eating biological agents are microorganisms which are able, naturally or as a result of genetic modification, to metabolize hydrocarbon (fossil) fuels. Genetic engineering makes it possible to grow an organism that requires only hydrocarbons and oxygen to live. Metabolite products render the fuel unusable. If adversaries' fuel supplies are contaminated with such organisms, after certain period of time, they will be completely destroyed. More than, if not detected at early stage the contamination may spread to all vehicles fuelling from the infected supplies. Potentially contamination can spread gradually to all adversaries' vehicles effectively immobilising them. If possible at all, disinfection would be incredibly costly and time-consuming operation.

Most certainly the act of use of fuel-eating biological agents will be considered as a violation of the Biological Weapons Convention.

The list of NLWs presented above covers most promising representatives, as per authors' opinion. Most probably the list is not complete. Some of the capabilities of discussed technologies are summarized in Table 2. It is pretty obvious that this domain of law enforcement and military technologies is under intensive development and number NLW will constantly grow. This is natural process which is predetermined by the striving for reduction of fatalities while increasing police and military effectiveness and capabilities.

3. Conclusion

Despite discernible humanitarian motives, many representatives of this category of weapons are still highly contradictory. At first glance, the idea for bloodless war shows promise. By using appropriate NLW in the course of riot control action or combat at the tactical level, an adversaries could potentially be incapacitated, which would allow control or victory to be achieved without or with minimal human sacrifices. The horrors of war will be avoided, and the military operation will obtain a character of military expedition. Undoubtedly, the achievements in the domain of NLW and chemical, biological, and medical science make it possible to implement this

idea. At the same time, many military and international law specialists have serious doubts about the lawfulness and humanity of such actions.

Firstly, the use of many of the abovementioned NLW representatives may be considered as a violation of certain international treaties or local policies. Biological Weapons Convention and Chemical Weapons Convention clearly stipulate purposes for which use of biological and chemical agents are allowed. Many environmental acts also prohibit use of certain elements of some NLW concepts.

Any revision of the Chemical or Biological Weapons Convention in a way that allows the use of the toxic properties of chemical agents or action of biological agents in the course of hostilities is impossible. Such act will be of a substantive nature and will largely suspend their action. This would create a dangerous international precedent and should not be allowed.

On the other hand, there are serious psychological barriers to the realization of the bloodless war.

War brings enormous demands on the psychological and physical endurance of participants. It is accompanied by a huge amount of a variety of stressful factors. The effects of these stressors are permanent, and under their influence, the participants undergo physiological processes leading to serious hormonal changes. As a result of the changed neurophysiological process, specific, visible changes occur in both the physical state of the person, and his emotional and behavioural responses.

Some of the natural emotional responses to stress are: loss of self-control, chronic feeling of danger, anxiety, tension, depressed mood, apathy, anger, irritability, aggression, sense of failure, and misunderstanding of others, etc. It can be said that stress, in all its manifestations, is a normal reaction to an abnormal event.

In the course of an armed conflict there is no commander in any army capable of fully guaranteeing the behaviour of his subordinates. With a high degree of probability, it can be expected that in the absence of a reciprocal reaction by the opposing party, the anger of the enraged and stressed soldiers will grow into violence, regardless of the strength of their pre-war moral foundation. Unfortunately, such behaviour has been seen repeatedly, including in the course of the conflicts of the last two decades. These psychological effects call into question for the observance of the norms of international humanitarian law.

Summing up the above considerations, we can conclude that undoubtedly there are broad perspectives for NLW use in the future conflicts or law enforcement practice. In the same time we should be more careful when fielding them. Opinions on the problem of the lawful use of NLWs, especially in war condition, are highly polarized. Proponents of the idea of

their use emphasize on their non-lethal nature, while adversaries highlight and analyze the risks associated with their use. As it has been mentioned, many of the listed NLW, although "non-lethal" or at least "less-lethal", are still in the grey area between admissible and prohibited. Use of most of the chemical substances and biological agents in the form of NLWs may be ban by Chemical Weapons Convention or Biological Weapons Convention in certain situations. Use of other representatives hides significant risks of disproportional collateral damages to environment or structures. NLWs advocates should be conscientious enough and not to over promise about the suitability and performance of NLW. No weapon, or family of weapons, from discussed above, is perfect or Omni purpose. At best, NLW offers a set of alternative tools rather than a sweeping solution.

What should occur at this point is an extensive work on exploring all aspects of NLWs employment, from lawful use limitations and ethic restrains to actual field effectiveness and safe, uninjurious tactics. Base on that, existing protocols and standard operational procedures should be refined and augmented. Serious investments should be made in education and training for commanders and operators which should reflect, again, all aspects NLWs employment. The level of collateral damages and unexpected effects during the conflicts where these new technologies were applied shows that we are still far from their skilful using.

REFERENCES:

1. E. Katuga, G. Donovic, Contemporary technologies and humanisation of the War, 2009 Report to JDH-bord Kanbera, AU
2. N. Eisenreich, J. Neutz and K.D. Thiel, 2003, Novel Barriers Systems as Non-Lethal Weapons, proceedings of the 2nd European Symposium on NLW, 13–14 May 2003, European Working Group on NLW, Germany;
3. General Dynamics, 2002, Long Range Acoustic Device (LRAD), Product Information Sheet.;
4. H. Griffioen-Young, 2003, Effects of Non-Lethal Weapons on Humans, proceedings of the 2nd European Symposium on NLW, 13–14 May 2003, European Working Group on NLW, Germany;
5. 5. See S. Le Vine, 2002, Human Effects and NLW Acceptability, presentation to the NLW conference, 26–28 March 2002, National Defense Industrial Association, US;
6. Chemical Weapons Conventyion, 1997;
7. Biological Weapons Convention.

Author's name: Milko Berner, PhD
Workplace: Deputy Minister at Ministry of Interior of Republic of Bulgaria
E-mail: alphachem@abv.bg

LEGISLATIVE BASIS FOR THE IMPLEMENTATION OF SPECIAL INTELLIGENCE MEANS IN THE UNITED STATES OF AMERICA

Ilin A. Savov

ABSTRACT: *This article examines some of the procedures for technical surveillance in criminal investigations of US citizens. The capabilities and limitations of individual entities entitled to control communications in the United States of America are outlined. Some of the procedures regarding the use of acquired intelligence data in connection with criminal proceedings are assessed.*

KEYWORDS: *National security, Technical surveillance, Criminal investigations, Electronic Communications Service, Special intelligence means.*

Introduction

Officially, the US is a federal constitutional republic consisting of 50 states and one federal district representing its capital; Washington. Forty-eight of the states and the Columbia County lie in the middle of the continent, located between the Pacific and the Atlantic, bordering Canada to the north and Mexico to the south. The State of Alaska is located northwest of Canada, and Hawaii is an archipelago located in the middle of the Pacific Ocean. The country also has five populated and nine uninhabited territories in the Pacific and the Caribbean. The United States ranked third in population numbers (318 million people), including diverse ethnic groups with diverse cultures, a product of intense immigration from many other countries. The state accounts for 36.6% of the world's military spending, making it an economic and military leader. Such a conclusion can also be made with regard to the means devoted to the protection of national security, the fight against international terrorism and crime. In the United States, the first of Echelon's global communications control systems, primarily designed for intercepting radio waves (satellite communications and terrestrial radio communications), was set up. Subsequently, other systems have been created, for example, to control and analyze data transmission networks.

Procedures for operational and technical surveillance in criminal investigations of US citizens

The Basic Law, which regulates the application of special operational and technical means to investigate crimes committed by US persons, is the Code of Laws of the United States of America. Abbreviated in various ways

such as: United States Code of Conduct, US Code, US Code, U.S.C. or USC, it is the official compilation and codification of the United States federal and federal law. Contains 53 titles (Volume 1 to 54, except Volume 53, which is saved). For the purposes of this article, the main interest is Volume 18 - Criminal Procedure and Criminal Procedure. For convenience of readers this basic document will be shortly referred to as the "Code".

Interception of wired, electronic and oral communications. It should be paid attention to that of particular interest is Chapter 119 "Interception of Wired and Electronic Communications and Interception of Oral Communications" (Chapter 119—Wire and electronic communications interception and interception of oral communications).

Section XVIII of 18 USC describes in great detail the prohibition of interception of wired, electronic and electronic messages. Unless otherwise provided in this Article, it shall be expressly prohibited to any person: (a) intentionally intercepting, attempting to intercept or compel any other person to intercept wire, or oral or electronic communication; (b) deliberately use, endeavor to use or assign to any other person to use or attempt to use any electronic, mechanical or other device to intercept any oral communication when:

- such device is attached to or otherwise transmitted by a wire, cable or other similar connection used in wired communications;
- such a device transmits messages over the radio or prevents the transmission of such communication;
- that person knows or has reason to know that such a device or component thereof is mailed or transported through inter-city or international trade;
- such use or attempt to use: (a) is carried out on the premises of any business or other commercial establishment whose operations affect inter-city or international trade; (b) receives or seeks to obtain information relating to the business of any business or other commercial object whose operations affect interstate or international trade; or (c) intentionally to disclose or to attempts to disclose to another person the content of any wired, electronic or electronic communication knowing or having reason to know that the information is received by tapping this communication; (d) knowingly use or attempts to use the contents of wire, electronic or electronic communications knowing or knowingly knowing that the information has been obtained by offsetting in violation of this paragraph.

At the same time, the same paragraph allows an operator, employee or agent of a cable or electronic communications service provider whose

equipment is used in the transmission of wire or electronic communications to intercept, disclose or use such communication in its normal course of business, while engaged in any activity required to perform the service or to protect the rights or property of the service provider, except that a public telecommunication service provider services does not use the control and surveillance service, except for periodic mechanical checks or service quality checks.

Notwithstanding any other law, providers of cable or electronic communications service, their operators, officers and agents, landlords, trustees or other persons are entitled to provide information, facilities or technical assistance to persons intercepting wired, or electronic or electronic communications or to perform electronic surveillance as defined in Art. 101 of the Foreign Intelligence Surveillance Act 1978, provided that such supplier, its operators, employees or agents, landlord, trustee or other specified persons are provided with:

A) A court order requiring such assistance or court order pursuant to Art. 704 of the Foreign Intelligence Surveillance Act 1978, signed by the authorizing judge, or

(B) Written testimony by a person referred to in § 2518 (7) of this Chapter of the Code or by the Attorney General of the United States that a law order or court order is not required by law, that all legal requirements are met and that a specific assistance, indicating the time period during which the provision of information, facilities or technical assistance is permitted, and specifies the specific requirements.

It is not unlawful for a person acting within the scope of the law to intercept wire or electronic messages to a computer offender transmitted to, through, or from a secure computer when: (a) the owner or operator of the secured computer allows the interception of the computer criminal's the secured computer; (b) the person acting within the law is legally engaged in an investigation; (c) the person has reasonable grounds to believe that the contents of the computer's communications - offenders - will be relevant to the investigation; and (d) such interception does not receive communications other than those transmitted to or from the computer - the offender.

It is also not an illegal provider of electronic communications services to the public or a remote computer service to intercept or disclose the content of wire or electronic communication in response to an order from a foreign government in response to an executive contract that the Prosecutor General has designated and certified before Congress, that it complies with § 2523 of the Code. Depending on the type and severity of the offenses, administrative or criminal sanctions are provided for.

Paragraph 2512 of the Code expressly prohibits the production, distribution, possession and advertising of wire, electronic or electronic interception devices. Penalty is imposed by a fine under this ordinance or imprisonment, but not more than five years, or both penalties together. Any electronic, mechanical or other device used, transmitted, transported, produced, assembled, owned, sold or advertised in violation of §2511 or §2512 of the Code may be seized and confiscated in the United States.

Chief Prosecutor, Deputy Attorney General, Associate Attorney General, one or any Assistant Attorney General, including the assistant attorney general, or any Assistant Deputy Attorney General a Chief Prosecutor, or the person in charge of that position in the Criminal Department or National Security Department, may grant a request to a federal judge from a competent court, and that Judge may provide, in accordance with § 2518 of the Code, an order to authorize or approve the set-off wire or verbal communications from the Federal Bureau of Investigation (FBI), or a federal agency responsible for investigating the offense for which the application is filed, where such set-off can provide or provide evidence.

Paragraph 2516 lists in very detail the crimes for which wire, electronic and electronic communications can be controlled. They are divided into 19 strands covering hundreds of types of crime.

In contrast to the Special Intelligence Means Act in the Republic of Bulgaria, besides mentioning the articles of the Bulgarian Penal Code, the American brief also mentions the nature of the offense. By way of example, we will mention a section of § 2516 (1) (a): ... Chapter 10 (Regarding Biological Weapons) Chapter 37 (Relating to Espionage) Chapter 55 (Relating to Abduction) Chapter 90 of trade secrecy), chapter 105 (referring to sabotage), chapter 115 (pertaining to treason), and so on.

It is important to note that this observation can be applied to any offense punishable by death or by imprisonment for more than one year.

The chief investigating prosecutor of each State or the chief investigating prosecutor of any of its State Units, if such a prosecutor is authorized to have that status, has the right to file a request with a court judge with the competent court for an order authorizing or approving the interception of wire, electronic messages. This judge may provide, in accordance with § 2518, an order authorizing or approving the interception of wire or electronic communications by investigating or law enforcement officers responsible for investigating the offense for which the application was filed. The judge must be convinced that when such offsetting can provide or have provided evidence of committing the crime of killing, kidnapping and trafficking in human beings, exploitation, child pornography, gambling, robbery, bribery, extortion, narcotics, marijuana or other

dangerous drugs or other crime that is dangerous to life, health or property, and punishable by a term of imprisonment of more than one year specified in any applicable State law permitting such interception, or any preparation for committing any of the above crimes.

Similar powers have any attorney for the government who can resolve an application to a federal judge with jurisdiction where such offsetting can provide evidence of federal crime.

Any request for an authorization to approve or approve the interception of wire, or electronic or electronic communication under this Chapter shall be filed in writing before a judge of the competent court and shall indicate the applicant's power to file such an application. Each application shall include the following information:

(a) The identity of the investigating or law enforcement officer who lodged the application and the officer authorizing the request.

(b) A full and complete account of the facts and circumstances to which the petitioner refers in order to justify his conviction that an order should be issued, including: details of the particular offense that has been committed; a specific description of the nature and location of the facilities from or to which the message is to be intercepted; a specific description of the type of communication to be intercepted; the identity of the person (if known) who committed the crime and whose messages should be intercepted.

(c) A full account of whether other investigative procedures have been taken and, if not, what the grounds are deemed to be unlikely to succeed if they were used or that they were too dangerous.

(d) A statement of the period of time for which the offsetting is required. If the nature of the investigation is such that the intercept of interception is not automatically terminated when the type of communication described above is initially intercepted, a specific description of the facts identifying the likely reason for believing that additional messages of the same type will then appear.

(e) A complete statement of the facts relating to all previous requests known to the person who made the request made to a judge for a set-off or for the approval of interception of wire, electronic or electronic communications of the same persons, facilities or places in the application, and the actions taken by the judge for any such request.

(f) Where the request relates to the continuation of a request, a statement indicating the past performance of the set-off or a reasonable explanation for the inability to obtain such results.

The judge may ask the applicant to provide additional evidence or documentary evidence in support of the application.

In response to such a request, the judge may authorize or approve the interception of wired, electronic or electronic communications in the territorial jurisdiction of the court in which the judge is sitting (both outside and within the United States in the case of a mobile interception device authorized by a federal court within such a jurisdiction) if the judge determines, on the basis of the facts presented by the applicant, that:

(a) Has a valid reason to believe that a person is or has committed, or intends to commit, a particular offense listed in § 2516 of the Code.

(b) There is good reason to believe that specific communications about this crime will be obtained by such offsetting.

(c) Normal investigative procedures have failed or were unlikely to succeed if they have been used or are too dangerous.

(d) There is a reasonable cause to believe that the equipment from or to which interception of wired, electronic or electronic communications is used or is to be used in connection with the commission of such a crime or is rented, on or customarily used by such person.

Any order authorizing or approving the interception of any wire, electronic or electronic communication shall contain:

(a) The identity of the person, if known, whose messages are to be intercepted.

(b) The nature and location of the communication facilities in respect of which or the location to which the offsetting permission is granted.

(c) A specific description of the type of message to be captured and descriptions of the specific offense to which it relates.

(d) The identity of the agency authorized to intercept communications and the person requesting the request and

(e) The period of time during which such interception is permitted, including a statement as to whether the set-off is automatically terminated at the time when the described message was received for the first time.

The order obliges the provider of a Wired or Electronic Communications Service, landlord, trustee or other person to provide without delay to the applicant all the information, facilities and technical assistance necessary to perform offsetting which do not cause difficulties and minimize interference with the services, which this provider performs for the person whose communications should be intercepted. Any supplier of a cable or electronic communications service providing such facilities or technical assistance shall be compensated by the applicant for reasonable costs

incurred in the provision of such facilities or assistance. This is done under the Law on Communication Assistance in Enforcement.[3]

The order may not authorize or approve the detention of any wire, electronic or electronic communication for a period longer than is necessary to achieve the purpose of the authorization and in any event not more than thirty days. Such a 30-day period shall begin to run from the day on which the investigating officer first commits offsetting according to the date in the order or within ten days after the order is registered. The continuation of an order may be made, but only when a request for an extension is made, by the court which issued the initial authorization. The extension period may not be longer than that which the authorizing judge considers necessary for the achievement of the objectives but in no case may it be more than thirty days. Each warrant and continuation must contain a provision that the set-off permit is executed as soon as possible, is conducted in such a way as to minimize the interception of messages that are otherwise not subject to interception and must ends when it reaches the authorized target, but not more than thirty days. In case the captured communication is coded or in a foreign language, and an expert in that foreign language or coding was missing during the set-off period, the action must take place as soon as possible after such set-off. Capture can be done wholly or partly by government officials or by a person under contract with the government acting under the supervision of an investigating officer or law enforcement officer authorized to offset.

The judge who issued the order may require that he be informed of the progress made to achieve the legitimate purpose and the need for continued interception. Such reports are made at intervals that the judge has the right to determine.

Any employee of an investigative or law enforcement authority specifically designated by the Prosecutor General, the Deputy Prosecutor General, the assistant to the Chief Prosecutor or the principal investigating prosecutor of a State or other person performing such duties in accordance with the status of that State may order interception of wire, electronic or electronic communications for a period of 48 hours if it considers that an emergency exists, which includes:

• Imminent danger of death or serious physical injury to a person;

• Conspiratorial activities that threaten the interests of national security; or

[3] Communications assistance for law enforcement act - [P.L. 103–414, Enacted October 25, 1994]]

• Organized crime conspiracy activities that require interception of wired, verbal or electronic messages.

Within this period an order for permission to set off must be obtained. In the absence of an order, such set-off shall be immediately terminated: when the requested notice is received or when the request for an order is denied, whichever is the earlier. In the event that such an application for approval is refused or in any other case where the set-off is terminated without an order being issued, the content of the wire, electronic or electronic communication captured shall be deemed to have been obtained in violation of the Code.

The content[4] of any wire, oral or electronic communication intercepted in any way should, if possible, be recorded on a tape or other similar device. The recording of the contents of each communication is done in a way that protects the record from editing or making other changes. Immediately after the expiry of the warrant or its continuation, these records shall be provided to the judge who issued the order and sealed as instructed. Record keeping is done wherever the judge orders. They can not be destroyed except by order of the judge who authorized or denied them and in any case kept for ten years. For the purpose of investigations, duplicate records may be made for use or disclosure under the provisions of § 2517, which will be considered later.

Requests and orders issued under this paragraph shall be sealed by the judge. They are also stored in a place they ordered. Such requests and orders shall be disclosed only on presentation of a valid reason to a judge of the competent court and shall not be destroyed except by order of the judge who authorized or rejected them but shall in any case be kept for at least ten years.

Within a reasonable time, but not later than ninety days after the application for approval has been filed, where it has been refused, or upon termination of the order or its extension, the Judge may order service of the notice to the persons referred to in the order or request, and the other persons of the seized messages, but if he judges this to be in the interest of justice. The notice includes:

- the fact of the order or the request;
- the date of entry and the period of the authorized, approved or non-approved set-off or rejection of the application; and
- the fact that wire, oral or electronic communications have been or have not been seized during the period.

[4]18 USC 2510 (8) "content" when used in connection with any wired, electronic or electronic communication includes any information about the nature, purpose (general meaning) or meaning of this message;

The judge may, at his or her discretion, provide such person or his lawyer with inspection of such parts of the intercepted messages, requests and orders as he judges to be in the interest of justice. Where sufficient reasons are provided to the judge by a competent court, the transmission of the notification required by this paragraph may be postponed.

§ 2517 of the Code regulates the way in which information obtained from the interception of wire, electronic and electronic communications may be used.

Any investigator or law enforcement officer who has received information on the content of any wire, electronic or electronic communication or evidence arising from it may disclose that content to another investigator or law enforcement officer as long as such disclosure is appropriate for the proper performance of the official duties of the employee who transfers or receives the disclosed information. He may use the content of these intercepted messages in a way that is appropriate for his / her duties.

Any person who has received, in any way permitted under this paragraph, information related to wire, electronic or electronic communications or the evidence obtained through it may disclose the content of that communication or the evidence when it gives evidence oath in any procedure conducted in accordance with the laws of the United States or of any state or US state.

When an investigator or law enforcement officer, while engaged in offsetting in its authorized manner, intercepts wire, electronic or electronic communications relating to offenses other than those specified in the permit or approval order, the content and evidence obtained from them may be discovered or used in a manner as already mentioned. Such content and any evidence may also be used when authorized or approved by a judge in the competent jurisdiction when the judge has determined from a subsequent request that the content has been otherwise seized. Such a request should be made as soon as possible.

Any investigator or law enforcement officer or lawyer of the Government who by any means permitted under this part of the Code has received information about the content of any communication or evidence arising from it may disclose such content to another employee of the federal immigration, national defense or national security when the content relates to foreign intelligence or counterintelligence (as defined in Section 3 of the National Security Act by 1947 (50 USC 401a)), or foreign intelligence[5], to

[5] "foreign intelligence" for the purposes of § 2517, (6) of this Volume 18 is:
(A) information, whether affected by a person in the United States, which relates to the ability of the United States to defend against:

assist the official who is to receive this information in the course of his duties. Any federal official who receives information under this provision may use such information only when necessary in the performance of his / her duties, subject to the limitations of unauthorized disclosure of such information. Similar rights and obligations are also disclosed when disclosing such information to a foreign public official when such content or evidence from its derivatives discloses a threat to actual or potential attack or other hostile hostilities by a foreign or foreign agent for national or international sabotage, domestic or international terrorism or illegal intelligence activities from an intelligence service or a network of foreign powers or a foreign force agent in United is the US or elsewhere, the goal is to prevent or respond to such a threat. Any official receiving information under this provision may use this information only in accordance with the guidelines jointly issued by the Prosecutor General and the Director of Central Intelligence[6].

Also interesting is the way in which information from the control of wire, electronic and electronic communications in US lawsuits can be used.

The content of any wire, oral, or electronic communications intercepted or evidence obtained from it can not be obtained as evidence or otherwise disclosed in proceedings, hearings or other proceedings in a federal or state court, unless less than ten days prior to receiving a copy of the court order and the accompanying application under which the set-off was authorized or approved. This ten-day time limit may be revoked by the judge if it finds that it is not possible to provide the parties with the above information ten days before the hearing and that the parties will not be affected by the delay in obtaining this information.

Any injured person in any court case may request from or in front of a judicial authority, department, official, agency, regulatory body, or other United States, state or US entity, cancellation of content from intercepted wired or voice communications and the evidence relating to them, on the basis of:

- the message is unlawfully intercepted;

(i) actual or potential attack or other serious hostile action by a foreign force or an agent of foreign power;
(ii) sabotage or international terrorism by a foreign force or an agent of foreign power; or
(iii) Illegal intelligence activities of an intelligence service or network of alien forces or an agent of alien power; or
(B) information, whether afflicting a person from the United States or not, in respect of a foreign authority or a foreign territory that relates to:
(i) the national defense or security of the United States; or
(ii) actions in the United States' foreign affairs.

[6] The Director of Central Intelligence (DNI) is the head of the United States Intelligence Community. Do not be confused with the Director of the Central Intelligence Agency (CIA).

- the authorization or approval order under which it was intercepted is incomplete; or
- the eavesdropping is not performed in accordance with the permit or approval order.

Such a proposal must be made before the trial, the hearing or the proceedings, unless it was possible to make such a claim or the person did not know the grounds of the proposal. If the proposal is made available, the contents of the wire or oral communication captured or the evidence obtained from it shall be deemed to have been acquired in violation of this Chapter of the Code. When submitting such a proposal by the victim, the judge may at his discretion provide the victim or his defense counsel for examination of such parts of the detained message or the evidence he or she receives when judging that it is in the interest of justice.

In addition to any other right of appeal, the United States has the right to appeal against an order to file a request to remove information obtained by intercepting communications, or to refuse an application for an approval order if the United States Prosecutor certifies to the judge or otherwise an official who has made such an offer or who refuses such a request that the appeal has not been lodged for the purpose of delay. Such an appeal will have to be dealt with within thirty days of the date of entry of the order and before the commencement of the trial.

The remedies described in respect of interception of electronic communications are the only remedies and penalties for unconstitutional infringements involving such communications, they do not apply to the specification of the facilities from which or where offsets are made.

Interception of messages transmitted by wire or electronic communication can not commence until the location where the message can be intercepted is detected by the person making the interception. The provider of these communications services may ask the court to amend or cancel the order on the grounds that the set-off can not be done in a timely or acceptable manner. The court, after notifying the government, immediately decides such a proposal.

Conclusion

In the current conditions, given the many potential threats to national security, obtaining up-to-date, forward-looking information is key to securing the security environment in the United States of America. In doing so, one of the sources of information should not be ignored. The information obtained through the use of special intelligence means and the control of communications networks and systems is crucial for the detection and detection of criminal offenses, but its importance is great and will continue to

increase for the purposes of information, analytical, prognostic and preventive activities in the protection of US national security.

REFERENCES:

1. Code of Laws of the United States of America
2. Communications assistance for law enforcement act - [P.L. 103–414, Enacted October 25, 1994]]
3. Foreign intelligence surveillance act of 1978 [Public Law 95–511; 92 Stat. 1783;]
4. Special Intelligiance Act of Republic of Bulgaria

Author's name: prof. Ilin Savov, PhD
Workplace: Higher School of Security and Economics, Dean of Department „National security and public order"
E-mail: ilin_savov@abv.bg

BASICS OF CORPORATE SECURITY

Marta D. Kovacheva

ABSTRACT: *In this article, an analysis of security threats for corporate security has been made. Different aspects of security, like crime prevention, information security, crisis management etc. are considered. Measures to improve the business security are proposed.*

KEYWORDS: *Corporate Security, Information Security, Cyber Attacks, Social-engineering.*

1. Introduction

With the rising number of cyber attacks, natural disasters and intellectual property theft cases, corporate security has become a priority in the business world. Each year, more than $600 billion is lost due to cybercrime. In 2016, there were over 4,000 ransomware attacks on a daily basis in the U.S. alone. Yet, many small businesses either overlook or ignore corporate security. Big companies, on the other hand, invest millions in the latest security software and equipment [1], [2], [5], [6], [7], [8], [10], [11].

2. What Is Corporate Security?

The role of corporate security is to protect organizations, their technologies, employees, technical resources and customer data from internal and external threats. Its ultimate goal is to ensure the proper functioning of your company and mitigate risks. As a business owner, you can hire security personnel, purchase security software and switch to more advanced technologies to protect your company's tangible and intangible assets [1].

Global security spending is forecasted to reach $96 billion this year, which is 8 percent more compared to 2017. Organizations are spending large amounts of money to prevent security breaches, protect financial data and detect cyber attacks before they escalate. In a 2016 survey, 53 percent of respondents stated that security risks are their primary concern [3], [4], [5].

In 2017, companies have spent more than $4.695 million on identity access management, $57.719 million on security services, $11.669 million on network security equipment and $17.467 million on infrastructure protection. The GDPR or General Data Protection Regulation, which came into effect on May 28 this year, has forced companies to prioritize data security and reveal the extent of cyber attacks within 72 hours [2].

The new data protection regulations apply to all companies that are dealing with EU customers, not just to European organizations. Failure to comply can result in fines of up to 20 million Euros or 4 percent of a company's annual global turnover. Corporations and other large organizations are now required to employ Chief Information Security Officers and Data Protection Officers to ensure their compliance with the GDPR. Under the new law, companies have significantly more legal liability in the event of a data breach [9], [10], [11], [12], [13].

Making sure your business follows the latest security practices is important. Whether you own an online store, a dining venue or a law firm, you must take the steps needed to protect customer data, safeguard your financial records and prevent cyber attacks. Failure to do so can damage your reputation and cause revenue loss. In the worst case scenario, you could end up in jail or be forced to close your business [1].

3. The Role of Corporate Security

The ever-changing business environment along with the rising number of security risks is driving the demand for data security professionals and services. It's estimated that over 4,000 ransomware attacks, 33,000 phishing attacks and 300,000 new malware cases are detected daily in the U.S. alone. Furthermore, approximately 780,000 data records are lost to hacking. In this digital era, cybercriminals are getting better and better at stealing information and evading network defenses.

In a survey, 71 percent of U.S. companies and 67 percent of international enterprises reported suffering at least one data breach. External threats account for more than 75 percent of these attacks. In 2017, the average cost of a data breach was $3.62 million.

Identity theft is on the rise, too. Cybercriminals often use stolen data to obtain credit, purchase goods, engage in drug trafficking or enter a country illegally. Large companies like Choice Hotels International, Allstate Insurance Company, Ullico Inc., M&T Bank and Equity Resources, Inc. reported data breaches in 2017. Not to mention Equifax, Scottrade, JP Morgan Chase and other breaches those were extensively covered by the media [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

Assuming that your business implements the latest technology to deter cybercrime, there still is the risk of employee theft, vandalism and burglary. Without a security team in place, your company is vulnerable to these threats.

Employee theft, for example, is responsible for losses of up to $50 billion annually. A staggering 75 percent of workers have stolen at least once from the company for whom they worked. Approximately 33 percent of U.S.

companies filed bankruptcy due to employee theft. It takes about two years on average to detect this kind of fraud.[4]

The role of security in the corporate world is to mitigate these risks and reduce their impact. This industry has several branches, including [1], [4], [5], [6], [7], [8], [9], [10], [11], [12]:

- Risk management.
- Fraud deterrence.
- Crime prevention.
- Compliance programs.
- Information security.
- Physical and personal security.
- Crisis management.
- Corporate governance.

Each niche has several sub-categories. Information security, for example, encompasses data security, cloud security, infrastructure protection, customer security software, identity access management and more.

Depending on your budget and type of business, you can focus on one or more of these areas. Currently, approximately 35 percent of companies are using multiple data security tools, such as data backup and encryption software. This number is expected to reach 60 percent by 2020.

Let's say you have a small retail store. In this case, you're facing the risk of employee theft and fraud, cash register tampering, false price adjustments, refund fraud, burglary and more. Therefore, it's crucial that you have a security policy in place and use the right tools to deter these crimes. Simple things such as streamlining the company's policies, implementing eligibility verification and installing surveillance cameras, can go a long way toward your security.

A corporation, on the other hand, has more extensive needs. It has to employ a security manager, hire a security team, implement awareness programs and invest in the latest technology to prevent data breaches and cyber attacks. Some companies also provide their employees with an Identity Monitoring benefit, which helps lower the risk of identity theft and increases cybersecurity [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

4. How to Increase Business Security

The first step to safeguard your small business from cybercrime, theft and fraud is to create a security policy. This document should outline the best security practices for your company, such as developing fraud prevention strategies, managing physical security hardware, controlling ID pass access and implementing security awareness programs for your staff.

Consider hiring a security officer to make sure your employees follow these practices. He will be responsible for keeping your business premises secure and protecting your staff. Security officer duties may include monitoring entrance of people or vehicles in the office building, maintaining order, detecting signs of intrusion and answering alarms. He may also take messages and answer phone calls on weekends and during non-business hours [1], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22].

Make sure you also purchase security software and update or upgrade existing technologies in the workplace. Depending on your needs, you may switch to multi-factor authentication, use data-centric encryption for your files and email, back up your data and set up individual logins for your employees.

Your security policy should also include the steps employees must follow in case of theft, data breaches, natural disasters and other emergencies. Ask them to regularly back up the files on their computers, use stronger passwords and keep their software up to date at all times. Train your staff on corporate security so they can identify and prevent any issues that may arise.

Protecting customer data and business premises should be a priority for your organization. Take action to secure your business online and offline, instruct and prepare your staff and put strict permission levels in place to safeguard your files.

"The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved", this was stated by Confucius. Corporate security has become an ongoing problem for small businesses owners around the country and many are facing difficulties in determining what kind of precautions to acquire when trying to prevent security concerns from happening. In order for a small business owner to have quality security over their business they must look at all different sectors including physical security, data security, business transaction security and finally computer security of their businesses [1], [4], [5], [6], [7], [8], [9], [10], [11], [12]. The security of a small business is dependent on how well the owner takes into consideration all the different possibilities and how the owner wants to monitor all procedures that may entail their business. Corporate Security is an important matter that all small business owners are going to have face and the sooner they confront the issues, the better the company will be in eliminating problems in the long run.

Physical security is significant to any company that wants to prevent invaders from entering their business without permission. Physical security

can include safety measures such as: door locks, alarms, security guards, cameras, fences and smoke detectors. Another type of physical security is separating the obligations among employees and not letting one major task be completed my just one person. Physical security is usually one of the first tasks accomplished by small business owners in undertaking the mission of protecting their businesses, without physical security businesses would be accessible for anyone within reach [1], [4], [5], [6], [7], [8], [9], [10], [11], [12], [23], [24], [25], [26], [27], [28].

Data information seems to be another sector of small business that needs to be confined and the appropriate accommodations must be applied by owners in order to keep any private documentation or information that does not want to be revealed to outsiders. Data security can include: passwords, finger prints, access cards and cryptography. Cryptography is used to protect data by transforming it into a form that seems useless, unless you have the cryptographic key to make sense of the data. Data security is used to enable outsiders to view any information that a small business might not want known and helps shield against any hacking that may involve their monetary accounts.

Business transaction security seems to have become another large challenge for small business owners in today's current market and monetary transactions are one of the most important division to protect against outsiders. Business transaction security includes bank vaults, one-time passwords, secure monetary transaction system and trustworthy employees. Small business owners must have a secure system designed to be able to account for all monetary transactions going in and out of the business. Bank safes must only be accessible to key employees and have a valid security system in order to gain admission into the vault.

Computer security puts constraints on a business computer and denies availability of information to those who are not inside the company. Computer security can include firewalls, back-ups of information on hard disks, encryption, anti-virus programs and detailed passwords. Hackers are increasing their knowledge everyday on the topic of computer security and they are inventing new ways of hacking into small businesses' computers. If small business owners use these precautions and observe all computer usage closely, they can avoid any future theft into their system [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

Small businesses today use the Internet and computing networks as important business necessities more than ever before. While connectivity is necessary for success in one's business, being connected also means that the company is more exposed to outside threats. Larger companies have the resources to have security experts to protect their systems, but small business

owners must make their own decisions on how to secure their important information.

Security issues such as viruses, hackers, and worms becoming a huge threat to the vital information of a company, one would assume preventative measures would be at top of the list of things to do for small businesses. After all, these are serious threats with serious consequences, but many small businesses have not taken the steps to safeguard their information. The problem is that small business owners are simply unaware as to what steps they should take or even where to start [5].

Many small business owners believe that they do not need to worry about computer and online security because why would someone target them when there are much bigger companies that can be hit. Hackers and thieves however know that small businesses are often more vulnerable to attacks because of limited security measures, making them an easier target. One of the favorite ways thieves attack small businesses is sending mass worm outbreaks in an effort to harvest credit card or other account information. Another important thing for the small business owner to realize is that not all attacks come from the outside. Many times an employee will purposely and sometimes even unintentionally compromise vital information [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

If a company's computer systems were attacked and down for a week it may lose a lot of business. Even worse it could lose all the vital data stored on the computers. The thief could sell the list of their customers along with sales figures to their biggest competitor. Attackers all have different motives, whether it be profit, mischievousness, or Internet glory; all is the same to the small business. Regardless of how or why one's business is attacked, fixing a compromised situation takes a lot of money, time, stress, and effort.

Here are some of the techniques used and simple definitions of each [5], [6], [13]:

Spam, or unsolicited commercial email messages, wastes bandwidth and time. The sheer volume of it can be overwhelming, and it can be a vehicle for viruses. Much of it is of an explicit sexual nature, which in some cases can create an uncomfortable work environment and, potentially, legal liabilities if companies do not take steps to stop it.

Phishing is increasingly becoming a tactic of choice for hackers and organized crime. Typically, an attacker sends an email message that looks very much like it comes from an official source (such as eBay or Microsoft). Links in the message take you to a website that also looks like the real thing. However, the site is just a front and the goal of the scam is to trick you into giving away personal information. The personal information received may be used for spam lists and for perpetrators to steal your account information or

even your identity. The victims of these scams are not only the users who may divulge personal and confidential information, but also the spoofed business' brand and reputation [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

Viruses are programs designed to replicate themselves and potentially cause harmful actions. They are often hidden inside innocuous programs. Viruses in email messages often masquerade as games or pictures and use beguiling subjects (for example, "My girlfriend nude") to encourage users to open and run them. Viruses try to replicate themselves by infecting other programs on your computer.

Worms are like viruses in that they try to replicate themselves, but they are often able to do so by sending out email messages themselves rather than simply infecting programs on a single computer.

Spyware refers to small, hidden programs that run on your computer and are used for everything from tracking your online activities to allowing intruders to monitor and access your computer. You might be the target of spyware or other unwanted software if you download music from file-sharing programs, free games from sites you don't trust, or other software from an unknown source.

Tampering consists of altering the contents of packets as they travel over the Internet or altering data on computer disks after a network has been penetrated. For example, an attacker might place a tap on a network line to intercept packets as they leave your establishment. The attacker could eavesdrop or alter the information as it leaves your network.

Information disclosure consists of the exposure of information to individuals who normally would not have access to it. For example, a user on your network might make certain files accessible over the network that should not be shared. Employees also tend to share important information, such as passwords, with people who should not have them.

DoS attacks are computerized assaults launched by an attacker in an attempt to overload or halt a network service, such as a Web server or a file server. For example, an attack may cause a server to become so busy attempting to respond that it ignores legitimate requests for connections.

Identity theft is considered "America's fastest growing crime problem" by the FBI and it affects more than ten million Americans each year. Small businesses are many of the victims as they send many important documents electronically and thru the mail. An identity thief can operate by looking through mailboxes, sifting through trash, stealing wallets/purses, breaching computer networks, or many other ways. It is important for small businesses to take measures to protect against identity theft. It can be devastating if not handled quickly and appropriately. The average loss of from Internet identity theft is $3,000. Besides possibly losing thousands of

dollars, an identity theft victim will on average spend over two hundred hours to reclaim their identity. If you are a victim of identity theft, it is important to respond quickly. Credit card companies will regard you less liable the earlier you report the theft. You can ask credit-reporting agencies to flag your report with a fraud alert so that no one is issued new credit under your name. You should also contact the police and file a report with them [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

Some companies engage in competitive intelligence, which is the practice of "gathering, analyzing, and applying information about products, domain constituents, customers, and competitors for the short term and long term planning needs of an organization". This practice keeps the company up to date on competing companies and the industry as a whole. There is a clear difference between this and industrial espionage. Reputable competitive intelligence professionals abide by laws and a code of ethics. One can legally and ethically gather information by examining public records or attending trade shows. Industrial espionage involves activities such as bugging, bribery, and blackmail. It is a bigger threat to businesses that are highly dependent on information [7].

Dumpster diving, or information diving, is the practice of recovering data that has been discarded. In earlier times it was possible to find sensitive documents on paper. However, after businesses became aware of this it was common to shred anything important that was thrown away. Recently, most sensitive information comes from data left on computers' hard drives. This can be memos, IDs, passwords, or anything else. Files are not completely removed from a hard drive until it needs to make room for other files. So even if the file is deleted and the Recycle Bin is cleared it is still possible to recover the file unless a program (or a powerful magnet) is used to completely wipe the hard drive. Besides getting rid of sensitive information on trashed computers, one should also take care when selling/donating [5].

There is a growing concern in the business world about data breaches. 10% of IT budgets will be spent on security this year, an increase from 8% last year. IT security professionals are enjoying greater influence. Unfortunately, over 80% of data breaches are caused by insiders. Almost 30% of companies are victim to at least five insider attacks per year. Being an insider makes the attack that much easier. The purpose of these attacks is to obtain research data, marketing statistics, HR records, and anything else that could be used or sold. There is software that allows administrators to limit the access of users which is a big help in preventing insider attacks [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

Firewalls protect not only the individual computer, but also the entire business network by preventing that malicious software from installing itself

or using the individual computer to spread the malware to others in the network. Often malware spreads through company intranets because of careless employee behavior. This can cause severe damage to the mainframes of the business. Firewalls help to prevent this [40], [41], [42], [43].

Physical security is very important, especially for small businesses. This category can be divided into passive and active protection. Any passive measurements such as CCTV or locks are usually very cost efficient. Installing a camera system that supervises the POS (Point-of-Sale) terminals is very effective in reminding customers as well as employees that somebody is watching over the business. Most passive methods are preventive. Every business owner knows its business and they should think about how to secure their assets. Business interruption can be extremely costly if not fatal for the business so every attempt to make the business run as smooth as possible should have a high priority [1], [4], [5], [6], [7], [8], [9], [10], [11], [12].

Anti-virus software is a must for every PC. Whether it is a business computer or a private machine it is absolutely essential that it is running up-to-date anti-virus software that protects the machine against circulating viruses. As a rule of thumb it can be said that from the point in time when a virus is recognized until it actually vanishes years can pass by since there are enough machines out there that run unprotected.

Anti-phishing filters should be used on browsers and email programs. In addition, the software employees must be trained in identifying phishing mails or at least be able to screen for these mails or programs. The lists of them are available online and they should be made public somewhere in the company in order for employees to be exposed to it on a frequent basis.

Corporate security events are an essential part in creating awareness among employees. In larger businesses, the owner or manager should consider hiring a third party to train staff about corporate security [35], [36], [37], [38], [39]. Also the use of online-based training can be very effective since they combine education and testing. These events (when paired with testing) provide the employee with a great incentive to take ownership for their workplace. Also, employees should be educated about maintaining an online profile and the possible consequences of having one [1], [4], [5], [6], [7], [8], [9], [10], [11], [12]. Online resources should be considered on a regular basis. A business owner's time is very expensive and so are losses. The owner should be aware of any industry specific threats and special security circumstances. A certain due diligence in information gathering and intelligence is necessary to make the business safe. Many online resources (often for a fee) are available to get this intelligence in one place.

Anti-social-engineering measurements should be taken by a business. Social engineering focuses on manipulating people to take advantage of them

through bribery, blackmail, extortion has been more and more popular in the recent years. Through technology it has become increasingly possible to gather information about a target that is free and publicly available. Companies must ensure that they protect their information and that suspicious activity of any kind is reported immediately to the respective authorities [32], [33], [34], [35], [36].

Despite what many might believe with the increase of security cameras and alarms theft has not dramatically decreased. As technology increases, so does the crook as they constantly try to stay one step ahead. It is particularly difficult for small businesses to protect themselves in the same way as larger firms usually because of the expenses of a great security system setup.

It is also very important to consider where you place your business. Even though some claim that operating in a high crime area gives you advantages over your competitors it also can lead to your downfall. In extremely high crime areas 30% of people will steal from you and 60% will if given an excellent opportunity. The state of Texas is currently ranked 45th in small business crimes committed. In 2006, Forbes named College Station 30th best small town to open a business for security [1], [4], [5], [6], [7], [8], [9], [10], [11], [12], [29], [30], [31].

It is critical that all small businesses try to prevent crimes as much as possible. Security systems can cost thousands of dollars, but they usually pay for themselves over time. All small businesses should do a detailed background check on employees before they hire them and research their business location. Also it is important to closely monitor the information you are allowing on the web and who is able to gain access to sensitive items. When the economy is in a downward spiral as it has been recently, people began to feel poorer and the chances for theft will significantly increase.

3. Conclusion

It is critical that all small businesses try to prevent crimes as much as possible. Security systems can cost thousands of dollars, but they usually pay for themselves over time. All small businesses should do a detailed background check on employees before they hire them and research their business location. Also it is important to closely monitor the information you are allowing on the web and who is able to gain access to sensitive items. When the economy is in a downward spiral as it has been recently, people began to feel poorer and the chances for theft will significantly increase.

REFERENCES:

1. Hristov, L., Hristov, Hr., Main features of the types of threats and attacks against the economic security of the corporation, A collection of scientific papers from the International Scientific Conference - „ European Union policy on data protection and personal data, “Vasil Levski” National Military University, Faculty of Artillery, AD and CIS, Information Security Department, Shumen 2018, ISBN 978-954-9681-89-5, стр. 73-77.
2. Cost of Data Breach Study. symantec.com. [Онлайн] (2018) http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-.en-us.pdf.
3. The Escalating Cost of Software Malice. HBR Blog Network. [Онлайн] http://blogs.hbr.org/2018/06/the-escalating-cost-of-softwar/.
4. Hristov, L., Stanev, St., Hristov, Hr., Tools for defensing the sensitive company information from insider threats, Conference proceedings - MATTEX 2018 Vol. 2, part 1, ISSN: 1314-3921, стр. 109-115.
5. Stanev, S., Zhelezov, S., Computer and network security, Shumen University, 2005, 182 p.
6. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Information Technology and Security” № 1(3) p. 79-86.
7. Станев, С. и Х. Христов. Роля на фирмените служби за сигурност при организиране на противодействие срещу стеганографски атаки. В: Сборник трудове на Годишна университетска научна конференция на НВУ "Васил Левски". В.Търново, 2013. стр.81-88.
8. Andreev A. Any aspects of security what concept. NMU- Shumen, Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.
9. Andreev A. The environment of security and influence national security and national interests. NMU- Shumen. Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.
10. Andreeva G., Andreev A. Survey and analysis of intercultural communication in Bulgaria and abroad. Journal "Scientific and applied research", USA, vol.3, p.89-97, 2013.
11. Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, Vol.3, 2013, pp. 114-124, available at: http://www.rst-tto.com/publication.html.
12. Boyanov, P., Educational exploiting the information resources and invading the security mechanisms of the operating system windows 7 with the exploit Eternalblue and Backdoor Doublepulsar, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 14, 2018, pp. 34-41, available at: http://www.rst-tto.com/publication.html.
13. Griffith, Eric. "The Best Free Software of 2010." (2008).
14. Ivanov, M., Intelligence Infrastructure, Sofia, Profisec, 2012, p. 215, ISBN 978-954-32927-1-8.
15. Ivanov, M., Nazism and Islam, MATTECH 2018, Shumen, St. Konstantin Preslavsky University Publishing House, 2018, ISBN 1314-3921.

16. Ivanov, M., Army and Police - Diffusion of Functions and Tasks, Fourth National Conference with International Participation "Metal Science, Hydro- and Aerodynamics and National Security 2014", Sofia, 2014, ISBN 1313-8308.
17. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
18. Савов, И., Един поглед върху същността на киберпрестъпленията, списание „Политика и сигурност", ВУСИ, 2017, ISSN 2535-0358, с. 36-47.
19. Савов, И., Един поглед върху противодействието на хибридните заплахи в Европейския съюз, международна конференция „Асиметрични заплахи, хибридни войни и влиянието им върху националната сигурност", Нов Български университет, март 2018 г., ISBN 978-619-7383-09-6, с. 179-185.
20. Христов, Х., Солаков, Т., Процеси на реислямизация сред мюсюлманската общност и провеждана малцинствена политика в Република България, Юридически сборник на Бургаски свободен университет, Център по юридически науки, том XXV -2018, ISSN 1311-377, гр. Бургас, България, 2018 год., с. 105 -114.
21. Христов, Х., Солаков, Т., Различия между ислямски радикализъм и турски рационализъм. Причини, довели до разделението на мюфтийството, Юридически сборник на Бургаски свободен университет, Център по юридически науки, том XXV -2018, ISSN 1311-377, гр. Бургас, България, 2018 год., с. 114 -123.
22. Солаков, Т., Христов, Х., Мюсюлманската общност в Република България, Сборник доклади от Годишна Университетска Научна Конференция, Национален военен университет „Васил Левски", гр. В. Търново, България, ISBN 978-619-7246-20-9 (online e-book), 14-15 Юни 2018, с. 621-630.
23. Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Русе, 2017, с.19-27, http://jei.uni-ruse.bg/Issue-2016/02.%20Zagorcheva%20-%20Pavlov.pdf.
24. Zagorcheva, D., Stages in the systems for financial management and control in the Bulgaria's public sector, The XIV International Scientific Conference Information Technologies and Management, 2016, Riga, Latvia.
25. Загорчева, Д, Велчева, Й., Бюджетната децентрализация като фактор за едновременно развитие на общините и индустриалния бизнес, Народностопански архив, година LXX, книга 3 – 2017, ISSN 0323-9004, стр. p.46-59, https://www.uni-svishtov.bg/NSArhiv/title.asp?title=981.
26. Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6 (available at: http://varepsilon.com/), indexed in Russian Science Citation Index, (РИНЦ: Научная электронная библиотека eLIBRARY.RU), ВИНИТИ РАН Электронный каталог научно-технической литературы VINITI.RU, National Centre for Information and Documentation (Bulgaria), Google Scholar, OpenAIRE, Polish Scholarly Bibliography (PBN), Index Copernicus International, ROAD, the Directory of Open Access scholarly Resources, DOAJ, Directory of Open Access Journals.
27. Hristov, Hr., Development of warfare and counter-terrorism. Journal Science Education Innovation, ISSN 1314-9784, vol. 3. 2014, pp. 104-111.

28. Hristov, Hr., A modern survey on problems of business organization's security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.
29. Velikov, I., Humanitarian aspects of protection of information, MATTEX 2018 Conference proceedings, Konstantin Preslavsky University of Shumen, ISSN 1314-3921, Shumen, Vol. 2, part 1, 2018, pp. 3-10.
30. Досев, Н., Създаване на склад от данни за определяне на риска за информационната сигурност на корпорацията, Научна конференция с международно участие на тема „Киберсигурността в информационното общество", Факултет "А, ПВО и КИС", Шумен 2017 г.
31. Досев, Н., Създаване на модел на система за ранно предвиждане рисковете за информационната сигурност на корпорацията, Научна конференция MATTEX на ШУ „Еп. К. Преславски", гр. Шумен, 2016 г.
32. Досев, Н., Обезпечаване сигурността на достъпа до интегриран склад от данни, Международна научна конференция 2016, Факултет „А, ПВО и КИС" гр. Шумен, 2016.
33. Добрев, Д., Европа – философия и политика. Издателство „Просвета-София", ISBN 978-954-01-3785-8, 2018 г.
34. Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.
35. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security" № 1(3)-2013 УДК 004 (056.5+413.5).
36. О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA", Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски", 2015г.
37. Василева, Р., Русева, В., Корупцията в сферата на държавната администрация, Сборник научни трудове от научна конференция с международно участие „MATTEX 2018", ШУ "Епископ Константин Преславски", 25-27 октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
38. Василева, Р., Русева, В., „Корупцията - обществен феномен в България", Сборник научни трудове от научна конференция с международно участие „MATTEX 2018", ШУ "Епископ Константин Преславски", 25-27октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
39. Василева, Р., Анализ на органите и структурата на местното самоуправление", Годишната университетска научна конференция, 14-15 юни 2018 г., гр. Велико Търново, ISSN:1314-1937 (print), 2367-7481 (online).
40. Dimitrova, N., 2014: The motivation for effective study of technical and technological information assimilation. International Scientific Online Journal – ISSN 2367-5721 Issue 4, December 2014, www.sociobrains.com, pp 94-99.
41. Dimitrova, N., 2015: Operationalize the aims of technological education International Scientific Online Journal. Issue 16, December 2015, www.sociobrains.com pp. 48 – 53.
42. Dimitrova, N., 2014: Role of informatization in technological education and information culture of students International Scientific Online Journal, Issue 2, October 2014, www.sociobrains.com pp. 26-30.

43. Димитрова, Н. Приносът на технологичното обучение за съхраняване на българските национални традиции. – Годишник на Шуменския университет „Епископ Константин Преславски”, Т. XX D, Научни трудове от конференция „Иновации в образованието”, 30 септември – 02 октомври 2016, Педагогически факултет, Шумен, Епископ Константин Преславски, 2016, 686 – 690.

Author's name: Marta D. Kovacheva, PhD student
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems“
E-mail: martakova4eva@gmail.com

COUNTERMEASURES AGAINST VARIOUS TYPES OF CYBER ATTACKS IN THE CONTEXT OF THE PROTECTION OF THE NATIONAL SECURITY OF REPUBLIC OF BULGARIA

Petar Kr. Boyanov

ABSTRACT: *In this paper a countermeasures against various types of cyber attacks in the context of the protection of the national security of Bulgaria is made.*

KEYWORDS: *Countermeasure, Hybrid firewalls, IDS, Cyber security, Vulnerability.*

1. Introduction

With the help of modern types of malicious software tools, cybercriminals are able to get information about the credit card number, the secret code of the credit card in order to defraud the victim's financial resources. In this way, there is an acute need to protect the transmitted information between the electronic devices [1], [2], [4], [7], [10], [11], [12].

For this reason, the security officers of the Automated Information Systems and Networks, the AIS/N Security Administrator and AIS/N users, analysts and information security researchers have to find ways, means and solutions for detecting and protecting against modern cyber-attacks. Cyber criminals are in fact highly erudite and smart developers who know in detail all the weak and strong places of old and new standards of data transmission and data protection [3], [5], [6], [8], [9], [13], [14], [15], [17], [18], [20].

The main task of AIS/N security officers and security administrators is to use penetration detection systems, firewalls, and honeypots, which are software programs and hardware devices, which have the task of detecting, analyzing and blocking the various types of malicious cyber attacks.

2. Main features of firewalls

The firewall is a complex software system or a set of software systems that need to strictly control, scan, and monitor all access policy resources for AIS/N and ASI staff on the computer machine of an employee of the organization [22], [23], [24]. From the point of view of information security, all software firewalls are characterized by the following features [16], [19], [21]:

- Software firewalls must detect and reject various types of malicious cyber attacks.
- Firewalls should act as a transit point for Linux-based operating systems in the chain (FORWARD) between local computer networks, thus all network traffic passes through them.
- Firewalls control and monitor access policies on the appropriate local computer network.

The best firewalls are built on UNIX or Linux-based operating systems. Always the Linux operating system has higher and bigger features in order to play the role of a software firewall than Windows-based operating systems [46], [47], [48], [49].

The main types of firewalls that are used by security officers on automated information systems and networks (AIS/N) and security administrators are [25], [26], [27], [28], [29], [30] ,[31], [32], [33], [34], [35]:

- Firewall with packet filtration [15], [36]. In most cases, the firewall is embedded in a router that has the task of filtering the contents of most of the network and transport layer packages from the Open System Interconnection (OSI) communications model [37].
- Dynamic firewall with full inspection [38], [39]. This firewall monitors the status of network connections by establishing when the connection is initialization, ending, or a data connection. This firewall filters and controls the information in network, transport, and session layer packets.
- Firewall with enclosed gate (Proxy Filtration Firewall) [10], [11], [12]. This firewall filters the information in network, transport, session, and application layer packets. In most cases, this firewall is implemented by software.
- Hybrid firewall, which is a collection of the above-mentioned firewalls, which means it is best performance solution against all kinds of cyber attacks. It is very important that the security administrator must be extremely and highly qualified to be able to build it.

3. Intrusion detection systems IDS

Intrusion Detection Systems (IDS) may be software or hardware devices that are programmed in such a way that security officers of automated information systems and networks as well as security administrators can detect events that can damage the processes of the operating system, detect anomalies in user actions and system services, and detect anomalies in the operation of the TCP/IP network protocol stack that is

firmly encrypted in the network map on the computer machine of the employee of the organization.

The IDS systems have a special database with all computer viruses, worms, back doors, Trojans hitherto discovered. They have a separate database that analyzes abnormalities in the SYN, ACK, URG, PSH, FIN, and RST bits for detecting network scanners and analyzers [38], [39], [40], [41], [42], [43], [44], [45].

The main types of intrusion detection systems that can be used by automated information systems and network security officers as well as security administrators are:

- Network-based IDS systems, which are generally the black boxes of the aircraft and are intended to alert the user if a network scanning is implemented.
- Host-based IDS systems deal with the local monitoring and analysis of system services and processes. If an anomaly in some of them is found, then the user is immediately alerted that he has been compromised by the cyber-attacker.
- IDS logging systems are used to monitor and track all recorded logs and based on them to alert the user whether the computer machine has been a victim of the cyber attack. Logs are all recorded events and actions that have occurred in the computer machine for a certain period of time.
- Files integrity IDS systems are systems that track all executable and non-executable files for modifications or changes to them due to Trojan horse, backdoor, computer virus, etc. One of the best software IDS systems that checks for changes to files is Tripwire.

3. Conclusion

Most state institutions and private companies must pay extraordinary attention to protection from modern cyber attacks. It is highly recommended to employ highly trained specialists in public and private organizations to ensure the security of the information transmitted between people and communication devices.

The training of information security students will acquire lasting habits in their future practice of coping with various types of malicious cyber attacks.

Security officers of automated information systems and networks, as well as security administrators, should exercise very strict control over the management of software security policies. It is desirable even to appoint certified cyber-attackers to conduct regular tests to check emerging new vulnerabilities or weaknesses in operating systems used by employees.

REFERENCES:

1. Alosefer, Yaser, and Omer Rana. "Honeyware: a web-based low interaction client honeypot." In Software Testing, Verification, and Validation Workshops (ICSTW), 2010 Third International Conference on, pp. 410-417. IEEE, 2010.
2. Beblavý, Miroslav, and Lucia Mýtna Kureková. "Into the First League: The Competitive Advantage of the Antivirus Industry in the Czech Republic and Slovakia." Competition & Change 18, no. 5 (2014): 421-437.
3. David, R. "Top 5 Free Antivirus for Mac: Reviews." (2013).
4. Filiol, Eric, Grégoire Jacob, and Mickaël Le Liard. "Evaluation methodology and theoretical model for antiviral behavioural detection strategies." Journal in Computer Virology 3, no. 1 (2007): 23-37.
5. Griffith, Eric. "The Best Free Software of 2010." (2008).
6. Hamlen, Kevin W., Vishwath Mohan, Mohammad M. Masud, Latifur Khan, and Bhavani Thuraisingham. "Exploiting an antivirus interface." Computer Standards & Interfaces 31, no. 6 (2009): 1182-1189.
7. Hessman, Kristy. "Pitfalls of Free Antivirus Software." (2011).
8. Heu, Kimberly. "Security of Client PCs." (2009).
9. James, K. L. The Internet: A user's guide. PHI Learning Pvt. Ltd., 2010.
10. Kryvenko, P., Computer viruses and anti-virus programs, 2013.
11. Marx, Andreas. "Antivirus outbreak response testing and impact." Virus Bulletin (2004).
12. Morgenstern, Maik, and Andreas Marx. "Runtime packer testing experiences." In 2nd International CARO Workshop. 2008.
13. Stoyanov, B. P., Kordov, K. M., Pseudorandom Bit Generator with Parallel Implementation (2014), Large Scale Scientific Computing 2013, Lecture Notes in Computer Science 8353, 557-564, SJR(2013)=0.310
14. Sukwong, Orathai, Hyong S. Kim, and James C. Hoe. "Commercial antivirus software effectiveness: an empirical study." Computer 44, no. 3 (2011): 0063-70.
15. Xue, Feng. "Attacking antivirus." In Black Hat Europe Conference. 2008.
16. Velikov, I., Humanitarian aspects of protection of information, MATTEX 2018 Conference proceedings, Konstantin Preslavsky University of Shumen, ISSN 1314-3921, Shumen, Vol. 2, part 1, 2018, pp. 3-10.
17. Zhelezov, S., H. Paraskevov, Possibilities for steganographic parallel processing with a cluster system, Contemporary Engineering Sciences, Volume 8, Issue 20, ISSN:1313-6569, 2015, SJR (2014) : 0.187.
18. Andreev A. The environment of security and influence national security and national interests. NMU- Shumen. Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.
19. Andreev A., Geo-information technologies for modeling of security disaster. Collection of scientific works, MATTEX Shumen's university "Bishop K. Preslavski "2012.
20. Andreeva I., Andreeva G., Andreev A. Conceptual models of retirement and promotion employment of older people in Bulgaria. Journal "Science, education, innovation", USA, vol.1, p.137-143, 2013.
21. Ivanov, M., Intelligence Infrastructure, Sofia, Profisec, 2012, p. 215, ISBN 978-954-32927-1-8.

22. Ivanov, M., Army and Police - Diffusion of Functions and Tasks, Fourth National Conference with International Participation "Metal Science, Hydro- and Aerodynamics and National Security 2014", Sofia, 2014, ISBN 1313-8308.
23. Савов, И., Един поглед върху противодействието на хибридните заплахи в Европейския съюз, международна конференция „Асиметрични заплахи, хибридни войни и влиянието им върху националната сигурност", Нов Български университет, март 2018 г., ISBN 978-619-7383-09-6, с. 179-185.
24. Савов, И., Рискове и заплахи за сигурността в Черноморския регион, Международна конференция „Проблеми на сигурността в черноморския регион", ВУСИ, септември 2017 г., ISBN 978-619-7343-09-0, с. 7-18.
25. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
26. Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Pyce, 2017, c.19-27, http://jei.uni-ruse.bg/Issue-2016/02.%20Zagorcheva%20-%20Pavlov.pdf.
27. Zagorcheva, D., Stages in the systems for financial management and control in the Bulgaria's public sector, The XIV International Scientific Conference Information Technologies and Management, 2016, Riga, Latvia.
28. Загорчева, Д, Велчева, Й., Бюджетната децентрализация като фактор за едновременно развитие на общините и индустриалния бизнес, Народностопански архив, година LXX, книга 3 – 2017, ISSN 0323-9004, стр. p.46-59, https://www.uni-svishtov.bg/NSArhiv/title.asp?title=981.
29. Solakov, T., The Bulgarian state and the religious organizations in the period after 1989, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press", ISSN 1311-834X, Vol. VI E, 2017, pp. 107-119.
30. Solakov, T., Religious fundamentalism and extremism, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press", ISSN 1311-834X, Vol. VI E, 2017, pp. 120-132.
31. Solakov, T., Radicalism and stages of radicalization, Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Konstantin Preslavsky University Press", ISSN 1311-834X, Vol. VI E, 2017, pp. 133-140.
32. Hristov, Hr., Development of warfare and counter-terrorism. Journal Science Education Innovation, ISSN 1314-9784, vol. 3. 2014, pp. 104-111.
33. Hristov, Hr., A modern survey on problems of business organization's security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.
34. Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6 (available at: http://varepsilon.com/), indexed in Russian Science Citation Index, (РИНЦ: Научная электронная библиотека eLIBRARY.RU), ВИНИТИ РАН Электронный каталог научно-технической литературы VINITI.RU, National Centre for Information and Documentation (Bulgaria), Google Scholar, OpenAIRE, Polish Scholarly Bibliography (PBN), Index Copernicus International, ROAD, the Directory of Open Access scholarly Resources, DOAJ, Directory of Open Access Journals.

35. Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.
36. Досев, Н., Създаване на склад от данни за определяне на риска за информационната сигурност на корпорацията, Научна конференция с международно участие на тема „Киберсигурността в информационното общество", Факултет "А, ПВО и КИС", Шумен 2017 г.
37. Досев, Н., Създаване на модел на система за ранно предвиждане рисковете за информационната сигурност на корпорацията, Научна конференция МАТТЕХ на ШУ „Еп. К. Преславски", гр. Шумен, 2016 г.
38. Досев, Н., Обезпечаване сигурността на достъпа до интегриран склад от данни, Международна научна конференция 2016, Факултет „А, ПВО и КИС" гр. Шумен, 2016.
39. Добрев, Д., Европа – философия и политика. Издателство „Просвета-София", ISBN 978-954-01-3785-8, 2018 г.
40. Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.
41. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security" № 1(3)-2013 УДК 004 (056.5+413.5).
42. О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA", Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски", 2015г.
43. Василева, Р., Русева, В., Корупцията в сферата на държавната администрация, Сборник научни трудове от научна конференция с международно участие „МАТТЕХ 2018", ШУ "Епископ Константин Преславски", 25-27 октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
44. Василева, Р., Русева, В., „Корупцията - обществен феномен в България", Сборник научни трудове от научна конференция с международно участие „МАТТЕХ 2018", ШУ "Епископ Константин Преславски", 25-27октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
45. Василева, Р., Анализ на органите и структурата на местното самоуправление", Годишната университетска научна конференция, 14-15 юни 2018 г., гр. Велико Търново, ISSN:1314-1937 (print), 2367-7481 (online).
46. Dimitrova, N., 2014: The motivation for effective study of technical and technological information assimilation. International Scientific Online Journal – ISSN 2367-5721 Issue 4, December 2014, www.sociobrains.com, pp 94-99.
47. Dimitrova, N., 2015: Operationalize the aims of technological education International Scientific Online Journal. Issue 16, December 2015, www.sociobrains.com pp. 48 – 53.
48. Dimitrova, N., 2014: Role of informatization in technological education and information culture of students International Scientific Online Journal, Issue 2, October 2014, www.sociobrains.com pp. 26-30.
49. Димитрова, Н. Приносът на технологичното обучение за съхраняване на българските национални традиции. – Годишник на Шуменския университет „Епископ Константин Преславски", Т. XX D, Научни трудове от конференция

„Иновации в образованието”, 30 септември – 02 октомври 2016, Педагогически факултет, Шумен, Епископ Константин Преславски, 2016, 686 – 690.

Author's name: assoc. prof. eng. Petar Boyanov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems“
E-mail: peshoaikido@abv.bg, peshoaikido@gmail.com

PROFINET – DIGITAL TRANSFORMATION FOR INDUSTRIAL AUTOMATION

Plamen L. Ribarski

ABSTRACT: *In this work, an analysis has been made regarding one of the fairly new communicative standards – PROFINET (IEC 61158) which significantly widens the functional abilities of data exchange and agrees with a wide specter of requirements regarding the use of internet networks for automation of production. The different mechanisms of connection between the modules and the different instrumental means for projection and automation of production have been reviewed with respect of the technical function of the PROFINET networks. Also noted are the network components of the system, the communication and software security, the investment attraction and other system indicators by providing a concise comparison with similar systems.*

KEYWORDS*: Profinet, industrial, communication, systems, internet.*

1. Introduction

The beginning of Profinet dates back to more than fourteen years ago. Profinet deals with installation technologies, real-time communication, network management and Web integration functions. To this day, Profinet is under fierce development and is being heavily implemented to the market as a favorite in the "Industrial Internet Communications" field [1], [2], [3], [4], [5], [6], [7], [8].

This technology has been developed by the Siemens Corporation and the company-members of the consumer organization of PROFIBUS (PNO). Profinet targets the organization of data exchange among all hierarchical management levels of the company. It makes the design of the industrial communicative systems significantly more simple, widens the usage of IT standards up to management level, permits the usage of already existing communicative channels and network components of Ethernet while also completes these networks with specialized components. Profinet provides support for all existing standard mechanisms for data exchange through Ethernet alongside data exchange between automated systems in real time [2].

Profinet's popularity still hasn't dealt with all the problems with regards to its practical application. With its flexibility, Profinet, while it severely surpasses the already established field communication systems, it also lags behind in some specific cases, mainly regarding work in real time.

2. How it works

Profinet represents a standard which deals with all the tasks with regards to the usage of the massively popular Ethernet in industrial communications. It covers the communication on lower level between controllers and sensors, communication on controller level, it is also used in managing real-time operations. Profinet allows direct access to already distributed field devices by the Ethernet network. All of the devices that are taking part in the automated process are connected in a unified network structure, which leads to a standard communication spreading through the whole production [1], [2], [3], [4], [5], [6], [7], [8]..

In order to maintain different classes of efficiency, PROFINET uses the principle of "producer/consumer" with different protocols and services. High priority useful information is transmitted directly through the Ethernet protocol in Ethernet borders with VLAN priority, and diagnose and configuration data is being transmitted through UDP/IP. This allows the system to achieve around 10ms for a cycle for I/O applications. PROFINET IRT offers cycles with synchronizing period of less than 1ms as it is required by the applications for movement management. This is done by using the multiplexing of time mode which is based on particularly controlled hardware-synchronized switches [4]. In the coming future, by using the so called DFP (Dynamic Frame Packing), consumers will get a new version of PROFINET with optimized cycle time, thanks to the application of the principle of the overall border to an exact set of network devices [1], [2], [3], [4], [5], [6], [7], [8].

The construction of an industrial Ethernet network differs from that of an office communications one since the choice of topology depends on the requirements of a certain application and the conditions for device placement. In practice, the networks can be used on copper couples as well as on optical fibers, from combinations of typical topologies: ring, tree, and linear (Fig. 1).

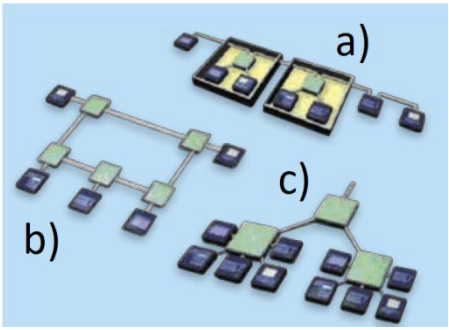

Fig.1. Topology of Profinet a) linear; b) ring; c) tree.

In case of linear structure, the commutator is closely connected to the device or it is installed in the terminal itself. In fact, every device has its own switch. This type of communication is appropriate for conveyor control, the connecting of independent production segments, etc. The ring structure is similar to the linear, but it is more reliable and less error prone. The end of the communicative line is connected in such way that in case of interruption the network will remain in exploitation. If the switch is connected to all network terminals simultaneously, for example in places where the density of such devices is high, the topology of a star is used. The tree structure can be made out of a few such networks which are usually used for combining of subsystems of complex machinery. In regards with constructing the PROFINET network, the client, depending on certain working conditions, prefers the traditional for the topology of "IT solutions" ("star") or the linear structures of PROFIBUS systems [1], [2], [3], [4], [5], [6], [7], [8]..

The peculiarities of wiring cables in industrial conditions are directly connected with specific equipment. The cables can be put under some serious stress. For data transmission, PROFINET uses two twisted copper couples (shielded, only!) with a 100 Ohm resistance. They correspond to Ethernet 100 Base TX and provide speed of up to 100 Mbps. Cables lower than 5th category and Class D, standardized under ISO/IEC11801-Information technology, are not allowed. The architecture of PROFINET allows the maximum length of the cable to be 100m. Both ends of the cable should be provided with connectors. PROFINET suggests the usage of removable ones, like RJ45 or M12. Every distant device is connected through the active network component. Like that, the data transmission cable is defined the same way as on the side of the device or its controller. In case where the device uses the connection not only for data transfer, but also for energy consumption (24V) a hybrid cable is used which contains four copper wires, for a charger and for data transmission – either two optic cables or four shielded copper cables. Also, PROFINET supports multimode mode of optic connections with a speed of 100 Mbit/s. The devices' interfaces correspond to ISO/IEC9314-3 и ISO/IEC 9314-3. This way, a greater network reception is achieved, in comparison with symmetric copper cables. The electromagnetic resistance grows higher, too. In order to be used outside of the distributive cabinets and channels, the optic cables have to correspond with the conditions (chemical, mechanical, temperature) in the particular network zone (Table 1) [6].

Table 1.

Characteristics	Inside	Outside
Field of application	Tracking systems, switching systems, management systems	Production (lerar systems, on/off systems, portable equipment)
Anti-pollution defense rate	IEC 625-1 rate 2 (VDE 0110)	IEC 625-1 rate 3 (VDE 0110)
Defense rate	IP20	IP6/IP675
Impact impingement	IEC 60512-4, test 6c, 20g/11ms, 3 axes in each direction	IEC 60512-4, test 6c, 20g/11ms, 3 axes in each direction
Vibrations 10-500GHz	IEC 60512-4, тест 6d 0,35 мм при 5g	IEC 60512-4, тест 6d 0,35 мм при 5g
Temperature range	0^0...60^0	-20^0…70^0

3.Architecture

In order to achieve optimal support for different practical applications and tasks, PROFINET suggests two main possibilities [1], [2], [3], [4], [5], [6], [7], [8].:

- Profinet IO for the construction of distributed input/output peripherals.

- Profinet CBA for the creating of a distributed modular automation for factories;

In the Profinet IO systems the devices are connected directly to Industrial Ethernet and are being serviced by a I/O S7-200-300 PROFINET controller. The high-speed data transfer is of a cyclic character and works with a speed of 100 Mbit/s. Depending on the components used in such network, real time (RT) data transfer and the use of clock synchronization (Isochro-nous RT - IRT) are supported. At the same time, the switch family SCALANCE X100 / 200 / X300 / X400 can be used as active network components supporting the RT mode, and only the family switches SCALANCE X200IRT / XF200IRT can support the IRT mode. The possibility of integrating already existing PROFIBUS DP networks in the PROFINET IO systems is also supported. In the meantime, the main device is connected to the PROFINET network and communicates with the PROFIBUS DP subordinates through a PROFINET Proxy. In the distributed emergency response for security and safety systems (F-systems), based on PROFINET for data transfer between the F-system components, PROFIsafe profile support is provided (Fig. 2).

The CBA technology is designed to simplify the organization of industrial communication through PROFINET among the equipment of different manufacturers. In this case, the operations of labor-intensive programming of communicative systems are substituted by the graphical design operations of such systems. The main productive module in the quality analyzing systems is a technological component representing all the mechanical, electrical, and electronic parts of a certain machine or

installation, as well as the respective software for applications. A software module is assigned to every technological component, which contains a full description of the interface of the said component in accordance to the requirements of the PROFINET standard [1]. In the future, those software modules are to be used for the projection of communicative connections. An example of architecture of PROFINET CBA is presented in fig. 3.

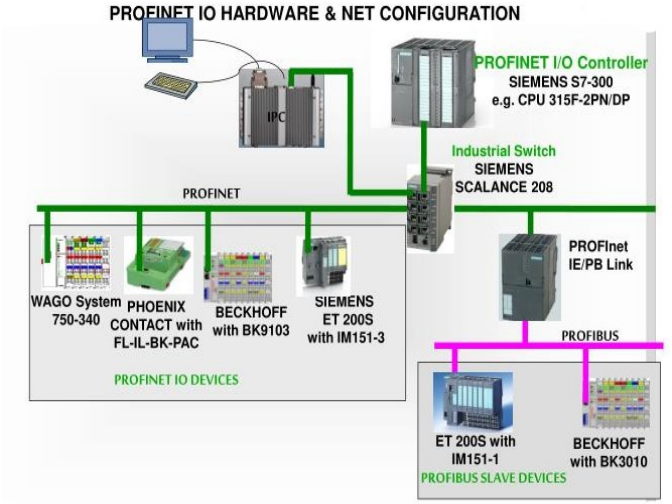

Fig.2. An example configuration of a PROFINET IO system

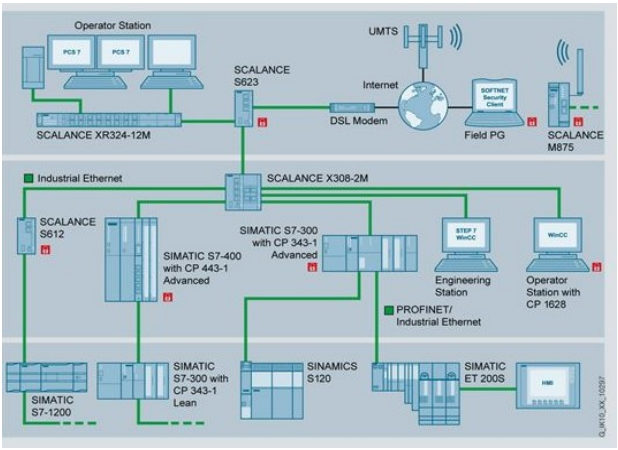

Fig.3.

The programming of the risk analyzing systems is done in three stages [1], [2], [3], [4], [5], [6], [7], [8].:

- Hardware configuration and development of the application software of the module for processing in the instrumental conditions of the respective manufacturer. At this stage, the SIMATIC components based systems, the STEP 7 pack can be used (LAD, FBD, STL), as well as the whole spectrum of instruments for projection (S7-GRAPH, S7-SCL, CFC, etc.).
- Creating software modules of technological components, while the tools of the respective manufacturer are used, and are saved under XML format files. At this stage, the STEP 7 pack is being used for the SIMATIC components based systems.
- Loading the XML files (including those of different manufacturers) in PROFINET's visual editorial library and graphic design of the communication connections. SIEMENS offers the usage of the SIMATIC iMAP pack for this purpose.

After the said work is done, SIMATIC iMAP automatically generates all the data needed in order for a connection to be organized. In the same time, it is possible for operations for interactive testing and diagnosing of all components to be done without having any effect over the application of the different technological components [1], [2], [3], [4], [5], [6], [7], [8].

Being used as a part of the PROFINEN CBA systems are:

• PROFINET stations whose' functions can be performed by the whole equipment described for the I/O PROFINET controllers. Meanwhile, the computers with Ethernet interface have to be equipped with PN CBA OPC server software.

• PROFINET CBA proxy like CPU 31x-2 PN / DP и CPU 31xF-2 PN / DP

• PROFIBUS DP network equipment:

- ET 200S stations with intelligent IM151-7 CPU / IM151-7 F-CPU / IM151 PN interface modules, ET200PRO stations with intelligent IM154-8 CPU interface modules;

- S7-300 / S7-300C centralized processors with built-in PROFIBUS DP interface working under the DP subordinate device mode;

• Visualization systems (WinCC, WinCC flexible) supporting OPC clients' functions and access to PROFINET component data through PROFINET OPC server.

4. Short analysis

Today, there are over 30 different types of industrial internet systems, with each and every one having its ups and downs. One of the main disadvantages of the Industrial Internet communication systems, and especially of Profinet, is the slow start-up of the smart devices when the power fails. It takes seconds for Profinet to start working in a normal working mode, whereas the already established standard field communication systems like Profibus, Powerlink, EtherCAT, and SERCOS III, for example, have a start-up time of up to 100ms. Profinet's manufacturing costs are relatively high due to the usage of Scalance X300/400 high-end commutators and IM 154 controllers [1], [2], [3], [4], [5], [6], [7], [8].

EtherCAT and SERCOS III networks always form a logical ring. This ring can physically isolate the main device in case of network breakdown through feedback from the last knot of the physical line. EtherCAT allows branching-out of the lines using special knots and such branches are placed along the whole system, i.e. the network makes a logical ring. Only the POWERLINK construction provides backup main device and cable which is realized in real projects. For PROFINET and EtherNet this is only possible with the use of special commutators. Due to the specifics of the construction of the systems, the direct comparison of their performance is impossible [1], [2], [3], [4], [5], [6], [7], [8]..

3. Conclusion

The slow start-up of Profinet devices can be corrected by configuring the ones that have the interface for management of asynchronous messages under overloaded commutators and that support the fast start-up function (FSU). Commutators from the Scalance X200 series have a configuration interface which means that certain configuration options might be able to affect the transfer time of asynchronous messages, the cheap and practical IM 151 controllers with ET 200 interface are also suitable for the job. With such functionality, the start-up time is reduced from a few seconds to 500 ms which is a considerable amount. Being built this way, the whole system has two main advantages – faster start-up and significantly lower manufacturing costs. It needs to be examined which options would affect the preliminary records with the loading of timely-noncritical data, which will be an object of the author's next workings.

REFERENCES:

1. Keseev V. Profinet IO – advantages, disadvantages and solutions. Research papers at Rousse University, Rousse, Rousse University, 2011.
2. Raimond P., Metter M. Automating with Profinet. Erlangen: Publicis Corporate Publishing, 2006.

3. Tsankov Ts. Network administration. E-learning platform, http://cdo.shu.bg/ (in Bulgarian), Shumen, 2013.
4. http://www.automation.siemens.com/
5. http://www.ethernet-powerlink.org/
6. https://www.siemens.com/ru/ru/home.html
7. Andreev A., Markov M. Geographic information systems. NMU-Shumen, 2009, ISBN: 978-954-9681-46-8, p. 189.
8. Andreev A., Markov M. Guide to exercises in geographical information systems. NMU-Shumen, 2009, ISBN: 978-954-9681-47-5, 222 p.

Author's name: Plamen L. Ribarski, PhD student
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences

USE IN INTERNET OF PROTOCOLS TRANSPORT LAYER SECURITY AND ITS NOW-DEPRECATED PREDECESSOR SECURE SOCKETS LAYER

Daniel R. Denev, Tsvetoslav St. Tsankov

ABSTRACT: *The subject of the study shows us how to use protocols on the Internet. The following protocols will be analyzed for the forthcoming report: Transport Security (TLS) And Secure Sockets Layer (SSL)*

KEYWORDS*: TLS, SSL.*

1. Introduction

Internet Protocol (IP) is the communication protocol that is the foundation of the Internet. The purpose of the protocol is to allow addressing of the information sent over the network. Each host on the network is given a unique address (called IP address). When sending information over the network, it is divided into small packages called IP packets. Each header is attached to the header, which contains the sender's and recipient's IP address and other service data. With the help of these addresses, the computers through which the package passes decide what to do with it. The protocol does not guarantee the secure arrival of the information and there is no error correction. IP is used by transport protocols like TCP and UDP [1], [2], [3].

2. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

2.1 Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) was the most widely deployed cryptographic protocol to provide security over internet communications before it was preceded by TLS (Transport Layer Security) in 1999. Despite the deprecation of the SSL protocol and the adoption of TLS in its place, most people still refer to this type of technology as ‘SSL’.

SSL provides a secure channel between two machines or devices operating over the internet or an internal network. One common example is when SSL is used to secure communication between a web browser and a web server. This turns a website's address from HTTP to HTTPS, the ‘S’ standing for ‘secure’. On Fig. 1 is shown the HTTPS websites [1], [2], [3].

Fig.1. HTTPS Web site

2.2 Transport Layer Security (TLS) and its current Secure Sockets Layer (SSL) predecessor are cryptographic protocols designed to provide communication security over a computer network. Several versions of the protocols are widely used in applications such as web browsing, email, instant messaging, and VoIP. Websites can use TLS to provide all communications between servers and Web browsers.

The TLS protocol is primarily intended to ensure privacy of data and data between two or more communications computer applications. When TLS is provided, links between a client (such as a web browser) and a server have one or more of the following properties [1], [2], [3]:

• The connection is private (or secure) because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret that was negotiated at the start of the session . The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted .The negotiation of a shared secret is both secure (the negotiated secret is unavailable to eavesdroppers and cannot be obtained, even by an attacker who places themselves in the middle of the connection) and reliable (no attacker can modify the communications during the negotiation without being detected).

• The identity of the communicating parties can be authenticated using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).

• The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

TLS supports many different methods for exchanging keys, encrypting data, and authenticating message integrity. As a result, secure configuration of TLS involves many configurable parameters, and not all

choices provide all of the privacy-related properties. Attempts have been made to subvert aspects of the communications security that TLS seeks to provide, and the protocol has been revised several times to address these security threats. Developers of web browsers have also revised their products to defend against potential security weaknesses after these were discovered. The TLS protocol comprises two layers [1], [2], [3]:

- TLS record
- TLS handshake protocols.

TLS is a proposed Internet Engineering Task Force (IETF) standard, first defined in 1999 and updated in RFC 5246 (August 2008) and RFC 6176(March 2011). It builds on the earlier SSL specifications (1994, 1995, 1996) developed by Netscape Communications for adding the HTTPS protocol to their Navigator web browser. Figure 2 shows changes in protocols and standards over time. As a NOTE, it can be added that SSL 1.0 was formally never released due to multiple errors.

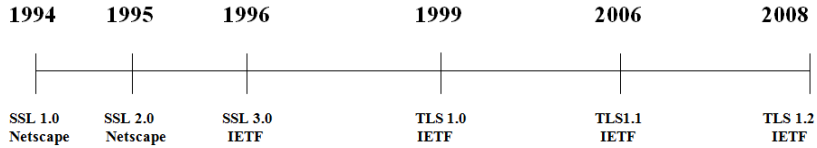

Fig.2. Changes in protocols and standards over time

3. TLS/SSL Architecture

The TLS/SSL security protocol is layered between the application protocol layer and the TCP/IP layer, where it can secure and send application data to the transport layer. Because it works between the application layer and the transport layer, TLS/SSL can support multiple application layer protocols.

TLS/SSL assumes that a connection-oriented transport, typically TCP, is in use. The protocol allows client/server applications to detect the following security risks [1], [2], [3]:

- Message tampering
- Message interception
- Message forgery

The TLS/SSL protocol can be divided into two layers. The first layer consists of the application protocol and the three Handshake sub-protocols: the Handshake Protocol, the Change Cipher Spec Protocol, and the Alert Protocol. The second layer is the Record Protocol. The following figure

illustrates the various layers and their components. Figure 3 illustrates the different layers and their components.

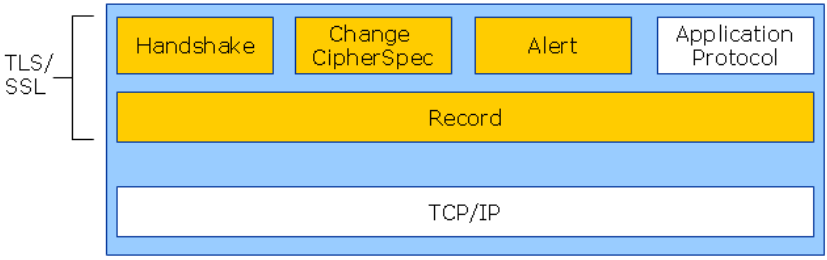

Fig.3. Preview of the layers and their components

3.1. The Handshake protocols of the TLS/SSL protocol are responsible for establishing or resuming secure sessions. The main goals of this layer are to:

- Negotiate cipher suites and compression algorithms.
- Authenticate the server to the client and, optionally, authenticate the client to the server through certificates and public or private keys.
- Exchange random numbers and a pre-master secret. Together with some further data, these values will be used to create the shared secret key that the Record Layer will use to hash and encrypt application data. The shared secret key is called the Master Secret

The Handshake protocol provides a number of very important security functions. It performs a set of exchanges that starts authentication and negotiates the encryption, hash, and compression algorithms [1], [2], [3].

3.2. The Change Cipher Spec Protocol

The Change Cipher Spec Protocol signals a transition of the cipher suite to be used on the connection between the client and server. This protocol is composed of a single message which is encrypted and compressed with the current cipher suite. This message consists of a single byte with the value 1. Message after this will be encrypted and compressed using the new cipher suite.

3.3. The Alert Protocol

The Alert Protocol includes event-driven alert messages that can be sent from either party. Following an alert message, the session is either ended or the recipient is given the choice of whether or not to end the session. The alerts are defined in the TLS specification in RFC 2246.

3.4. The Record Layer

The recording protocol receives data from the application layer and delivers them to the transport layer. Then he takes the data, fragments them to an appropriate size for the cryptographic algorithm, applies MAC or HMAC, and then encrypts (or decrypts) the data using the information agreed upon during the Handshake protocol. HMAC is only supported by TLS.

4. Operating principle

Once a client starts communication with the server, TCP connection gets established following these steps [1], [2], [3]:

- The Client first communicates with the server by sending a Hello message. The message includes number of options that will be used in the communication, such as version of the protocol to be used, Cipher Suite supported by the client, compression methods and a 32 byte random number.
- Server replies to the Hello message and makes choices about the option to be used, like version of protocol, Cipher Suite and compression methods. It also fills up the Session ID and replaces the 32 byte random number with date and timestamp.
- The server now sends Digital Certificates to the Client. The Digital Certificates contains the public key of the server.
- The Clients verifies the Digital Certificate with Certificate Authority.
- After the Digital Certificate is verified, the client starts to negotiate the symmetric key. There are a number of algorithms it can use. For an example of them is Diffie – Hellman key exchange algorithm shown on fig. 4.

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher

Cryptographic explanation of the algorithm by the studied Example [1], [2], [3]:

In the most accessible and elementary way, the protocol uses the multiplicative group of integers mod (module) P, where P is base and G is the primitive root of P. These two values are chosen in such a way to ensure that the shared secret can accept any value from 1 to P-1. In the example of the protocol we will mark non-target values in blue and secret values in red.

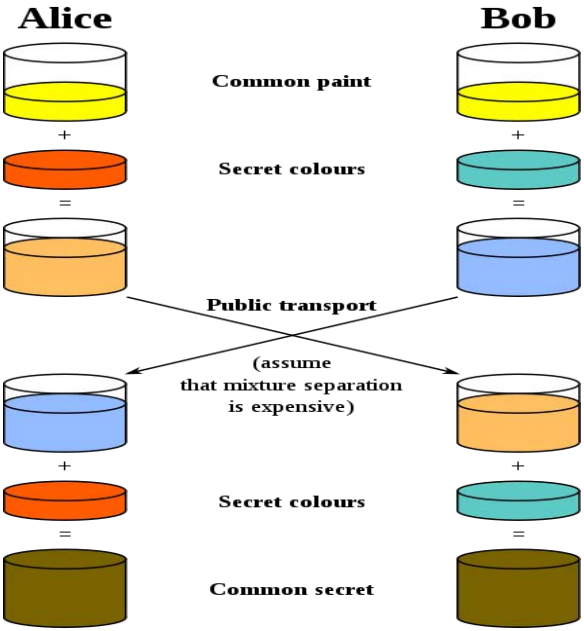

Fig.4. Diffie – Hellman key exchange algorithm

Silvi and Gosho agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).

Silvi chooses a secret integer $a = 4$, then sends Gosho $A = g^a \bmod p$

- $A = 5^4 \bmod 23 = 4$

Gosho chooses a secret integer $b = 3$, then sends Silvi $B = g^b \bmod p$

- $B = 5^3 \bmod 23 = 10$

Silvi computes $s = B^a \bmod p$

- $s = 10^4 \bmod 23 = 18$

Gosho computes $s = A^b \bmod p$

- $s = 4^3 \bmod 23 = 18$

Silvi and Gosho now share a secret (the number 18).

Conclusion : Both Silvi and Gosho have arrived at the same value s, because, under mod p,

$A^b \bmod p = g^{ab} \bmod p = g^{ba} \bmod p = B^a \bmod p$ **and more precisely**

$(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$

The server processes the key exchange parameters. It also checks the MAC or Message Authentication Code to the server.

If everything goes well, a secure TLS connection is established between the server and the client and secure communication starts to transfer sensitive application data. Fig. 5 shows a schematic view of the operating principle [1], [2], [3].

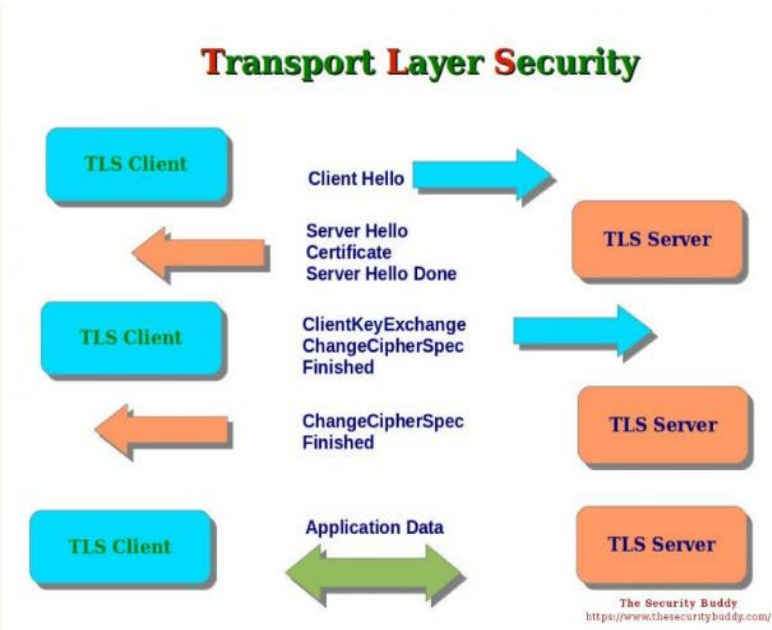

Fig.5. Principle of TLS protocol operation

5. Network ports used by TLS / SSL

Each standard TLS / SSL protocol is described by "service name" and its "network port"

Table 1. Description of TLS / SSL on Service Name and its network port

Service Name	smtp	https	nntps	ldaps	ftps-data	ftps	telnets	imaps	tftps
TCP Port	25	433	563	636	989	990	992	993	3713

3. Conclusion

The purpose of the study is to show the use of protocols on the Internet Transport Layer Security and Secure Sockets Layer. Our research is widely used in computer networks

REFERENCES:

1. Pease, S. (2009). Secure Sockets Layer. Cengage Learning, Boston.
2. Andreev A. The environment of security and influence national security and national interests. NMU- Shumen. Scientific Conference "Problems of national security", 2009, ISSN 1314-0647).
3. Andreev A. Any aspects of security what concept. NMU- Shumen, Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.

Author's name: Daniel Rosenov Denev, student
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences

Author's name: assoc. prof. Tsvetoslav St. Tsankov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences
E-mail: c.cankov@shu.bg

THE RELATIONS BETWEEN THE STATE AND THE RELIGIOUS ORGANIZATIONS AS A FACTOR POSING THREATS TO THE NATIONAL SECURITY OF BULGARIA

Tihomir I. Solakov

ABSTRACT: *The relations between the state and the religious communities have always been crucial for the state policy in the area of security. This is due to the fact that the religion of the traditional church determines the self-awareness of a great part of the members of the society who may influence all spheres of state government and national security. The spreading of non-traditional religious denominations over the territory of a country bears risk for a drastic change in the behavior of certain groups of individuals and also for establishment of communities that are often violent in one form or another, and this gives rise to serious threats to the national security.*

KEYWORDS*: Religious organizations, Threats, National security.*

1. Introduction

The purpose of the present paper is to make brief review of the attitude of the state to the religious freedom and the religious denominations in Bulgaria in the period after 1989 as a factor posing threats to the national security of the country.

The faith in the divine creation, in the existence of supernatural and divine powers lies in the foundations of the religious public awareness. If any extreme forms of religious thinking, concepts and philosophies exist, they give rise to the formation of religious fanaticism.

In Bulgaria the religious freedom (freedom of religious denominations) is regulated by the Constitution of the Republic of Bulgaria and by the Religious Denominations Act which set the Christian Orthodox denomination as the official religion of the country. These two regulatory acts do not place the Christian Orthodox religion above the other religious denominations, rather they are equal. In its essence, this provides the opportunity to all people who live in the Republic of Bulgaria, regardless of their status, to have the freedom to choose to practice a religion that is close to their personality within the framework of the public life.

2. Main text

The Constitution and the Criminal Code strictly forbid the following:

- Association in organizations based on religious principle, establishment of religious movements and unions;
- Instigation of racist and religious hatred, detestation, disrespect and opposition to traditional religious canons, written rules and generally adopted as valid by sects preaching non-democratic religious concepts.

In the modern world there are different religions, however five of them are recognized as traditional religions:

1. Christianity is a monotheistic religion, one of the most wide spread religions in the world. [7] It is an epitome of the divine beginning of Jesus Christ and his Apostles and followers. The aim of Christianity is to establish a close relation with God the Father. This relation becomes possible through the life of Jesus Christ and the serving to the Holy Spirit in the Christians' lives. Christians believe in one god who exists in three faces – God the Father, God the Son (Jesus Christ) and the Holy Spirit.[8];

2. Islam has been a syncretistic religion in its beginning.[9] It is focused on the belief that Allah is the only God and Mohamed is his prophet.[10] Muslims believe in the only, eternal God who created the sky and the earth and everything that exists. Muslims do not believe that Mohamed was the only prophet; they rather believe that he was the last prophet.[11];

3. Judaism is based on sacred writings called TENAKH. The main dogmas of Judaism are as follows: recognition of the single deity Yahweh and the Hebrew people as being the God chosen people, belief in the divine Saviour (messiah), the holiness of the Old Testament and Talmud.[12];

4. Buddhism is a unique world religion which has origins in Indochina, although it has much in common with Hinduism in that both religions speak of "karma" (cause-and-effect relation), "maya" (illusory nature of the world) and "samsara" (cycle of repeated birth). Buddhists believe that the ultimate goal of life is to achieve "enlightenment" according to their own perceptions.[13];

5. Hinduism is a religion practiced by the predominant part of the people in India[14]. It is considered to be a polytheistic religion which

[7] http://www.znam.bg/com/action/showArticle?encID=1&article=266593971
[8] https://www.gotquestions.org/Bulgarian/Bulgarian-Christianity.html
[9] https://www.kaldata.com/forums/topic/149994-ислям-за-любопитни/
[10] https://www.gotquestions.org/Bulgarian/Bulgarian-Islam.html
[11] http://www.way-to-allah.com/bul/islam/was_ist_islam_bul.htm
[12] https://www.forumnauka.bg/topic/411-юдаизмът/
[13] https://www.gotquestions.org/Bulgarian/Bulgarian-Buddhism.html
[14] Vladislavov Ivan, The 10 Major World Religions („10-те най-големи световни религии"), 30.10.2013, https://www.10te.bg/obshtestvo/10-te-nai-golemi-svetovni-religii/

recognizes not less than 330 million gods, however there is one "God" who is the supreme god – Brahma.[15] The main dogmas are as follows: dharma (duty), karma (retribution) and samsara (reincarnation of the soul).[16] Hinduism covers a wide circle of differentiating strains, from people's Hinduism and Vedism to Bhakti and Vaishnavism. All of them are united on the basis of shared concepts, recognizable rituals, common cosmology and textual basis, pilgrimages to common sacred places. [17]

In the period from 1945 to 1989 the Bulgarian state leaders imposed the Communist party policy and namely their atheistic policy. In that time the security and public order services were used for [36], [37], [38], [39], [40]:

- Prosecution of people for their religious beliefs regardless of the religion their practice;
- Destruction of the Bulgarian Orthodox church, eliminating the clergy and appointing obedient and harmless bishops and patriarch, thus making the church voiceless and without individuality.

During the 45-year long period of atheism in Bulgaria the active religious organizations and communities were entrepreneurial and optimistic. Contrary to any expectations, they made frantic attempts to take prominent positions in the Bulgarian spiritual space and to evangelize the people despite the strict control of State Security. [18]

The political regime in Bulgaria changed after 10 November 1989. The Communist party gradually lost its power and gave way to the newly founded political parties. In spiritual aspect the Bulgarian society was found to be bouncing from one extremity to another – from strict control to absolute lack of any control. The political change suggests a spiritual change as well. The state has provided its people freedom of religious denominations, which apart from establishing the right of religious denominations as an absolute and inviolable right, it also provides opportunity for free and indiscriminate inflows of new religious movements into the country.[19] This is due to some extent to the fact that the unit performing control over the religious denominations at the State Security structure has been closed, and this in turn

[15] https://www.gotquestions.org/Bulgarian/Bulgarian-Hinduism.html

16 http://www.znam.bg/com/action/showArticle;jsessionid=6A892EFEAE16A501987E95943F2522BC?encID=1&article=534844185

[17] http://religii.pmg-silistra.com/индуизъм/

[18] Hristova Milka, Religious Movements in Bulgaria („Религиозните движения в България"), 19.06.2006, https://dveri.bg/component/com_content/Itemid,139/catid,112/id,2426/view,article/

[19] Hristova Milka, Religious Movements in Bulgaria („Религиозните движения в България"), 19.06.2006, https://dveri.bg/component/com_content/Itemid,139/catid,112/id,2426/view,article/

gives chance for religious denominations to enter the country freely and to spread sectarian religious dogmas that are unacceptable for the Bulgarian society. On the other hand, due to the attitude of the state to the Orthodox Church before 1989, the church has lost to some extent the influence which an official religion should have. And where the traditional religions and churches are weak, immediately aggressive or less active new religious denominations come in. The aims and the activity of the latter are focused on taking the niches in the spiritual and religious life of the Bulgarian society through obliteration of the role of the Christian Eastern Orthodox Church and the official religions registered in Bulgaria in accordance with the Religious Denominations Act. In principle the new religious communities aim at attracting Bulgarian citizens with life problems and dramas (divorced, uncared for, people who have gone poor or live in extreme poverty and crisis). Those people find spiritual consolation and material mission, and the sect (the religious community) performs supportive mission to its followers.

In accordance with the Religious Denominations Act adopted not until 2002, new religious movements, sects and cults have to be registered and entered in a special register kept at Sofia City Court. The Council of Ministers is the body appointed to conduct the state policy in the area of religious denominations through its special *Denominations* Directorate. Unfortunately, gaps in the legislation before the adoption of the Religious Denominations Act allowed the denominations to avoid the special registration regime by registering as non-profit legal entities. Religious movements registered as non-commercial legal entities lay down in their Statutes that they perform humanitarian activities and educational services, and not religious activity. This registration scheme is still applied even after the Religious Denominations Act has been adopted. This allows for active religious activity to be performed without the state being able to exercise control over it in accordance with the above specified act.

In Bulgaria, especially after 1989, various religious methods of influencing the personality have been applied aiming at distancing different groups of the society from the traditional rules and canons.

Regarding the Roma ethnicity a flurry of activity is performed by the following:

- evangelical denominations stemming from the Anglican Church;
- humanitarian non-governmental associations of various religious denominations originating from the Scandinavian countries;
- “Jehovah's witnesses”, who through their various forms of denominations influence in a focused, aggressive and specific manner the Roma ethnicity.

Regarding the Islamic religion, after 1989 there can be noticed islamification among the Bulgarian citizens practicing the Muslim religion. This process is not initiated by followers of traditional Islam, but rather it is a consequence of the professed by emissaries of the Arab world religious fanaticism, coming with the new forms of Islam associated with interpretation of the main holy book of the Muslims, the Quran. As a supreme authority of the Islamic religion in Bulgaria, the Muslim Mufti's Office does not accept the new Islamic dogmas. The ethnic groups towards which the Islamic sects have targeted their activity are the Bulgarian Turks, the Bulgarian Mohammedans (pomaks), the Turkish gypsies and Bulgarian citizens practicing Christianity (after converting to the Muslim religion these people become converts) [29], [30], [31], [32], [33], [34], [35], [41].

After 1989 through Europe the Hindu sect called *Krishna Consciousness* established itself on the territory of Bulgaria and since then it has been actively performing its activity. In the Bulgarian society the sect is more popular as a communal society – KRISHNO. It is known about the followers of *Krishna Consciousness* in Bulgaria that after been accepted in this denomination they had to provide their leaders with a letter of authorization granting them rights to manage their followers' property without any restrictions, as well as their relatives' title deeds for ownership of properties. At a later stage the sect leaders would sell the properties in question. The buildings and premises inhabited by the sect members have no furniture, and the followers sleep on the bare floor. They take opiates and in a state of intoxication have indiscriminate and uncontrolled sexual intercourses. Only the male followers of the sect perform their labour activity during daytime.

Another denomination which is active mostly among school and university students after 1989 is called *Branch Davidians*. This denomination influences its followers in a psychological manner convincing them that life has no purpose, and at a later stage makes them sacrifice their own lives, presenting this act as ultimate pleasure. As a result of this, the cases of suicides and people throwing themselves from high buildings become more frequent.

According to the advisor from *Denominations* Directorate at the Council of Ministers Mr Georgi Krastev, with regards to the different religious denominations active on the territory of the country, "Some of the biggest do not even correspond to our idea of religion, they are combinations – a public phenomenon. A symbiosis of policy, religion and economy". In support of the latter, the expert from the Centre for Research of New Religious Movements Mr Blagovest Varbakov says: "They organize numerous seminars and courses for improvement of management and

communication skills, focusing on leadership qualities. All this is targeted to the business, and they attack exactly this sector, because Bulgaria is still in the beginning of its economic development. They are not registered as a denomination with their name, rather they and other organizations similar to them, act as foundations. To attract new members the sects use all tools and techniques of modern advertising. Some of them are campaigning at the doorstep, disseminating materials in the street, demonstrated compassion to the other people's problems. "Many modern techniques are used, for instance the religious doctrine is translated in the language of modern music culture. It's one thing to listen to songs dating back to several centuries ago, and it's a completely different thing to listen about Jesus Christ in pop music style. There are such music groups. And it's not by chance that Protestants are very successful among the Roma people", says Mr Georgi Krastev"[20]

The possibility for free practice of religious activity with the state being unable to exercise efficient control leads to the establishment of extreme forms of religious dogmas, based on extremist principle. Religious extremism is striving for reorganization of the world based on the religious beliefs. And it is not only a radical rejection of the constitutional foundations, but it is expressed through violent acts aiming at destruction of a state system, and all extremist acts are performed by groups of individuals. In addition, this concept is interpreted as a rejection of the integral system of the traditional religious values of the society, the desire for one religion to expand its beliefs and religious laws for the society as a whole. The main goal of the religious extremism is the recognition of its denomination as the only one, together with the suppression and destruction of all other religious denominations, and their forced adherence to this denomination [21]. Religious fanaticism and extremism of sects is focused on fulfilling the idea of overthrowing the secular form of state governance, the constitutional way of living and public system by introducing:

- religious totalitarian style of governance in the religious community led by a spiritual leader;
- religious norms and dogmas of conduct, lifestyle, mentality and communication.

[20] Dimitrov Samuil, Faith, Sects – Religion and Something Else. The new movements are a combination of religion, policy and economy. There are already 95 denominations registered in our country, Sega newspaper 25.01.2008, http://old.segabg.com/article.php?id=354635

[21] https://muzruno.ru/novini-i-obshhestvo/237137-vnimanie-religiozen-ekstremizm.html

3. Conclusion

The evolution of the relations between the state and the religious communities before and after 1989 leads to the entry of various denominations, different from the traditional religions, in the territory of the country. After 1989 they perform free and uncontrolled activity on the territory of the country, mainly focused on spreading the ideas of non-traditional denominations and radical ideas which pose threat to the national security.

REFERENCES:

1. See details in Marinov, Boris, Is religion the opium for the human soul and the people? (Опиум ли е религията за човешката душа и за народите?) Yearbook of St. Kliment Ohridski Sofia University . vol. XXI, I. C., 1943-1944, p. 3-24.
2. http://www.znam.bg/com/action/showArticle?encID=1&article=266593971
3. https://www.gotquestions.org/Bulgarian/Bulgarian-Christianity.html
4. https://www.kaldata.com/forums/topic/149994-ислям-за-любопитни/
5. https://www.gotquestions.org/Bulgarian/Bulgarian-Islam.html
6. http://www.way-to-allah.com/bul/islam/was_ist_islam_bul.htm
7. https://www.forumnauka.bg/topic/411-юдаизмът/
8. https://www.gotquestions.org/Bulgarian/Bulgarian-Buddhism.html
9. Vladislavov Ivan, The 10 Major World Religions („10-те най-големи световни религии“), 30.10.2013.
10. https://www.10te.bg/obshtestvo/10-te-nai-golemi-svetovni-religii/
11. https://www.gotquestions.org/Bulgarian/Bulgarian-Hinduism.html http://www.znam.bg/com/action/showArticle;jsessionid=6A892EFEAE16A501987E95943F2522BC?encID=1&article=534844185
12. Hristova Milka, Religious Movements in Bulgaria („Религиозните движения в България“), 19.06.2006г, https://dveri.bg/component/com_content/Itemid,139/catid,112/id,2426/view,article/
13. Timothy Shah, Monica Toft, Why God is Winning?, Forum on Religion & Public Life, http://glasove.com/categories/kultura-i-obshtestvo/news/zashto-bog-pecheli
14. https://muzruno.ru/novini-i-obshhestvo/237137-vnimanie-religiozen-ekstremizm.html
15. Dimitrov Samuil, Faith, Sects – Religion and Something Else. The new movements are a combination of religion, policy and economy. There are already 95 denominations registered in our country („Вяра, Сектите - религия и още нещо, Новите движения са комбинация от религия, политика и икономика. У нас вече са регистрирани 95 вероизповедания“), Sega newspaper, 25.01.2008, http://old.segabg.com/article.php?id=354635.
16. Ivanov, M., Intelligence Infrastructure, Sofia, Profisec, 2012, p. 215, ISBN 978-954-32927-1-8.
17. Ivanov, M., Nazism and Islam, MATTECH 2018, Shumen, St. Konstantin Preslavsky University Publishing House, 2018, ISBN 1314-3921.
18. Ivanov, M., Army and Police - Diffusion of Functions and Tasks, Fourth National Conference with International Participation "Metal Science, Hydro- and Aerodynamics and National Security 2014", Sofia, 2014, ISBN 1313-8308.

19. Савов, И., Един поглед върху противодействието на хибридните заплахи в Европейския съюз, международна конференция „Асиметрични заплахи, хибридни войни и влиянието им върху националната сигурност", Нов Български университет, март 2018 г., ISBN 978-619-7383-09-6, с. 179-185.
20. Савов, И., Борисов, Т., A look on the nature of agreements for the application of the readmission institute, International conference – European integration, Nikola Tesla University, 2018, Beograd, ISBN 978-86-6113-050-2, p. 45-56.
21. Савов, И., Рискове и заплахи за сигурността в Черноморския регион, Международна конференция „Проблеми на сигурността в черноморския регион", ВУСИ, септември 2017 г., ISBN 978-619-7343-09-0, с. 7-18.
22. Savov, I. Some aspects of legislative system of the institutes migration and readmission in the European Union, International conference - Law and Security in migration process and the consequences of the migration crises, Nikola Tesla University, Beograd, 2017, ISBN 978-86-6113-046-5, p. 265-277.
23. Andreev A. Any aspects of security what concept. NMU- Shumen, Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.
24. Andreev A. The environment of security and influence national security and national interests. NMU- Shumen. Scientific Conference "Problems of national security", 2009, ISSN 1314-0647).
25. Andreeva G., Andreev A. Survey and analysis of intercultural communication in Bulgaria and abroad. Journal Scientific and applied research, USA, vol.3, p.89-97, 2013.
26. Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Русе, 2017, с.19-27, http://jei.uni-ruse.bg/Issue-2016/02.%20Zagorcheva%20-%20Pavlov.pdf.
27. Zagorcheva, D., Stages in the systems for financial management and control in the Bulgaria's public sector, The XIV International Scientific Conference Information Technologies and Management, 2016, Riga, Latvia.
28. Загорчева, Д, Велчева, Й., Бюджетната децентрализация като фактор за едновременно развитие на общините и индустриалния бизнес, Народностопански архив, година LXX, книга 3 – 2017, ISSN 0323-9004, стр. p.46-59, https://www.uni-svishtov.bg/NSArhiv/title.asp?title=981.
29. Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6 (available at: http://varepsilon.com/), indexed in Russian Science Citation Index, (РИНЦ: Научная электронная библиотека eLIBRARY.RU), ВИНИТИ РАН Электронный каталог научно-технической литературы VINITI.RU, National Centre for Information and Documentation (Bulgaria), Google Scholar, OpenAIRE, Polish Scholarly Bibliography (PBN), Index Copernicus International, ROAD, the Directory of Open Access scholarly Resources, DOAJ, Directory of Open Access Journals.
30. Hristov, Hr., Development of warfare and counter-terrorism. Journal Science Education Innovation, ISSN 1314-9784, vol. 3. 2014, pp. 104-111.
31. Hristov, Hr., A modern survey on problems of business organization's security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

32. Boyanov, P., Educational exploiting the information resources and invading the security mechanisms of the operating system windows 7 with the exploit Eternalblue and Backdoor Doublepulsar, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 14, 2018, pp. 34-41, available at: http://www.rst-tto.com/publication.html.
33. Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, Vol.3, 2013, pp. 114-124, available at: http://www.rst-tto.com/publication.html.
34. Досев, Н., Създаване на склад от данни за определяне на риска за информационната сигурност на корпорацията, Научна конференция с международно участие на тема „Киберсигурността в информационното общество", Факултет "А, ПВО и КИС", Шумен 2017 г.
35. Досев, Н., Създаване на модел на система за ранно предвиждане рисковете за информационната сигурност на корпорацията, Научна конференция MATTEX на ШУ „Еп. К. Преславски", гр. Шумен, 2016 г.
36. Досев, Н., Обезпечаване сигурността на достъпа до интегриран склад от данни, Международна научна конференция 2016, Факултет „А, ПВО и КИС" гр. Шумен, 2016.
37. Добрев, Д., Европа – философия и политика. Издателство „Просвета-София", ISBN 978-954-01-3785-8, 2018 г.
38. Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.
39. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security" № 1(3)-2013 УДК 004 (056.5+413.5).
40. О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA", Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски", 2015г.
41. Velikov, I., Humanitarian aspects of protection of information, MATTEX 2018 Conference proceedings, Konstantin Preslavsky University of Shumen, ISSN 1314-3921, Shumen, Vol. 2, part 1, 2018, pp. 3-10.

Author's name: Tihomir I. Solakov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems"

PROBLEMS OF THE ECONOMIC DEVELOPMENT OF BULGARIA

Tsvetelina I. Metodieva

ABSTRACT: *Bulgaria is above all a country of labor emigration. Half of the unemployed young people in the EU between the ages of 24 and 34 are ready to move to job search, according to the latest Eurostat study. This objective fact determines the focus of our attention above all on the problems of labor migration from Bulgaria. Economic, social, demographic, etc. the importance of labor emigration from Bulgaria is a well-known fact.*

KEYWORDS: *labor emigration, economic security, unemployed young people.*

In the conditions of radical economic and socio-political transformation, Bulgaria is actively involved in the international migration of labor, where a strong asymmetry can be noted.[1] Bulgaria is primarily a country of labor force migration, while the immigration of labor resources for now has more of a symbolic nature [1], [2], [3], [4], [5], [6], [9], [10].

Half of the unemployed young people in the EU aged between 24 and 34 are willing to relocate in search for a job, shows the latest Eurostat survey. In 2016, 21% of them had to go to another city within the country they live in, another 12% – in another country, but within the EU. For 17% of the young people, searching for a job and moving to countries outside the EU is admissible [2], [5], [11], [12], [13], [14], [15], [16], [17].

This objective fact makes directing our attention towards the problems of emigration of the labor force from Bulgaria. Economic, social and demographic importance of labor emigration from Bulgaria is a generally acknowledged fact. The presence of information deficit should not surprise us about the substantially differing estimates for the amount of labor emigration from Bulgaria and its economic effects (e.g., the amount of cash transfers of migrants to their relatives in the country). The intensive emigration of labor force from Bulgaria after 1990 is a result from a whole set of economic, social, political, institutional and legal factors [3], [13], [14], [15], [16], [17].

An attempt for a vague characterization of these factors will surely highlight the following essential points [13], [14], [15], [16], [17]:

• The huge unemployment in the country. As far as the Bulgarian transition was accompanied by rapid deindustrialization, sharp "contraction" in economic activity, the deep crisis of the system transformation, etc. for a

short time the unemployment in the country has become a mass occurrence. People from all social groups poured into the ranks of the unemployed ones. The emerging small and medium private business was unable to provide jobs in an attempt to absorb the huge mass of unemployed people. According to the official national statistics in 2001 the unemployed citizens were 636 500 (19.5% of the total number of workforce) [4]. We have to add and 513 700 people, defined as "discouraged", i.e. persons who are outside the workforce for more than 10 years. Completely understandable is the desire of the unemployed and discouraged to look for a job abroad not only for a work realization, but also as a real opportunity for survival [13], [14], [15], [16], [17].

• The substantial differences in the levels of economic development and income between our country and other developed and post-socialist countries. According to the interesting analysis of Prof. Stephan Stoilov [5], the gross domestic product per capita in Bulgaria for 2005 is 3.28 times lower than the one in the EU-15. In the same year, the average nominal wage in Bulgaria was 17.3 times lower than its size in the EU-15. The level of wages in Bulgaria is 3 to 6 times lower than in Central European countries that joined the EU in 2004. The substantial differences in the levels of economic development and income are a key factor for the rapid leakage of work force from Bulgaria to Western and Central Europe, North America and other destinations. As far as overcoming these differences is possible within a relatively large historical period, it is reasonable to suggest that this factor (as opposed to the unemployment factor) will retain its importance for a long period of time [13], [14], [15], [16], [17], [43], [44], [45], [46].

• The deep frustration from the Bulgarian transition [6]. The system transformation in our country, as is well known, didn't go particularly civilized. The opaque privatization, the all-embracing corruption, massive household and business crime, social polarization, marginalization of large groups of the population, cultural degradation, erosion of traditional Bulgarian values and other such negative phenomena, have lead up to a massive disappointment from the Bulgarian transition and laid the foundations for deep pessimism among Bulgarian citizens, feeling disappointed by the lack of any positive perspective in Bulgaria. A socio-psychological environment like this inevitably stimulates the emigration to a better „settled“ country, with greater social security and perspectives for a successful professional realization [13], [14], [15], [16], [17].

• The presence of already established immigrant networks in some key countries for the Bulgarian emigration. The existence of such networks facilitates the gathering of the necessary information from potential migrants,

saves expenses abroad, assists immigrants in their searching for a job in the respective host countries, etc [7].

• Liberalization of the Bulgarian State policy towards immigration. At the beginning of the democratic changes all restrictions on emigration in Bulgaria were eliminated, which made it possible to leave the country in 1990-1992. Each year, between 50 and 60 thousand people left Bulgaria in search for a job abroad, 2.5 million Bulgarians in working age are abroad. Each year these people send in the country over 1.7 billion euro. This is the cause of another Bulgarian absurdity-the largest investor of Bulgaria are ... the Bulgarians [8].

• The adequate legal and institutional framework of labor emigration. A major role among the normative acts plays the Employment Promotion Act and the Ordinance on the conditions and procedures for the conduct of intermediary activity information and acceptance of work. Significant bilateral agreements have been signed at interstate level for sending and exchanging labor. These agreements set out the international legal frameworks under which the legal migration of labor force between Bulgaria and the respective partner countries takes place [13], [14], [15], [16], [17].

The protection of interests of the Contracting Parties and their citizens requires that the stated bilateral labor agreements to be signed "together" with readmission agreements and social security agreements for migrants.

The competent state institution, which is entrusted with the implementation of the state emigration policy, is the Executive Employment Agency. It cooperates with the public employment services of the partner countries, responsible for the employment of foreigners. The Agency is a major information center for the terms and conditions under which Bulgarian citizens can legally work in different partner countries. It also performs significant intermediary activity. Such activity on the recruitment and sending of labor emigrants abroad is also carried out by a number of private companies, which have been explicitly authorized to do so [13], [14], [15], [16], [17], [43], [44], [45], [46].

• The European integration of Bulgaria. The European Association Agreement, signed on 8 March 1993, retained the competence of the EU Member States to regulate the movement of workers with Bulgaria on the basis of bilateral interstate agreements. EU member states undertook to maintain existing facilities for Bulgarian workers to access their labor markets and, if possible, to improve these facilities. EU member states that did not have bilateral agreements signed with Bulgaria were obliged to "consider favorably the possibility to conclude such agreements".

With the Treaty of Accession of the Republic of Bulgaria to the European Union, signed on 25 April 2005, a relatively flexible regime for the

regulation of labor migration between our country and the EU-25 countries was enrolled. Our country accepted the transition period (maximum 7 years) about the full opening of the labor markets of the Union member states for Bulgarian workers under the EC internal market legislation. EU Member States were given the option of autonomously deciding about the opening of their labor market to Bulgarian workers, depending on the specific situation in each country. Since the beginning of 2007, 10 EU Member States have fully opened their national labor markets for Bulgarian workers. Another 9 EU Member States will apply an authorization regime for the employment of Bulgarian workers during 2007-2008 [13], [14], [15], [16], [17], [41], [42].

The rest of the EU Member States will apply a facilitated authorization regime for the recruitment of Bulgarian workers with the gradual opening of their national labor markets and the elimination of restrictions about the free movement of Bulgarian workers. The clearly expressed strategic course towards Bulgaria's integration into the EU and the adequate regulatory and institutional basis that has been established, explains the assertion of the EU member states as the main countries of immigration for the Bulgarian workers [9], [13], [14], [15], [16], [17].

Evaluation about the amount of labor emigration from Bulgaria after 1990 shows significant differences. According to a representative migration survey accompanying the 2001 census, between 1992 and 2001, 196,000 people emigrated from Bulgaria [10]. According to the study of V. Minchev and V. Boshnakov at the end of 2005, Bulgarian labor emigrants were more than 217 000 people [11]. According to official data of the Ministry of Labor and Social Policy, between 1991 and 2001,177,000 Bulgarian citizens left the country [18], [19], [20], [21], [22], [23], [24], [25].

A survey made by the Institute for Market Economics sets the number of emigrants from Bulgaria in the period 1990-2005 to about 800 000 people.

The main part of Bulgarian labor emigration is directed to EU member states - Greece, Spain, Germany, Great Britain, and Italy. It can be expected that with the further opening of the labor markets of these countries for Bulgarian workers and specialists, with the high level of coordination of our social security system and that of the EU member states, the European direction will keep its leading position over the emigration of labor force from Bulgaria in the future. Obviously the labor migration to the "southern flank" of the EU - Greece, Cyprus, Italy, Spain and Portugal - is clearly increasing. Some authors define this trend as a manifestation of South-South migration and explain this with the effects of factors, such as geographical proximity and the similar mentality of South Europeans [26], [27], [28], [29], [30], [43], [44], [45], [46].

The main host countries for Bulgarian workers and professionals outside Europe are the traditional countries of immigration - the United States and Canada. These two countries, as well as the UK and Germany, are the main attraction centers for the highly qualified labor force leaving Bulgaria after 1990 [31], [32], [33], [34], [35], [43], [44], [45], [46].

In her report, Vanya Grigorova explains that work migration and mobility must be stopped first, i.e. stopping the import efforts of cheap third-country workers. Second - reviving vocational schools, but with a guarantee from employers that when graduated, the student will have an opportunity to evantuate against a decent pay. The third important thing is for employers to be obliged to declare their vacancies at the labor offices. This will allow workers to have a concept about the situation at the moment and the government will have ‘’clear picture’’ in which areas there is or no shortage of staff and what are the levels of payment. These three steps will pay off and will not allow Bulgaria to pull back Europe and its level of payment, because that is exactly what will happen if we continue to do that.

Emigration may be good for emigrants and their relatives in the country who are receiving financial help from those who have live abroad, but it is not good in the long run for Bulgaria. Because the combination of these and many other factors questions it is future as a nation and as a country with a prosperous and happy population. The world is big and full of difficulties, no one will care about Bulgaria and come to solve its problems. This can only be done by the fewer Bulgarians who have remained in their homeland [36], [37], [38], [39], [40].

The earth as a social space acquires different dimensions - the country, the homeland or, more precisely, the birthplace, the historical land or the native land, and finally the state-political institution with its specialized bodies for the introduction of order [13].

REFERENCES:

1. International labor migration: economic aspects,file:///C:/Users/%D0%A6%D0%B2%D0%B5%D1%82%D0%B8/Downloads/docl_24873_370392297%20(7).pdf, 43.
2. www.investor.bg/evropa/334/a/polovinata-bezrabotni-mladeji-v-es-sa-sklonni-da-stanat-trudovi-migranti-258269/.
3. file:///C:/Users/%D0%A6%D0%B2%D0%B5%D1%82%D0%B8/Downloads/docl_24873_370392297%20(7).pdf, 44, 1. International labor migration: economic aspects, https://www.minfin.bg/upload/9023/I.B.2001.pdf, p. 22.
4. International labor migration: economic aspects,file:///C:/Users/%D0%A6%D0%B2%D0%B5%D1%82%D0%B8/Downloads/docl_24873_370392297%20(7).pdf, 44.
5. Minchev, V., V. Boshnakov, Economics of Bulgarian emigration, p. 31, 35, 36.
6. www.investor.bg/ikonomika-i-politika/332/a/mejdu-50-i-60-hil-dushi-napuskat-bylgariia-vsiaka-godina-v-tyrsene-na-rabota-209183/.
7. International labor migration: economic, p. 46.

8. http://departments.unwe.bg/Uploads/ResearchPapers/Research%20Papers_vol2_2007_No1_V%20Marinov.pdf, p. 46.
9. Minchev, V., V. Boshnakov, A look at the Bulgarian migration model..., p. 64.
10. file:///C:/Users/%D0%A6%D0%B2%D0%B5%D1%82%D0%B8/Downloads/docl_24873_370392297%20(7).pdf, 46, International labor migration: economic, newspaper "Trud", 9 December 2005 year., p. 2.
11. http://bnr.bg/radiobulgaria/post/100958973/balgarskite-emigranti-izprashtat-poveche-pari-v-stranata-otkolkoto-chujdestrannite-investitori.
12. http://bnr.bg/radiobulgaria/post/101054254/zakrivaneto-na-profesionalnite-uchilishta-e-problem-za-balgarskata-ikonomika.
13. Христов, Х., Солаков, Т., Процеси на реислямизация сред мюсюлманската общност и провеждана малцинствена политика в Република България, Юридически сборник на Бургаски свободен университет, Център по юридически науки, том XXV -2018, ISSN 1311-377, гр. Бургас, България, 2018 год., с. 105 -114.
14. Христов, Х., Солаков, Т., Различия между ислямски радикализъм и турски рационализъм. Причини, довели до разделението на мюфтийството, Юридически сборник на Бургаски свободен университет, Център по юридически науки, том XXV -2018, ISSN 1311-377, гр. Бургас, България, 2018 год., с. 114 -123.
15. Солаков, Т., Христов, Х., Мюсюлманската общност в Република България, Сборник доклади от Годишна Университетска Научна Конференция, Национален военен университет „Васил Левски", гр. В. Търново, България, ISBN 978-619-7246-20-9 (online e-book), 14-15 Юни 2018, с. 621-630.
16. Andreev A. The environment of security and influence national security and national interests. NMU- Shumen. Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.
17. Andreev A., Geo-information technologies for modeling of security disaster. Collection of scientific works, MATTEX Shumen's university "Bishop K. Preslavski "2012.
18. Andreeva I., Andreeva G., Andreev A. Conceptual models of retirement and promotion employment of older people in Bulgaria. Journal "Science, education, innovation", USA, vol.1, p.137-143, 2013.
19. Ivanov, M., Intelligence Infrastructure, Sofia, Profisec, 2012, p. 215, ISBN 978-954-32927-1-8.
20. Ivanov, M., Army and Police - Diffusion of Functions and Tasks, Fourth National Conference with International Participation "Metal Science, Hydro- and Aerodynamics and National Security 2014", Sofia, 2014, ISBN 1313-8308.
21. Савов, И., Един поглед върху противодействието на хибридните заплахи в Европейския съюз, международна конференция „Асиметрични заплахи, хибридни войни и влиянието им върху националната сигурност", Нов Български университет, март 2018 г., ISBN 978-619-7383-09-6, с. 179-185.
22. Савов, И., Рискове и заплахи за сигурността в Черноморския регион, Международна конференция „Проблеми на сигурността в черноморския регион", ВУСИ, септември 2017 г., ISBN 978-619-7343-09-0, с. 7-18.

23. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
24. Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Pyce, 2017, c.19-27, http://jei.uni-ruse.bg/Issue-2016/02.%20Zagorcheva%20-%20Pavlov.pdf.
25. Zagorcheva, D., Stages in the systems for financial management and control in the Bulgaria's public sector, The XIV International Scientific Conference Information Technologies and Management, 2016, Riga, Latvia.
26. Загорчева, Д, Велчева, Й., Бюджетната децентрализация като фактор за едновременно развитие на общините и индустриалния бизнес, Народностопански архив, година LXX, книга 3 – 2017, ISSN 0323-9004, стр. p.46-59, https://www.uni-svishtov.bg/NSArhiv/title.asp?title=981.
27. Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6 (available at: http://varepsilon.com/), indexed in Russian Science Citation Index, (РИНЦ: Научная электронная библиотека eLIBRARY.RU), ВИНИТИ РАН Электронный каталог научно-технической литературы VINITI.RU, National Centre for Information and Documentation (Bulgaria), Google Scholar, OpenAIRE, Polish Scholarly Bibliography (PBN), Index Copernicus International, ROAD, the Directory of Open Access scholarly Resources, DOAJ, Directory of Open Access Journals.
28. Hristov, Hr., Development of warfare and counter-terrorism. Journal Science Education Innovation, ISSN 1314-9784, vol. 3. 2014, pp. 104-111.
29. Hristov, Hr., A modern survey on problems of business organization's security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.
30. Boyanov, P., Educational exploiting the information resources and invading the security mechanisms of the operating system windows 7 with the exploit Eternalblue and Backdoor Doublepulsar, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 14, 2018, pp. 34-41, available at: http://www.rst-tto.com/publication.html.
31. Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, Vol.3, 2013, pp. 114-124, available at: http://www.rst-tto.com/publication.html.
32. Velikov, I., Humanitarian aspects of protection of information, MATTEX 2018 Conference proceedings, Konstantin Preslavsky University of Shumen, ISSN 1314-3921, Shumen, Vol. 2, part 1, 2018, pp. 3-10.
33. Досев, Н., Създаване на склад от данни за определяне на риска за информационната сигурност на корпорацията, Научна конференция с международно участие на тема „Киберсигурността в информационното общество", Факултет "А, ПВО и КИС", Шумен 2017 г.
34. Досев, Н., Създаване на модел на система за ранно предвиждане рисковете за информационната сигурност на корпорацията, Научна конференция MATTEX на ШУ „Еп. К. Преславски", гр. Шумен, 2016 г.

35. Досев, Н., Обезпечаване сигурността на достъпа до интегриран склад от данни, Международна научна конференция 2016, Факултет „А, ПВО и КИС“ гр. Шумен, 2016.
36. Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.
37. Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.
38. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).
39. Andreev A. Any aspects of security what concept. NMU - Shumen, Scientific Conference "Problems of national security", 2009, ISSN 1314-0647.
40. Василева, Р., Русева, В., Корупцията в сферата на държавната администрация, Сборник научни трудове от научна конференция с международно участие „MATTEX 2018“, ШУ "Епископ Константин Преславски", 25-27 октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
41. Василева, Р., Русева, В., „Корупцията - обществен феномен в България“, Сборник научни трудове от научна конференция с международно участие „MATTEX 2018“, ШУ "Епископ Константин Преславски", 25-27октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.
42. Василева, Р., Анализ на органите и структурата на местното самоуправление", Годишната университетска научна конференция, 14-15 юни 2018 г., гр. Велико Търново, ISSN:1314-1937 (print), 2367-7481 (online).
43. Dimitrova, N., 2014: The motivation for effective study of technical and technological information assimilation. International Scientific Online Journal – ISSN 2367-5721 Issue 4, December 2014, www.sociobrains.com, pp 94-99.
44. Dimitrova, N., 2015: Operationalize the aims of technological education International Scientific Online Journal. Issue 16, December 2015, www.sociobrains.com pp. 48 – 53.
45. Dimitrova, N., 2014: Role of informatization in technological education and information culture of students International Scientific Online Journal, Issue 2, October 2014, www.sociobrains.com pp. 26-30.
46. Димитрова, Н. Приносът на технологичното обучение за съхраняване на българските национални традиции. – Годишник на Шуменския университет „Епископ Константин Преславски”, Т. XX D, Научни трудове от конференция „Иновации в образованието”, 30 септември – 02 октомври 2016, Педагогически факултет, Шумен, Епископ Константин Преславски, 2016, 686 – 690.

Author’s name: Tsvetelina Metodieva, assistant and PhD student
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems“
E-mail: tsvetelina.metodieva@abv.bg

ANALYSIS OF THE EVOLUTION OF GLOBAL NAVIGATION SATELLITE SYSTEMS

Evgeni Gr. Stoykov

ABSTRACT: *The article analyzes the development of global navigation satellite systems used for military and civilian purposes.*

KEYWORDS: *Geodesy, GNSS.*

The widespread use of GNSS is an indisputable fact, and the need for them and their multilateral application is growing. While they were primarily used for military purposes at the beginning, the use and effectiveness of civilian life has now been demonstrated in everyday practice as well. This is a basic prerequisite for their development and improvement for civilian purposes. The originally designed for military purposes GPS and GLONASS systems are accessible to the civilian sector but are still dependent and controlled by the military. This necessitates new solutions, which lead to the development of existing and the construction of new, mostly continental, regional or national satellite navigation systems.

For the United States and Canada, the GPS system is developed as a comprehensive WAAS system. It is based on 25 precisely defined ground reference stations covering the US and Canada. The signals from GPS satellites are received by these reference stations, identifying any errors in them. All reference stations are interconnected and represent the WAAS network. Data from each station is sent to the main station where the corrections are calculated. These adjustments are transmitted to a geostationary communications satellite (GEO) where they can be received by GPS receivers at the same frequency as GPS signals for the respective territory. The creation of this system has two main objectives:

- The first is to give the user information on whether signals from separate GPS or GEO satellites can be used in the navigation solution;
- The second is to provide differential corrections to be applied to measurements to improve the accuracy of the situation.

Information about the ionosphere transmitted by the WAAS system is much more accurate than the GPS model. In addition, WAAS will be much more accurate than DGPS-based broadcasting, as the correction reflects remoteness from the reference station. GPS receivers only need to apply the appropriate corrections corresponding to their location [2].

EGNOS is the first European joint satellite navigation project between the European Commission, the European Commission (EC) and the European Organization for the Protection of Air Navigation, Eurocontrol (European Organization for the Safety of Air Navigation Eurocontrol), developing two GLONASS systems and GPS. The EGNOS system is a European version of WAAS. It consists of three geostationary satellites and a network of terrestrial reference stations which transmit a signal containing information on the reliability and accuracy of the signals sent by GLONASS and GPS [2].

This allows users in Europe and beyond to determine their position with accuracy of the order of 5 m and even up to 1 m. The main application of this system is air navigation and maritime navigation as well as road transport. It can be said that EGNOS is Europe's first step in the realization of GNSS and the predecessor of GALILEO. The system reaches its full operational capability in 2005. The system receives signals from Glonass and GPS satellites that are subject to corrections that improve accuracy to 2 m and better. Corrected signals are re-broadcast and transmitted to Inmarsat satellites. From there, they are transmitted to the receiver located in the appropriate means of transport to determine its position [2].

The GALILEO system, unlike EGNOS, is a stand-alone and independent system. It is designed entirely for civilian purposes and has a very wide range of applications. This system is designed as an alternative to the US GPS system to ensure user independence [2].

In essence, the GALILEO system is a global constellation of 30 mid-Earth satellites located in three orbital planes with an inclination at an angle of 56 ° to the equator at a height of 23,222 km from Earth. In each orbital plane, nine satellites will be equally spaced, each of which will travel around the Earth for 14 hours. In each orbital plane, there will be one additional hidden back-up companion to provide coverage in a malfunctioning satellite in the corresponding plane.

Satellite operations will be supported by a network of ground stations consisting of observation stations, control centers and base stations for uplink to the satellite. A global network of GALILEO observation stations will continuously monitor the satellites. Exactly measured navigation signals will be sent to two GALILEO Control Centers in Europe to be processed. There, sophisticated software will determine satellite orbits and timing synchronization errors of satellite atomic clocks against the time of the GALILEO system maintained on the ground. Orbits and clock data will be loaded on satellites about every 2 hours for distribution to users who can use them in their positioning algorithms. This update frequency will ensure the high level of positioning accuracy required by the system. The control centers will also calculate the integrity data provided as part of the life safety service.

Integrity data will be loaded on satellites for distribution to consumers even more often than satellite orbital data and clocks. For alerts (e.g., malfunctions), the system will be able to alert users to a delay of only 6-10 seconds.

The transmission of data to and from the satellites will be via a global network of telemetry, telecommunication and tracking stations (satellite control and monitoring data) and mission base stations (bottom-up navigation data: orbits, clock errors , integrity).

Integrity data computed in the GALILEO Control Centers can be used by every user worldwide because they will be based on global network monitoring.

However, regional service providers will be able to deploy their own networks of observation stations in their own region to calculate the integrity of GALILEO alerts. These regional integrity data may be made available to users through GALILEO satellites authorized by the GALILEO Satellite Interoperability Channels. Alternatively, these data may be sent to GALILEO Control Centers for integration with centrally calculated integrity data.

The above-described features will be enhanced by local components by spreading local data over terrestrial radio links or over the existing communications network to provide additional accuracy, integrity or extended coverage around airports, ports, railways and urban areas. Local components will also be deployed to extend the coverage of navigation services and to include in-house users.

The GALILEO system will transmit 10 signals: six of them will serve the free service and the safety of life service (although some of them can also be used for the commercial service), two will be for commercial service and two for the public regulated service. They will be transmitted in the following frequency bands:

- E5A-E5B (1164-1215 MHz) and E6 (1260-1300 MHz) allocated to the Radiocommunication Service (RNSS) at the 2000 World Conference in Istanbul;
- E2-L1-E1 (1559-1591 MHz) have already been allocated to the RNSS before the World Radio Conference in 2000 and are used by GPS. The co-location of this GPS band will take place under conditions of discomfort to prevent the current GPS services being interrupted, while users will simultaneously gain access to both GPS and GALILEO while minimizing the cost and complexity of the terminal.

GALILEO navigation signals will consist of distance codes and data messages. The data messages will include a satellite clock, an ephemeris, a flag for identification and a status of the spacecraft, and information about the constellation of the cosmic almanac. It will also include the "cochieve signal

accuracy" parameter, which will offer users a satellite timing prognosis and accuracy over time. The data messages will also include integrity data, determined centrally on the basis of measurements from the global observation network that monitors the constellation of GALILEO satellites and when there is regional integrity data.

GALILEO will provide the following different navigation services:

- The Free Service (FS) will be free to all users. FS signals will be broadcasted in two frequency bands, 1164-1214 MHz and 1563-1591 MHz. Receivers will reach <4 m maximum horizontal accuracy and <8 m maximum vertical accuracy if they use both FS bands. Single-band receivers will have <15 m horizontal and <35 m vertical accuracy, which is comparable to the GPS-provided civilian signal.
- The encrypted Commercial Service (CS) will be provided for a fee and will have an accuracy of less than 1 m. The CS will also be complemented by transmitters located on the ground, which has the potential to increase accuracy to less than 10 cm. The signal will be broadcast in three frequency bands: the two bands from the CS and the 1260-1300 MHz band.
- The encrypted Public Regulated Service and Safety of Life Service (SoL) will provide precision comparable to the FS. Their goal is resistance to mute and reliable detection of problems within 10 seconds of their occurrence. The market for these services will be limited to power authorities (police, military, etc.) as well as transport services where signal quality is of great importance (air control, automatic landing of airplanes, etc.)

An important aspect of the GALILEO concept is the provision of revenue generating services for which data transmission is an important element. A range of data rates of up to 1000 characters per second are considered, which will maximize the potential of value-added services such as climate abnormality warnings, incident alerts, traffic information, and card updates.

GALILEO is a system designed primarily for civilian use, unlike the US military-supported GPS. The US reserves the right to reduce the signal strength or accuracy of the system, or to completely exclude public access to it in the event of a conflict. Until 2000, GPS accuracy was deliberately reduced for civilian needs (a process called selective access). The European system, which cannot be switched off (although it can be silenced), will provide a significant improvement in GPS signal, providing full precision to both civilian and military users.

The BeiDou Navigation Satellite System (BDS) is a Chinese satellite navigation system. It consists of two separate satellite constellations - a limited test system that has been in operation since 2000 and a full-scale (global) global navigation system currently under construction [7].

The first Beidou system, officially called the BeiDou Satellite Navigation Experimental System, also known as Beidou-1, consists of four satellites (three working and one backup) and offers limited scope and applications. It offers navigation services, mainly for customers in China and neighboring regions since 2000.

The second-generation system, officially called the BeiDou Satellite Navigation System (BDS), also known as COMPASS or Beidou-2, will be a 35-satellite global satellite navigation system under construction from January 2013 Launched in December 2011 with 10 satellites in China and began to offer service to users in the Asia Pacific region in December 2012. Global use is foreseen after its completion in 2020.

Unlike the American system GPS, Russia's GLONASS and the European Galileo system, using satellites in medium Earth orbit, Beidou-1 uses satellites in geostationary orbit. This means that the system does not require a large constellation of satellites but also limits the scope of the Earth's areas where the satellites are visible. The area that can be serviced is of longitude 70 ° E to 140 ° E and latitude 5 ° N and 55 ° N. The frequency of the system is 2491.75 MHz. In 2007, Xinhua's official agency reported that the decision of the Beidou system was of the order of 0.5 meters, and the accuracy of the system with the existing consumer receivers ranged in the order of 20 meters [7].

Beidou-2 (known as COMPASS) is not an extension of the older Beidou-1, but rather will replace it definitively. As we said above, the new system will be a constellation of 35 satellites that include 5 GEO satellites for backward compatibility with Beidou-1 and 30 non-geostationary satellites (27 in mid-earth orbit and 3 in sloping geostationary orbit, MEO) that will offer full coverage of the globe. Like other GNSS, there will be two levels of service: free service and limited (military).

China's representatives have also said that issues related to frequency bands have yet to be settled with Russian, American and European countries that also have satellite navigation clusters. And so far, the Chinese system has been operating at the frequency of the B1 signals, marked by the EU as E2, at a frequency of 1559,052-1591,788 MHz. The two countries have not yet reached a final agreement on the compatibility issues of their future satellite navigation systems despite the ongoing 2009 negotiations on the superposition of special Compass signals on the special PRS signals of the Galileo system (range L1, center frequency 1575.42 MHz).

Assumed frequencies are: B2: 1166.22 - 1217.37 MHz, B3: 1250.618 - 1286.423 MHz.

The Indian Regional Navigation Satellite System (IRNSS) is an Indian regional satellite navigation system, the project of which was adopted by the

Government of India. The development is carried out by the Indian Organization for Cocical Research (ISRO). The system will provide only regional coverage of India itself and parts of neighboring countries.

- Total amount of IRNSS satellites: 7.
- Design date for completion: 2015

Structure: The IRNSS satellite group should consist of seven satellites of geosynchronous orbits at an altitude of about 24,000 km in apogee. In addition, four of the seven IRNSS satellites will be displaced in orbit with an angle of 29 ° with respect to the equatorial plane. All seven satellites will have continuous radio visibility with the Indian control stations.

The IRNSS Earth Segment will have a monitoring station, tracking station, control station and onboard controls. The state-owned company ISRO is responsible for the IRNSS, which will be entirely under the control of the Indian government. The navigation receivers that will receive the IRNSS alerts will also be developed and produced by Indian companies.

IRNSS suggests that the coordinates of the site are accurate to the order of 20 meters for the Indian Ocean region (about 1,500 kilometers around India) and less than 10 meters - directly in India and the territories of the neighboring countries covered by the navigation system.

India launched its first navigational satellite in orbit on July 1, 2013, and has already successfully transmitted signals to Earth.

Conclusion

The widespread use of GNSS is a dispassionate fact and the need for them is growing. For surveying purposes, the multichannel receivers are capable of receiving signals from many satellites at the same time. Upgrading and introducing additional GPS signals improves user accuracy and accessibility. With the introduction and development of permanent geodetic networks, measurements in RTK mode become much faster and more accurate.

REFERENCES:

1. Стойков Е., Изследване на възможността за използване на двучестотен GPS приемник в режим RTK за създаване на РГО, заснемане и трасиране на обекти. Дисертационен труд, Шумен 2015.
2. Милев Г., Вълев Г., Минчев М., Матова М., Василева К., Гъбенски П. Европейската референтна система в България, София, 2006.
3. Михайлов Пл., Държавна GPS мрежа на Република България – настояще и бъдеще, Научна сесия с международно участие МАТТЕХ 2010, ШУ "Епископ Константин Преславски".
4. Иванов С., Извод на формула за изчисляване на началния посочен ъгъл, при решаване на обратна засечка чрез синусите и косинусите на измерените

хоризонтални ъгли, научна сесия с международно участие МАТТЕХ 2016, ШУ "Епископ Константин Преславски".
5. Иванов С.,Кастрева П.,Безинска К.-Проблемни ситуации в състоянието и експлоатацията на обектите на културното наследство, научна сесия с международно участие МАТТЕХ 2016, ШУ "Епископ Константин Преславски".
6. Иванов С., Сравнителен анализ на геодезически системи БГС 2000 и БГС 2005, научна сесия с международно участие МАТТЕХ 2014, ШУ "Епископ Константин Преславски".
7. Михайлов Пл., "Съвместно изравнение на геодезически и GPS измервания върху повърхността на елипсоида", НВУ "Васил Левски", " Факултет "А, ПВО и КИС" - Шумен,Научна сесия, 2004.
8. Михайлов Пл., "Ръководство за упражнения по геодезични мрежи" – Учебно пособие; Шуменски университет „Епископ Константин Преславски", 2007.
9. Михайлов Пл., Андреев А.," Обучението в специалност „Геодезия" в ШУ. сп. "Геодезия, картография, земеустройство", 2017 г.
10. Андреев А., Кирилова Кр. Изследване на ефективността на гравиметричните построения по МНМК. Годишник на ШУ "Еп. К. Преславски" Технически науки т.IVE, стр. 73-85, 2015 г.
11. Андреев А., Съвременни методи за локално моделиране на геоида. 162 с. НВУ "В.Левски" – Шумен, ВТС, 2008.
12. URL:https://en.wikipedia.org/wiki/BeiDou_Navigation_Satellite_System.

Author's name: Chief Assistant eng. Evgeni Stoykov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Geodesy
E-mail: e.stoykov@shu.bg

ANALYSIS OF GEODETIC NETWORKS

Evgeni Gr. Stoykov

ABSTRACT: *The article analyzes the networks used for working surveying, surveying and tracing.*

KEYWORDS: *Geodesy planar, height.*

Depending on the size of the space in which they are identified, the geodetic networks can be one-dimensional (height), two-dimensional (planar) and three-dimensional (spatial).

To determine the coordinates of a certain number of points in a particular coordinate system, it is necessary to make dimensional measurements by which the coordinates of the points can be calculated. The number of measurements that connect two points depends on the size of the network. For single-dimensional networks, one measurement is sufficient, two-dimensional - two, and three-dimensional - three. Geodetic networks usually perform more than the minimum number of measurements required. Results processing is most often done using the Smallest Squares Method, resulting in a uniquely accurate estimate.

For elevated nets, weights are measured between the points, which can be done by geometric, trigonometric or hydrostatic leveling.

Two measured values are sufficient to determine a point in the plane. Such may be two lengths, two angles or an angle and a length. Horizontal angles, as known, are defined as a difference in two directions. In trilateral networks, measurements are only long, and in triangular ones only angular. The combination of linear and angular measurements is preferable in geodetic networks due to the higher accuracy and compactness of the buildings.

When point coordinates are determined by satellite measurements, spatial chords (vectors) between points are used. Satellite measurements in geodesy are relative. They define the components of the spatial vector between two points representing co-ordinate differences.

One of the main purposes of geodetic networks is to materialize the terrain coordinate system in which it is being worked. In order to define the coordinate system, a certain number of dimensions, called defining parameters, need to be known.

When creating geodetic networks, you may have more than the required number of dimensions. For a height network, the minimum number of given dimensions is one - that is, the height of at least one point. For planets, the minimum required number of given dimensions is four. Depending on the type of network, they can be the coordinates of two points, the coordinates of one point, the given angle and base (for the triangular networks), the coordinates of a point and a given angle (for angular-line networks). For linear-angled networks, the scale of the mesh is determined by the measured lengths. Errors in output data affect the accuracy of determining all points in the new network.

The individual geodetic networks have the exact number of given dimensions. They are defined with sufficient precision, so their errors are negligible. In practice, local or height systems are defined.

With free geodetic networks, some dimensions may be missing. The solution thus obtained is used for specific tasks, and can then be applied to a stand-alone network (when some items are accepted) or included.

Geodetic networks can be single-class and multi-class. For single-row networks, all points are applied, measured, and aligned. For multi-class networks, building is by classes, with each subsequent class being included in the previous one. For multiple class networks, the relative error decreases rapidly when switching to a lower class, which in some cases is a drawback of this type of network.

Prior to proceeding with activities to create a working geodetic base, geodetic surveying and tracing of objects, it is necessary to assess the condition of the supporting geodetic network. For the unity of all geodetic measurements in solving different scientific and practical tasks, for the creation of plans, maps and digital models, a uniform geodetic basis is laid on the territory of the country. This role is implemented by the state geodetic networks.

Geodetic network is the set of points stabilized on the ground, the position of which is determined in a single coordinate and height system (x, y and H).

Geodetic networks by nature are determined by many factors that determine their diversity in the end. The main factor is the accuracy they have to satisfy when they are used to solve different scientific and applied tasks. An important factor is also the nature of the terrain in terms of the configuration of the terrain and the size of the area on which geodetic networks are being built.

When creating geodetic networks, the principle of "general to private" must be respected, ie. should go from "big to little". On the basis of this

principle, geodetic networks of general interest are created first with the highest accuracy.

For specific purposes of creating topographical plans and maps for a given area, the state support geodetic networks in it are compacted by locally based geodetic networks - their accuracy is less than that of the state networks.

Thus compressed geodetic networks are in most cases insufficient for detailed capture. They are supplemented to the required density with an additional network of points that form the so-called working geodetic basis. It is uniform for horizontal and vertical measurements, with certain coordinates and heights of the points. Depending on the object, the scale of the plan, the topographic conditions, the selected method of capture and a specific tool for operation, its density, shape and accuracy are determined. The points of the supporting and working geodetic bases form the shooting base from which a geodetic capture is made to create a plan, map or digital topographic model. Thus geodetic networks are determined by their division into:

- ✓ State geodetic network (State GPS network);
- ✓ Geodetic networks for local use;
- ✓ Scenic (working) geodetic networks.

The main classical methods used to plan the basic geodetic networks in the recent past are triangulation, polygonometry, trilation, and combinations between them, depending on the nature and coverage of the earth's surface. Nowadays GNSS measurements (cosmic triangulation) are widely used for the installation of basic geodetic networks.

Conclusion

By establishing the satellite navigation methods in geodesy, it is possible to create a modern, unified and accurate geodetic coordinate system on a global and regional scale. This allows the application of GNSS technologies in the creation of geodetic networks, surveying and tracing of objects.

REFERENCES:

1. Стойков Е., Изследване на възможността за използване на двучестотен GPS приемник в режим RTK за създаване на РГО, заснемане и трасиране на обекти. Дисертационен труд, Шумен 2015.
2. Русев Б. Основни геодезични мрежи. София, Техника, 1989.
3. Михайлов Пл., Държавна GPS мрежа на Република България – настояще и бъдеще, Научна сесия с международно участие МАТТЕХ 2010, ШУ "Епископ Константин Преславски".
4. Иванов С., Извод на формула за изчисляване на началния посочен ъгъл, при решаване на обратна засечка чрез синусите и косинусите на измерените

хоризонтални ъгли, научна сесия с международно участие МАТТЕХ 2016, ШУ “Епископ Константин Преславски”.
5. Иванов С.,Кастрева П.,Безинска К.-Проблемни ситуации в състоянието и експлоатацията на обектите на културното наследство, научна сесия с международно участие МАТТЕХ 2016, ШУ “Епископ Константин Преславски”.
6. Иванов С., Сравнителен анализ на геодезически системи БГС 2000 и БГС 2005, научна сесия с международно участие МАТТЕХ 2014, ШУ “Епископ Константин Преславски”.
7. Михайлов Пл., Петров Д., "Съвременни технически средства и технологии за събиране на геопространствени данни за местността", ШУ “Епископ Константин Преславски”, монография, 2014.
8. Михайлов Пл., ”Ръководство за упражнения по геодезични мрежи“ – Учебно пособие; Шуменски университет „Епископ Константин Преславски“, 2007.
9. Андреев А., Съвременни методи за локално моделиране на геоида. 162 с. НВУ ”В.Левски” – Шумен, ВТС, 2008.
10. Андреев А., Андреева П. "Локално моделиране на геоида за територията на Североизточна България", Научна конференция с международно участие МАТТЕХ 2010, ШУ “Епископ Константин Преславски”, 2010 г.
11. Андреев А., Андреева П. "Анализ на системите височини от гледна точка на физическата геодезия и приложението им в Р. България.", Научна конференция с международно участие МАТТЕХ 2010, ШУ “Епископ Константин Преславски”, 2010 г.

Author’s name: Chief Assistant eng. Evgeni Stoykov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Geodesy
E-mail: e.stoykov@shu.bg

ANALYSIS AND EVALUATION OF GNSS METHODS IN GEODESY

Evgeni Gr. Stoykov

ABSTRACT: *The article analyzes and assesses the GNSS methods used in geodesy.*

KEYWORDS: *Geodesy, GNSS, RTK.*

For the determination of geodetic points and traceability, relative phase GNSS methods are applied. In cases where accuracy of 0.5 m or less is required, differential code methods may also be applied. Depending on the operability of their application, methods for determining geodetic points can be performed [8]:

- ✓ in real time;
- ✓ with subsequent processing.

In order to implement the said methods, satellite navigation signals are received and processed. The following GNSSs are applicable:

1. GPS;
2. GLONASS, Galileo and others - depending on their current status and the capabilities of the available equipment.

The primary data received from the navigation of the observed satellites is:

- ✓ Pseudo-distances measured using one or more PRN codes;
- ✓ Phase measurements of one or more carrier frequencies;
- ✓ Predicted data on orbits, time scales, ionosphere status, satellites, etc. When a post-processing method is used, the primary data from the signal processing is recorded in the memory of the receiving apparatus.

GNSS measurements are made at geodetic points that meet all the common requirements for site selection, the way to stabilize and benchmark, the visibility to other points, and native subjects stemming from applicable normative documents.

Depending on the role of the points in the measurement scheme differ:

- ✓ Base stations;
- ✓ Determinable points;

Depending on the available data and their purpose, some of the points may be [8]:

✓ Output points, with coordinates and heights set in a geodetic coordinate system, which serve to determine the results of GNSS measurements in this system;

✓ Transformation points, with coordinates and heights set in a local coordinate system, which serve to determine the results of GNSS measurements in this system through a transformation path.

For the implementation of geodetic GNSS methods it is necessary to carry out simultaneous measurements of one base station and one determinable point, in which:

1. The measurements of the base stations are continuous and continue all the time until measurements are made at the destination points;
2. The measurements of the set points are with a duration specific to the applied GNSS method and the type of work performed.

When using GNSS real-time methods, base stations coincide with exit points [8]. In the 1980s, second-generation satellite radionavigation systems emerged in the field of space technologies. These are the NAVSTAR (GPS) systems - developed by the US and GLONASS (Global Navigation System) - developed by the USSR and then by Russia. Over time, a more common name for the NAVSTAR system was GPS (Global Positioning System). The common names of these systems also use Satellite Radio Navigation Systems (SRNS) and Global Navigation Satellite Systems (GNSS).

Global navigation satellite systems consist of a part (24 satellites for GPS and GLONASS systems), a ground station (control stations) and a receiver (receiver). The satellites move on orbit orbits at an altitude of about 20,000 km. Each satellite continuously gives a signal containing information about the location of the satellite, exact time and codes to measure distances between satellites and receivers [2], [3].

Determining the coordinates of the receiver is done by measuring pseudo-space to satellites and calculating a spatial linear fault. At the present stage of development, global satellite navigation systems are mainly used in two directions - navigational and geodetic.

Navigation uses different types of navigation receivers, each working independently. Pseudo-distances to codec and phase satellites are measured. In a single measurement the accuracy of the coordinates is 1-15 m. The use of GNSS for navigation purposes is widely used in many areas of human activity but, for geodesy, it does not represent a serious practical interest. For geodetic purposes, special geodetic receivers are being developed. They can be different in terms of options, way of management and purpose.

The main difference between navigation and geodetic measurements using GNSS is that in navigation, the measurement is absolute (each receiver works independently and coordinates coordinates in a single, Cartesian,

geocentric coordinate system). In geodetic measurements, relative determinations are made, which define the components of the spatial vector between two points, also in a unified Cartesian, geocentric coordinate system. Relative measurements are made by observing the same satellites simultaneously from two receivers located at the points between which a spatial vector is measured.

The use of GNSS for geodetic purposes began almost with their creation, but with their development, especially in recent years, GNSS has found a wider and broader application in geodesy. In addition, new types and models of receivers are refined and developed, measuring methods and technology are improved, more attention is paid to the processing and presentation of results. All this is due to a number of advantages of satellite technology, some of which are:

- ✓ As a result of the development of GNSS, it is possible to achieve high accuracy sufficient for many types of geodetic activities;
- ✓ High performance;
- ✓ There is no mandatory visibility between the set points;
- ✓ Opportunity for kinematic measurements;
- ✓ Determination of spatial coordinates;
- ✓ Almost complete independence from weather conditions;
- ✓ High degree of automation.

Along with the advantages presented, GNSS is not universal and has certain shortcomings, the more significant of which are:

- ✓ Dependence on non-radio frequency barriers;
- ✓ Inability to work underground and indoors;
- ✓ Accuracy for height determination is 2 to 5 times lower than for coordinate determination;
- ✓ Problem with transformation of geodesic heights into normal;
- ✓ High cost of equipment.

These deficiencies restrict the use of GNSS in certain situations, while in others they require the development of a special technology for measuring and processing the results. The GPS receiver manufacturers tend to reduce the size of the equipment. This is another important factor, as the equipment is easier to carry, easier and safer to use.

Conclusion

The results obtained from measurements in GPS networks are subject to mathematical processing (alignment). Before converting to alignment, it is necessary to align the coordinate systems, i. to introduce a single coordinate system. This is done by taking out points from the State GPS network and / or stations from GNSS infrastructure, at least three in number.

REFERENCES:

1. Стойков Е., Изследване на възможността за използване на двучестотен GPS приемник в режим RTK за създаване на РГО, заснемане и трасиране на обекти. Дисертационен труд, Шумен 2015.
2. Хофман-Веленхоф Б., Лихтенегер Х., Колинс Дж. Глобална система за определяне на местоположение: Теория и практика. Превод от английски, София, УАСГ, 2002.
3. Антонович, К. М. Использование спутниковых радионавигационных систем в геодезии, том I. Москва, ФГУП „Картгеоцентр", 2005.
4. Михайлов Пл., Държавна GPS мрежа на Република България – настояще и бъдеще, Научна сесия с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски".
5. Иванов С., Извод на формула за изчисляване на началния посочен ъгъл, при решаване на обратна засечка чрез синусите и косинусите на измерените хоризонтални ъгли, научна сесия с международно участие MATTEX 2016, ШУ "Епископ Константин Преславски".
6. Иванов С.,Кастрева П.,Безинска К.-Проблемни ситуации в състоянието и експлоатацията на обектите на културното наследство, научна сесия с международно участие MATTEX 2016, ШУ "Епископ Константин Преславски".
7. Иванов С., Сравнителен анализ на геодезически системи БГС 2000 и БГС 2005, научна сесия с международно участие MATTEX 2014, ШУ "Епископ Константин Преславски".
8. Инструкция № РД-02-20-25 от 20 септември 2011 г. за определяне на геодезически точки с помощта на глобални навигационни спътникови системи. Издадена от Министерството на регионалното развитие и благоустройството, Обн. ДВ. бр.79 от 11 Октомври 2011 г.
9. Михайлов Пл., Петров Д., "Съвременни технически средства и технологии за събиране на геопространствени данни за местността", ШУ "Епископ Константин Преславски", монография, 2014.
10. Михайлов Пл., "Ръководство за упражнения по геодезични мрежи" – Учебно пособие; Шуменски университет „Епископ Константин Преславски", 2007.
11. Андреев А., Съвременни методи за локално моделиране на геоида. 162 с. НВУ "В.Левски" – Шумен, ВТС, 2008.
12. Андреев А., Андреева П. "Локално моделиране на геоида за територията на Североизточна България", Научна конференция с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски", 2010 г.
13. Андреев А., Андреева П. "Анализ на системите височини от гледна точка на физическата геодезия и приложението им в Р. България.", Научна конференция с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски", 2010 г.

Author's name: Chief Assistant eng. Evgeni Stoykov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Geodesy
E-mail: e.stoykov@shu.bg

METHODS FOR DETERMINING PLANE RECTANGULAR COORDINATES OF TOPOGRAPHIC MAP POINTS

Sabin I. Ivanov

ABSTRACT: *The article analyzes the methods for determining plane rectangular coordinates of topographic map points.*

KEYWORDS: *Coordinates, map, plane.*

Plain rectangular coordinates are linear values (the X-line and the Y-ordinate) defining the position of points in the plane (map) relative to two mutually perpendicular lines (coordinate axes).

For coordinate axes, the image of the axial meridian of the coordinate zone (abscissa axis X) and the image of the equator (ordinate axis Y) are taken - Fig.1.

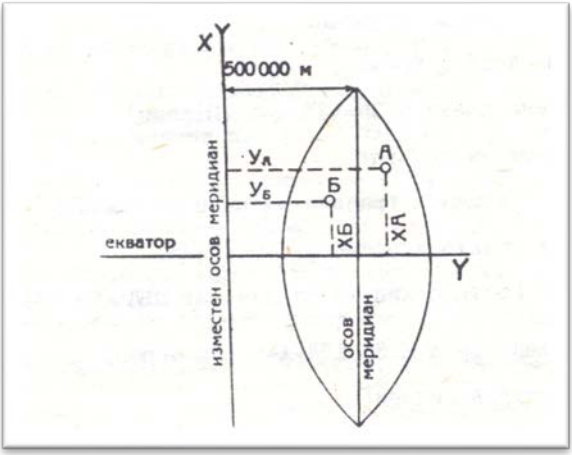

Fig.1. Flat rectangular coordinates

In order not to work with negative values, it is conditionally assumed that the value of the ordinate Y of the axial meridian of each zone is equal to 500 km.

Since in each zone the numerical values of the ordinates are repeated, then in order to be able to determine the coordinates of the point in which area it is located, the area number is entered to the left before the value of the ordinate.

The mileage lines closest to the corners of the leaf frame are labeled with the full number of kilometers, and the others are the last two digits. For example, the figure 4462 on the southernmost horizontal line means that this line is 4462 km north of the equator.

The figure 5256 of the most extreme western vertical line means that it is in the fifth zone and is located 256 km from the abscissa or 244 km (500-256 = 244) west of the axial meridian of the zone.

1.Determining Rectangular Coordinates of a Point on Map:

- by measuring distances (Fig.2);

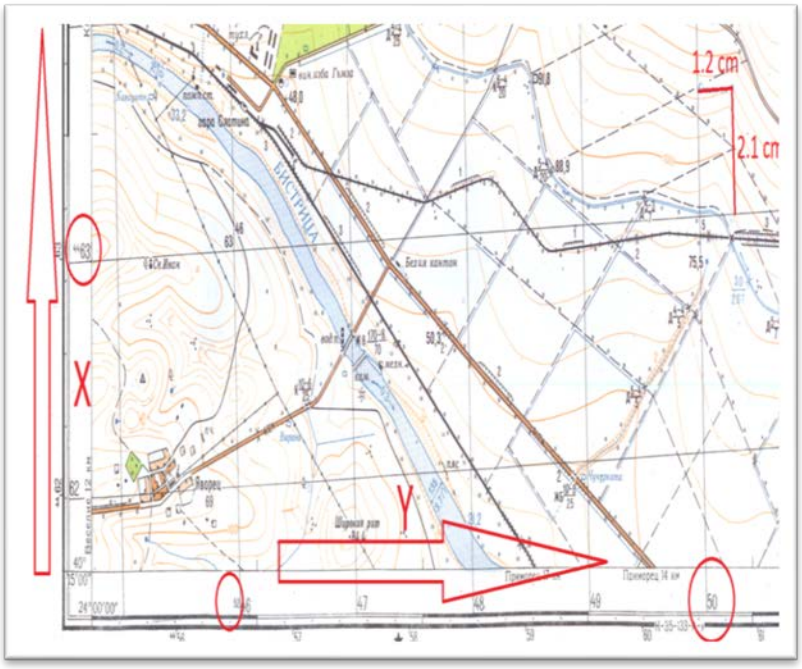

Fig.2. Determination of X and Y by measuring distances

To determine Y at a given point, the figure for the nearest western vertical line is taken: for example, 5250. A perpendicular to the given point is

then drawn from the reading line and its length in cm is measured, for example 1.2 cm. Having a map scale (e.g., 1: 25,000), we know 1 cm of it, how many meters of the site it responds to (for example, 1: 25,000 scale, 1 cm of the map corresponds to 250 m from the area). The measured length (1.2 cm) is multiplied by 250 m. The value so obtained (300 m) is added to the figure of the closest western vertical line. Since the reported figure (5250) is in km (see point 1), it must be converted into meters (5250 km x 1000 m = 5250000 m). As the final result for Y of point M we get:

$$Y_M = 5250000 + 300 = 5250300 \text{ m.}$$

To determine X at a given point, the figure for the nearest southern horizontal line is taken: for example, 4463. A perpendicular to the given point is then drawn from the reading line and its length in cm is measured, for example 2,1 cm. Having a map scale (e.g., 1: 25000), we know 1cm from it, how many meters from the area it responds to (for example, 1: 25000 scale, 1cm of map corresponds to 250m from the area). The measured length (2.1 cm) is multiplied by 250 m. The value thus obtained (525 m) is added to the figure on the nearest southern horizontal line. Since the reported figure (4463) is in km (see point 1), we have to convert it in meters (4463 km x 1000 m = 4463000 m). As the final result for X of point M we obtain:

$$X_M = 4463000 + 525 = 4463525 \text{ m.}$$

- with a ten-centimeters ruler (Fig.3);

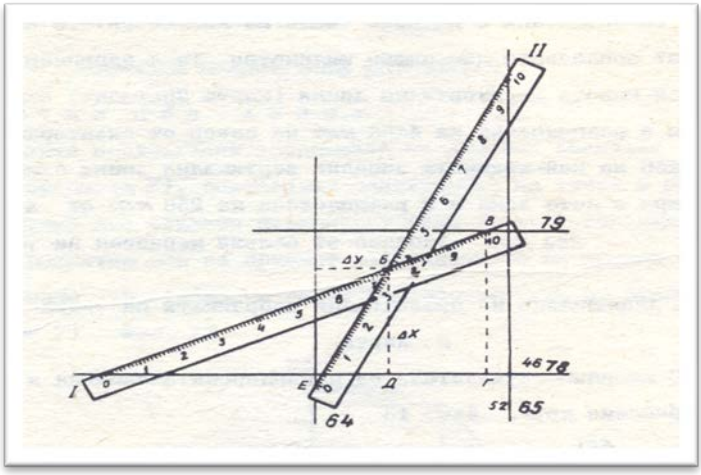

Fig.3. Determination of X and Y with a ten-centimeters ruler

To determine X at a given point, the figure of the nearest southern horizontal line is taken into account: eg 4478. We set the zero of the rudder to the nearest southern horizontal line and the tenth to the nearest northern horizontal line. Slide the rump until it passes through the point. We report in mm and multiply by 10. Example: We report 75 mm - 75x10 = 750 m. The value so obtained (750 m) is added to the figure on the nearest southern horizontal line.

$$XM = 4478000 + 750 = 4478750 \text{ m.}$$

To determine Y at a given point, the figure of the closest western vertical line is reported: for example, 5264. Set the rudder zero to the closest western vertical line and the tenth to the closest eastern vertical line. Slide the ruler until it passes through the point. We report in mm and multiply by 10. Example: we measure 37mm - 37x10 = 370m. The value so obtained (370 m) is added to the figure of the closest western vertical line.

$$YM = 5264000 + 370 = 5264370 \text{ m.}$$

Conclusion

The methods for determining the planar rectangular coordinates of topographic map points are easy to perceive. The methods are convenient for use in field conditions as they do not require any specialized equipment.

REFERENCES:

1. Андреев А., Михайлов Пл., Стойков Е., "Сравнителен анализ на получените резултати от височинни измервания по различни методи", Научна конференция с международно участие MATTEX 2016, ШУ "Епископ Константин Преславски".
2. Стойков Е., "Модернизация и въвеждане на допълнителни GPS сигнали", научна конференция с международно участие MATTEX 2014, ШУ "Епископ Константин Преславски".
3. Кастрева П. Географски информационни системи и компютърна картография. Университетско издателство "Неофит Рилски", гр.Благоевград, 2011г.
4. Plamen Mihajlov, Evgeni Stoykov, 'Evaluation of the accuracy of measurements with dual-frequency GPS receiver Trimble R4 in the RTK (Real Time Kinematics) mode', International conference on Bionics and Prosthetics, Biomechanics and mechanics, mechatronics and robotics, June 17-21, 2013, Riga, Latvia, 2013 г.
5. Иванов С., Ръководство за работа с топографска карта, Университетско издателство „Епископ Константин Преславски", Шумен 2018.

Author's name: chief assistent Sabin Ivanov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Geodesy"
E-mail: s.ivanov@shu.bg

METHODS FOR DETERMINING AREAS ON TOPOGRAPHIC MAPS

Sabin I. Ivanov

ABSTRACT: *The article analyzes the methods for determining areas on topographic maps*

KEYWORDS: *Coordinates, map, plane, areas.*

One of the main tasks that can be done on topographic maps is to define areas. Used for large areas with clearly defined boundaries.

Several ways of plotting are used: by plane (rectangular) coordinates of angular points, graphical, analytical (geometric) and mechanical (using a planner).

1. Determination of area by rectangular coordinates of corner points. Used for areas whose outlines are straight lines.

- number the corner points of the figure clockwise;
- the rectangular coordinates (X and Y) of all points are determined;
- by the given formulas (1 and 2) the area of the figure (for control in both formulas) is calculated.

$$P' = \frac{1}{2}\left[X_i \cdot \left(Y_{i+1} - Y_{i-1}\right) + X_{i+1} \cdot \left(Y_{i+2} - Y_i\right) + ... \right] \qquad (1)$$

$$P'' = \frac{1}{2}\left[Y_i \cdot \left(X_{i-1} - X_{i+1}\right) + Y_{i+1} \cdot \left(X_i - X_{i+2}\right) + ... \right] \qquad (2)$$

i - the number of the first point;

(i - 1) - the last point number.

Example: Specify the area of the vineyard mass, shown in Figure 1, by the coordinates of the corner points.

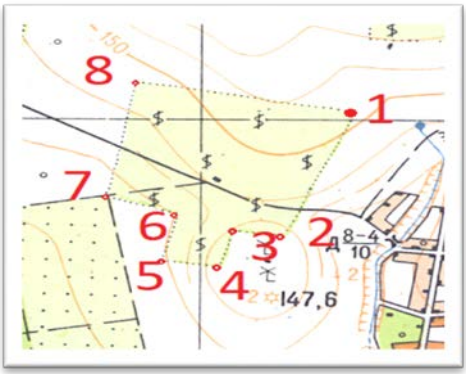

Fig.1. Vineyard massif

- number the angles of the figure (clockwise) - from 1 to 8;
- define rectangular coordinates:

1. X1 = 4465025 m; Y1 = 5248362.5 m;
2. X2 = 4464612.5 m; Y2 = 5248200 m;
3. X3 = 4464625 m; Y3 = 5248075 m;
4. X4 = 4464500 m; Y4 = 5248050 m;
5. X5 = 4464525 m; Y5 = 5247900 m;
6. X6 = 4464687.5 m; Y6 = 5247950 m;
7. X7 = 4464750 m; Y7 = 5247712.5 m;
8. X8 = 4465125 m; Y8 = 5247837.5 m;

- we calculate the area twice by formulas (1) and (2):

P = ½. [4465025. (5248200-5247837,5) +4464612,5. (5248075-5248362,5 + 4464625. (5248050-5248200) +4464500. (5247900-5248075) +4464525. (5247950-5248050) +4464687,5. (5247712,5-5247900) +4464750. (5247837,5-5247950) +4465125. (5248362,5-5247712,5)] = 239843,75 m^2;

P = ½. (4465025-4464612,5) +5248200. (4465025-4464625) +5248075. (4464612,5-4464500) +5248050. (4464625-4464525) +5247900. (4464500- 4464687,5) +5247950. (4464525-4464750) +5247712,5. (4464687,5-4465125) +5247837,5. (4464750-4465025)] = 239843,75 m^2.

2. Analytical way of determining areas. This way, as well as the previous one, is used in areas whose outlines are straight lines.

- we designate the tops of the area figure with appropriate markings (A, B, C, etc.);

- divide the territory into smaller geometric shapes (triangle, parallelogram, trapezoid, square, etc.);

- using the formulas for the faces of the resulting geometric figures, we calculate the area of each figure;

1. Face of triangle - $S = \frac{a.h_a}{2} = \frac{b.h_b}{2} = \frac{c.h_c}{2}$;

2. Parallel face - $S = a.h_a = b.h_b$;

3. The face of the trapeze - $S = \frac{(a+b).h}{2}$;

4. Rectangle face - $S = a.b$;

5. Face of a square - $S = a.a = a^2$;

- we sum the areas of all shapes and get the area of the given territory.

Example: Determine the area of the vineyard mass shown in Figure 2 in an analytical way.

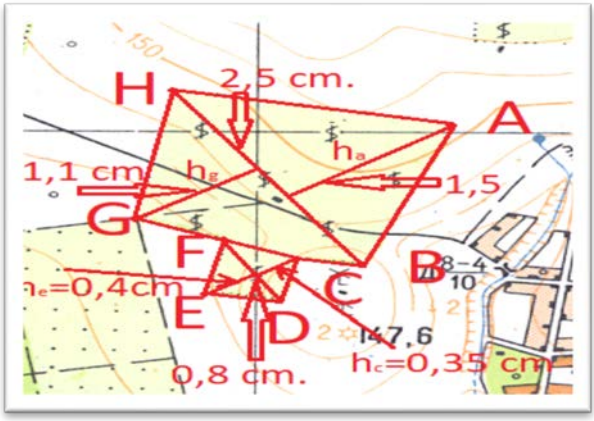

Fig.2. Analytical way of determining areas

- denote the arcs of the array - A, B, C, D, E, F, G and H;

- divide the array into smaller geometric shapes, as shown in Figure 2. We get - ΔABH, ΔBGH, ΔCDF and ΔDEF;

- In order to calculate the figures in the figures, several measurements should be made:

• Measure distances SHB = a = g = 2.5 cm. 250 m = 625 m (common side for the two triangles ΔABH and ΔBGH) and SDF = c = e = 0,8 cm. 250 m = 200 m (common side for the two triangles ΔCDF and ΔDEF);

• Measure the height in each triangle: ΔABH - ha = 375 m; ΔBGH - hg = 275 m; ΔCDF - hc = 87.5 m; ΔDEF - he = 100 m;

• Calculate the areas of the triangles:

ΔABH - P1 = (a.ha) / 2 = (625,375) / 2 = 117187,5 m^2;

ΔBGH - P2 = (g.hg) / 2 = (625.275) / 2 = 85937.5 m^2;

ΔCDF - P3 = (c.hc) / 2 = (200.87,5) / 2 = 8750 m^2;

ΔDEF - P4 = (e.he) / 2 = (200,100) / 2 = 10000 m^2;

- Sums P1, P2, P3 and P4 - 117187,5 + 85937,5 + 8750 + 10000 = 221875 m^2;

3. Graphic way of determining areas.

This method is very rarely used because it is very inaccurate - it provides approximate results.

- We break a sheet of transparent paper on the same squares with a side of 1 cm;

- We have a pause on the figure whose area we are looking for and counting all the squares that fall into the figure. Subsequently, the non-target squares are counted, and in the estimation of the compiler they are combined in whole squares;

- The resulting number of squares is multiplied by the face of one square. We know that, depending on the scale of the map, the scale is different. The squares labeled on a square have a side 1 cm - the face of the square - the scale number raised to the second degree

4. Mechanical way of determining areas

This is also rarely used, as we need a planner.

Planimetry is a device for measuring the face of figures, bounded by any closed loop, by crawling with their leading edge contours on a drawing, a plan, a map.

When making topographical plans in M 1: 5000 and 1: 2000 the areas are calculated mainly by the graphical and mechanical method.

Conclusion

The methods for determining the determining areas on topographic maps are easy to perceive. They are convenient for use in field conditions as they do not require any specialized equipment.

REFERENCES:

1. Кастрева П. Географски информационни системи и компютърна картография. Университетско издателство “Неофит Рилски”, гр.Благоевград, 2011г.
2. Plamen Mihajlov, Evgeni Stoykov, 'Evaluation of the accuracy of measurements with dual-frequency GPS receiver Trimble R4 in the RTK (Real Time Kinematics) mode', International conference on Bionics and Prosthetics, Biomechanics and mechanics, mechatronics and robotics, June 17-21, 2013, Riga, Latvia, 2013 г.
3. Андреев А., Михайлов Пл., Стойков Е., "Сравнителен анализ на получените резултати от височинни измервания по различни методи", Научна конференция с международно участие MATTEX 2016, ШУ “Епископ Константин Преславски”
4. Стойков Е., "Модернизация и въвеждане на допълнителни GPS сигнали", научна конференция с международно участие MATTEX 2014, ШУ “Епископ Константин Преславски”
5. Иванов С., Ръководство за работа с топографска карта, Университетско издателство „Епископ Константин Преславски“, Шумен 2018.

Author’s name: chief assistent Sabin Ivanov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Geodesy“
E-mail: s.ivanov@shu.bg

METHODOLOGY FOR DETERMINING THE DIRECTION TO A POINT

Sabin I. Ivanov

ABSTRACT: *The article analyzes the methodology for determining the direction to a point.*

KEYWORDS: *Map, direction, magnetic, abscissa.*

Very often, when solving different tasks on the map and on the site, it is necessary to determine the direction (Fig.1)to a certain point in relation to some other direction - initial. The starting point is the most common:

- Geographical North (ГС) - The northern direction of the central axis meridian of the area (the map frame);
- Map North (КС) - positive direction of the abscissa (vertical mileage);
- Magnetic North (МС) - the northern direction of the magnetic meridian (the direction that the magnetic arrow of the compass points to).

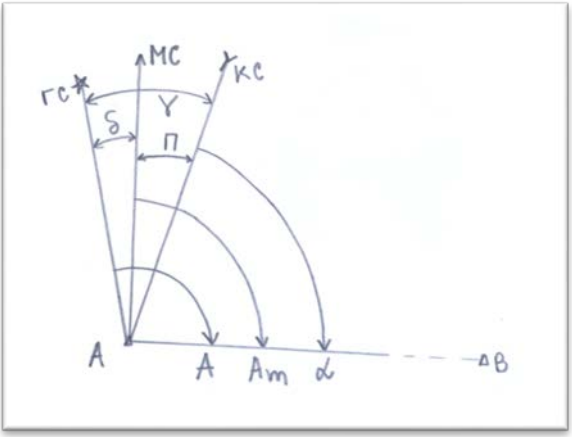

Fig.1. Types of north, angles between them and direction

When we determine the direction from one point to another, in relation to the given north, we distinguish three types of angles:

- Geo (real) azimuth - the angle recorded clockwise from the geographic north to a given direction. Marked - A;

- Specified angle - the angle recorded clockwise from the map north to a given direction. It is marked - α;

- Magnetic azimuth - the angle between the magnetic north and a given direction. Mark - Am.

Azimuths and pointed corners are straight and inverse. Reverse azimuth or pointed angle is equal to ± 180 °.

From the figure it can be seen that several angles are made between the initial or the main directions, namely:

- Meridian convergence (γ) - The angle between the geographic North and the Map North. To the east of the geographic north c there are positive values (+) and west negative (-);

- Magnetic Declination (δ) - The angle locked between the geographic north and the magnetic north. To the east of the geographical north, there are positive values (+) and west negative (-);

- Correction of direction (Π) - the angle locked between the magnetic north and the map north. To the east of the magnetic north, there are positive values (+) and west negative (-).

The dependencies between the azimuth and the pointed angle are as follows:

$$A = Am + (\pm\delta) \quad (1)$$

$$Am = A - (\pm\delta) \quad (2)$$

$$A = \alpha + (\pm\gamma) \quad (3)$$

$$\alpha = A - (\pm\gamma) \quad (4)$$

$$Am = \alpha + (\pm\Pi) = \alpha + (\gamma - \delta) \quad (5)$$

$$\alpha = Am - (\pm\Pi) = Am - (\gamma - \delta) \quad (6)$$

The data for γ, δ and Π are determined for the center of the card sheet and are given for the year of printing the card. Accordingly, in order to find the values of these angles for the required year, they have to be recalculated taking into account the annual variation of the magnetic deviation ($\Delta\delta_{1Y}$).

Operating mode

- Place the triangle perpendicular to the north or south frame, sliding as we pass through the point. We draw from the point in a north-line direction - Geographic North (ГС);

- set the triangle perpendicular to a horizontal mileage line, sliding as we pass through the point. We draw northward a second line - Map North (КС);

- with the transport operator, we take into account the actual azimuth (A) - the angle between (ГС) and the direction to a given point and the indicated angle (α) - the angle between (KC) and the direction to a given point;

- The data for the values of γ, δ and $\Delta\delta_{1Y}$ are reported from the text in the southwest field of each topographic map fig.2.

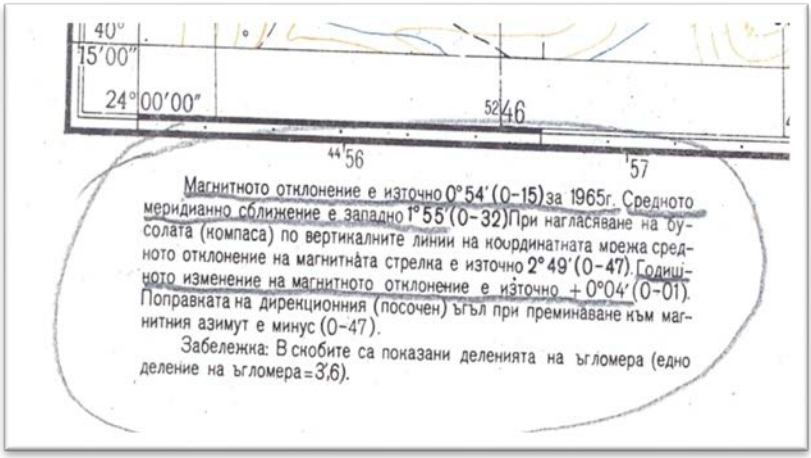

Fig.2. Reporting of δ, γ and Δδ1Y

- calculate δ for the desired year (δ_{2000}):

Example:

- we estimate γ = -1 ° 55 '
- we note δ_{1965} = + 0 ° 54 '
- we report $\Delta\delta_{1Y}$ = + 0 ° 04 '
- δ_{2000}-δ_{1965} = δ_{35}
- δ_{35} = $\Delta\delta_{1Y}$ x 35years = + 0 ° 04'x 35 = + 2 ° 20 '
- δ_{2000} = δ_{1965} + δ_{35} = + 0 ° 54 '+ 2 ° 20' = + 3 ° 14 '
- calculated Π:

$$\Pi = (\pm\gamma) - (\pm\delta_{2000}) = -1°55' - 3°14' = -5°09'$$

By the formulas (1) to (6) for azimuth dependencies and the indicated angle we can make all the necessary calculations.

Conclusion

The methodology for determining the direction to a point are easy to perceive and are convenient for use in field conditions as they do not require any specialized equipment.

REFERENCES:

1. Кастрева П. Географски информационни системи и компютърна картография. Университетско издателство "Неофит Рилски", гр.Благоевград, 2011г.
2. Plamen Mihajlov, Evgeni Stoykov, 'Evaluation of the accuracy of measurements with dual-frequency GPS receiver Trimble R4 in the RTK (Real Time Kinematics) mode', International conference on Bionics and Prosthetics, Biomechanics and mechanics, mechatronics and robotics, June 17-21, 2013, Riga, Latvia, 2013 г.
3. Андреев А., Михайлов Пл., Стойков Е., "Сравнителен анализ на получените резултати от височинни измервания по различни методи", Научна конференция с международно участие МАТТЕХ 2016, ШУ "Епископ Константин Преславски"
4. Стойков Е., "Модернизация и въвеждане на допълнителни GPS сигнали", научна конференция с международно участие МАТТЕХ 2014, ШУ "Епископ Константин Преславски"
5. Иванов С., Ръководство за работа с топографска карта, Университетско издателство „Епископ Константин Преславски", Шумен 2018.

Author's name: chief assistent Sabin Ivanov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Geodesy"
E-mail: s.ivanov@shu.bg

ANALYSIS AND EVALUATION OF MEASUREMENT ACCURACY WITH DUAL -FREQUENCY GNSS RECEIVER TRIMBLE R4 IN THE RTK (REAL TIME KINEMATICS) MODE

Evgeni Gr. Stoykov

ABSTRACT: *In the GNSS measurements of points on the National Geodetic Map in the region of the town of Shumen are being considered. Study of the dependence and accuracy in the results depending on the time of measurement in RTK (Real Time Kinematics) mode. The obtained results compare them with equal results post-processing.*

KEYWORDS: *Geodesy, GNSS, RTK.*

At the beginning let us mention the National GPS network in Bulgaria.

National GPS network established pursuant to Decree 140/04. 06. 2001, which defines the Bulgarian Geodetic System 2000 and serves as a renewal of the State Geodetic Network of the Republic of Bulgaria.

National GPS network of the country is based on:

- ✓ The permanent GPS stations of the permanent European network EPN (European Permanent Network), respectively, of the International GNSS Service IGS (International GNSS Service);
- ✓ Network EUREF points in Bulgaria or "BULREF" as the realization of the European Reference System ETRS89 in Bulgaria.

National Network consists of two classes of points combined in the primary and secondary network and includes a total of 497 points, distributed as follows: 112 points from the main GPS Network, 40 extra points and 345 points of the secondary GPS network.

The core network is designed to realize, distribute and maintain the ETRS89 European Coordinate System with accuracy of 10 mm in position and 15-20 mm in height using GNSS technology.

Table 1. Points from the main GPS network

№	Type of points	Number	Note
1	Points from the „BULREF“ Network	15	Of them 2 State Geodetic Network I and II class
2	Points from EUVN	2	
3	Points State Geodetic Network I	25	2 points from "BULREF"

	and II class		
4	Points State Geodetic Network III and IV class	46	
5	New points	22	
6	Points with special status	2	
	Everything	112	

Responsibilities for the construction, measurement, processing, dissemination of results and maintenance of the State GPS Network were implemented by the Council of Ministers Decree 1/06. 01.05.2005, for assignment of geodesy and cartography tasks of national importance.

Table 2. Additional points

№	Type of points	Number	Note
1	Connecting - to „BULREF“ points - others	24 10 14	
2	Duplicates - to „BULREF“ points - to points with special status	16 14 2	
	Everything	40	

Table 3. EUREF Points (BULREF) in Bulgaria

№	Points from "BULREF"			Connecting		Duplicates	
	Number	Name	Class	Number	Class	Number	Class
1	11101M002[1]	SOFI	I	11101M002	I		
2	31	PANA	II	31	II		
3	8140	GABR		79	II	8404	
4	8141	SHUM		177	II	8405	
5	8142	KAVA		93	II	6748	IV
6	8143	HARM		148	II	8409	
7	8144	BURG		70	I	8406	
8	8145	SAPA				8412	
9	8146	PETR		103	I	8411	
10	8147	SATO					
11	8148	BERK				8402	
12	8149	VIDI		7	I	8401	
13	8150	GULI		67	II	8403	
14	8151	KERM		165	II	4499	IV
15	8152	MAMA		194	II	8408	

[1] This is the SOFI point number in accordance with the accepted EUREF / IGS standards

Table 4. Points with special status

№	Point	Location	Description	Duplicate point
1	TROY	Troyan	Subdivision 24430	8318
2	VVUA	Shumen	Military school	

Table 5. Points of the secondary GPS network

Points State geodetic network I and II class	Points State geodetic network III and IV class	Geodetic network with local use	Gravity points	New points	Total
25	226	3	1	89	345

The work done and the results achieved in the construction and processing of the State GPS network have a fundamental importance for the state, comparable to that of the State Geodetic Network established in the 1930s. On the basis of the results obtained, a new realization of the ETRS89 European Coordinate System for the territory of Bulgaria was adopted, consisting of 25 points.

Fig.1. Government GPS network

Trimble R4 is a modern receiver that accepts 5 frequencies, namely GPS L1/L2, L2E, Glonass L1P/L2P, SBAS, with the ability to work both in real-time GNSS network and in post processing. It is 10Hz receiver, which means you can make ten independent determinations of position in the

second, which helps it retain its initialization and fixed solution for dynamic applications and work in RTK (Real Time Kinematics).

Achieved accuracy: Kinematic mode: Accuracy "horizontal" - 8 mm + 1 ppm RMS; Accuracy "Vertical" - 15 mm + 1 ppm RMS; during initialization - usually < 8 sec.; Reliability initialization - typically> 99.9%.

In order to investigate the accuracy of the measurements with the receiver in RTK mode, depending on the time of standing, in the month of April 2018 were measured 21 the number of points - triangulation and working in the region of Shumen. Each of the points was assessed for 3, 5, 10 and 15 min, except for item № 21 which is measured downstream of 3, 5 and 10 minutes. In this mode, at the time of measurement is given flat rectangular coordinates of the points in a coordinate system in 1970, using a team made Trimble's transformation and implemented in software transformation parameters for the country.

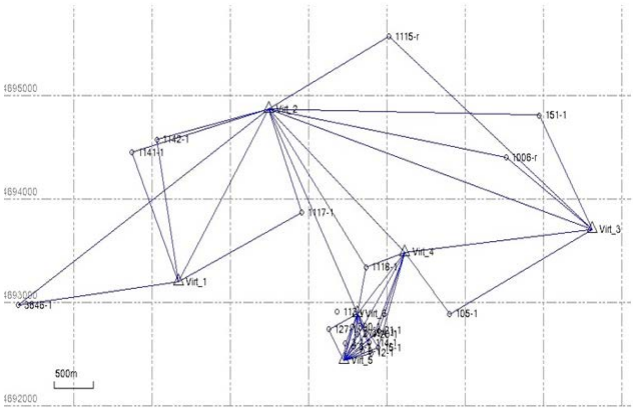

Fig.1. Network circuit

When comparing the coordinates of the points obtained in the RTK mode in dependence on the time of standing, the following results (as was a combination of different timings): mean differences in the coordinates (differences 3-5 minutes) - 0.60 cm in X, 0.63 cm in Y and the average error in position 0.87 cm, (differences 3-10 minutes) - 0.57 cm in X, 1.03 cm in Y and the average error in position 1.18 cm, (differences 3-15 minutes) - 0.83 cm in X, 0.73 cm in Y and the average error in position 1.10 cm (differences 5-10 minutes) - 0.55 cm in X, 0.56 cm in Y and average error set to 0.79 cm (differences 5-15 minutes) - 0.73 cm in X, 0.88 cm in Y and the average error in position 1.14 cm (differences 10-15 minutes) - 0.42 cm in X, 0.42 cm . on

Y and average error in position 0.60 cm. The differences are minimal - the average error in position ranged from 0.79 to 1.18 cm. In fact, they are much smaller for most items do not exceed 1.0 cm. Greater difference was observed in paragraph 27 (this is a detailed section), where it ranges from 1.32 to 4.18 cm.

We made a comparison between the flat coordinates of the points obtained in RTK mode and they received after the settlement and adjustment of the network with specialized software - Trimble Business Centre. For this purpose, a reference is generated virtual network stations GeoNet and retrieves data. As can be expected, they are also minimal - mean error in position varies from 0.61 to 1.45 cm.

As a result of GPS measurements are obtained elliptical coordinates and height (B, L, H) of points or their spatial rectangular Cartesian coordinates (X, Y, Z) in a coordinate system WGS84. In this case it is necessary to transform the coordinate system results in 1970. There is no functional relationship between the two coordinate systems (WGS 84 geocentric and flat 1970) and to obtain the coordinates of our points in the coordinate system 1970 having to do transformation. As we know we need common points with coordinates in both coordinate systems. Current transformation object is achieved with the available points for the coordinate system 1970, which in most cases are of varying accuracy that produces the same results with a lower accuracy. Thus each case is made specific transformation and the results are distantly related to the other ones in other regions of the country.

Previous studies have found [3] that any WGS coordinates of the starting points to use (given by the Cadastre Agency or directly obtained from the GPS measurements), almost identical results are obtained in the 1970 coordinate system. This confirms the view that the coordinates of the exit points in the same system, rather than their WGS coordinates, are essential for obtaining good co-ordinates in the 1970 coordinate system. For this purpose, it is necessary to determine the coordinates of a sufficient number of points simultaneously in the WGS84 system and in the 1970 system (or any other one that is accepted) with the appropriate accuracy, including the heights. These coordinates are to be provided by the Cadastre Agency, in particular by the cadastre offices of companies working in the field of geodesy. Or, it is better to have the functional links between the two coordinate systems and to solve this really important question once and for all.

Conclusion

From the comparisons made, a preliminary conclusion can be made: if the relevant points are measured in RTK mode, for a longer time than is provided in the software, then we can save time and postprocessing means (post-processing). As we have seen above, the differences in received mean errors in RTK mode and after equalization are minimal.

REFERENCES:

1. Минчев М., Здравчев Ив., Георгиев Ив., Основи на приложението на GPS в геодезията-, УАСГ - София, 2005 г.
2. Михайлов Пл., Държавна GPS мрежа на Република България – настояще и бъдеще, Научна сесия с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски".
3. Михайлов Пл., Върху резултатите от трансформирането на точки, резултат от GPS измервания , годишник на ШУ, Технически науки 2009 г.
4. Иванов С., Сравнителен анализ на геодезически системи БГС 2000 и БГС 2005, научна сесия с международно участие MATTEX 2014, ШУ "Епископ Константин Преславски".
5. Иванов С., Извод на формула за изчисляване на началния посочен ъгъл, при решаване на обратна засечка чрез синусите и косинусите на измерените хоризонтални ъгли, научна сесия с международно участие MATTEX 2016, ШУ "Епископ Константин Преславски".
6. Михайлов Пл., Петров Д., "Съвременни технически средства и технологии за събиране на геопространствени данни за местността", ШУ "Епископ Константин Преславски", монография, 2014.
7. Михайлов Пл., "Ръководство за упражнения по геодезични мрежи" – Учебно пособие; Шуменски университет „Епископ Константин Преславски", 2007.
8. Андреев А., Съвременни методи за локално моделиране на геоида. 162 с. НВУ "В.Левски" – Шумен, ВТС, 2008.
9. Андреев А., Андреева П. "Локално моделиране на геоида за територията на Североизточна България", Научна конференция с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски", 2010 г.
10. Андреев А., Андреева П. "Анализ на системите височини от гледна точка на физическата геодезия и приложението им в Р. България.", Научна конференция с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски", 2010 г.

Author's name: Chief Assistant eng. Evgeni Stoykov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Geodesy
E-mail: e.stoykov@shu.bg

TECHNOLOGY OF SATELLITE MEASUREMENTS WHEN CREATING A GPS NETWORK

Evgeni Gr. Stoykov

ABSTRACT: *The article describes the technology of satellite measurements in creating a GPS network for the needs of geodesy.*

KEYWORDS: *Geodesy, GNSS, RTK.*

Designing a GPS network poses some important issues related to equipment, measurement methods and organization.

GPS measurements differ significantly from classic geodetic measurements as they are time independent and there is no need for direct visibility between the points. Due to these differences, GPS measurements require other ways of planning, performing and processing. Depending on the case of an application or project, planning GPS measurements may or may not be necessary. Initially, the exact measurement goal and accuracy in the search results (coordinates) should be determined. Undoubtedly, significant planning efforts are required to successfully perform high-end measurements, however, lower-end measurements may not require detailed planning except in heavily wooded areas or areas with other obstacles.

Optimal planning of GPS measurements involves the consideration of several parameters, such as: station and satellite configuration, number and type of receivers used, and economic aspects. Contrary to the design of triangular or trilateral networks that require considerable effort to maintain imbalance in their geometry, for GPS networks, the geometry and lengths of the countries are not as critical. Planning should also take into account some aspects of processing, for example, whether single base vectors can be calculated with the software available or that multi-point solutions can be made. For large, multi-point projects and if more receivers are available, planning GPS measurements can be alleviated by using computer programs.

1. Pre-planning.

- ✓ Select points.

The first step in planning GPS measurements is to provide cartographic materials (map) of the area on an appropriate scale on which to place the relevant points. All new points, along with the existing datum points, are placed on the map. In most cases, it is not worthwhile to use reference points that are not included in the State Geodetic Network. When using coordinates of points of unknown accuracy, many problems can be

created, so it is better to choose one point of the State Geodetic Network even if it is longer than the projected points than other points of reference [2].

- ✓ Session length and recording interval.

The specific time period chosen for measurement is called a session.

To determine a vector by double phase differences, measurements over ten seconds are sufficient, and two more epochs are needed to resolve ambiguities in pseudo-space between satellites and receivers. However, in order to obtain a stable solution of the vector and an indefinite evaluation of the accuracy of its components, continuous observation is required with a good geometric configuration of the satellite constellation [3]. The factors that determine the duration of the individual measurement are:

- o Length of the base vector;
- o Number of visible satellites (affects geometry);
- o Relative geometry of satellites and change in geometry;
- o The "signal / noise" ratio (SNR) of the satellite received signal.

In general, the more satellites are available, the better the geometry and the shorter the measurement period. In the case of shorter base vectors, the length of the session may also be shortened.

When planning real-time sessions, two factors are to be considered. Typically, the time is selected when five or more satellites are over, and when the satellites have a GDOP of less than six. For most standardized GDOPs, the condition is met when five or more satellites are present. A problem occurs when one of the satellites has an obstacle during the measurement, and the other four satellites have a high GDOP. This problem is solved, as the mobile receiver stays stationary until the fifth satellite appears [2].

The other main parameter of the observation session, except its duration, is the recording interval. This is the time interval between two consecutive satellite signal registrations. This interval is a minute per minute. It is desirable to gather as many observations as possible during the session. A recommended interval may be 5 sec. A shorter interval is not necessary as there would be no significant change in the position of the satellites for two or three consecutive epochs. Data accumulation is very fast, and the same takes up a lot of memory without much information.

2. Survey of the terrain.

Field research is mandatory before real-time measurements are taken (except when using OTF- On the Fly receivers). Every point of the working geodetic base should be checked for visibility to the skyline, and also the chosen path between the points should have good visibility to the sky. Because real-time measurement requires constantly maintaining a connection to four or more satellites, good visibility practically means a situation that is

free of obstructions (above 15 ° vertical angle). When obstacles appear on the measurement path (eg engineering facilities or tall buildings) static points can be placed on both sides of the obstacle so that the mobile receiver can be re-initialized. It is also important that the path we have chosen between the points is clearly marked on the pad to make sure that unwanted cyclic errors are not present [2].

In addition to the obstacles, an issue with the multipath of the alerts is also important. The multipath we examined above is the result of unwanted reflected satellite signals that are received by the antenna. This problem is greater when the antenna is placed near fences of a knit mesh or other metallic equipment. In this case, the satellite signals are reflected by the metallic devices, and the reflected signals distort the direct signals by causing phase errors. When we have fences from a knit mesh, we can lift the antenna above it to eliminate the problem. If we have a point that is close to a metal building, the only practical solution is to move the point elsewhere [2].

3. Initialization and measurement.

Kinematic initialization (OTF – On the Fly) is a modern way to solve phase ambiguity. The theoretical method can be applied to single-frequency receivers if the error in determining the distance with code measurements is small enough, this is achievable by the narrow correlation method, which reduces noise and multipath. This method is best applied to two-way receivers in which the carrier phase and the code phase are measured at both frequencies. For real-time measurements, after initialization, the fixed receiver (if any) and the mobile receiver are placed on the fixed starting point for several observation periods. Thereafter, the mobile receiver is moved to the points whose coordinates are to be determined. Fixed point vectors can be determined with high accuracy if continuous measurements are made from the two receivers to four or more satellites (with a small PDOP). When there is a signal interruption or cyclic errors, the initialization must be repeated. This may have happened when the satellite signal came into the shadow of buildings (some obstacle - bridges, trees or other objects). In practice, the points to be measured are to be staged twice so as to make a determination of the situation. Also, if possible, include several points with known coordinates (e.g., static measurement) to provide additional verification.

The mobile receiver usually stays at any point for several measurement periods, whereby the measurement results can be averaged and the situation obtained more accurately [2].

Conclusion

With the introduction and development of GNSS and permanent geodetic networks, RTK measurements become much faster and more

accurate. Precision analysis and assessment, optimal planning, choice of geodetic network locations, session duration, and record interval are critical to improving the performance and quality of GNSS observations.

REFERENCES:

1. Стойков Е., Изследване на възможността за използване на двучестотен GPS приемник в режим RTK за създаване на РГО, заснемане и трасиране на обекти. Дисертационен труд, Шумен 2015.
2. Хофман-Веленхоф Б., Лихтенегер Х., Колинс Дж. Глобална система за определяне на местоположение: Теория и практика. Превод от английски, София, УАСГ, 2002.
3. Янков И. Геодезически методи за изследване деформации на инженерни съоръжения. Дисертационен труд, София, 2009.
4. Михайлов Пл., Държавна GPS мрежа на Република България – настояще и бъдеще, Научна сесия с международно участие МАТТЕХ 2010, ШУ "Епископ Константин Преславски".
5. Иванов С., Извод на формула за изчисляване на началния посочен ъгъл, при решаване на обратна засечка чрез синусите и косинусите на измерените хоризонтални ъгли, научна сесия с международно участие МАТТЕХ 2016, ШУ "Епископ Константин Преславски".
6. Иванов С.,Кастрева П.,Безинска К.-Проблемни ситуации в състоянието и експлоатацията на обектите на културното наследство, научна сесия с международно участие МАТТЕХ 2016, ШУ "Епископ Константин Преславски".
7. Иванов С., Сравнителен анализ на геодезически системи БГС 2000 и БГС 2005, научна сесия с международно участие МАТТЕХ 2014, ШУ "Епископ Константин Преславски".
8. Михайлов Пл., Петров Д., "Съвременни технически средства и технологии за събиране на геопространствени данни за местността", ШУ "Епископ Константин Преславски", монография, 2014.
9. Михайлов Пл., "Ръководство за упражнения по геодезични мрежи" – Учебно пособие; Шуменски университет „Епископ Константин Преславски", 2007.
10. Андреев А., Съвременни методи за локално моделиране на геоида. 162 с. НВУ "В.Левски" – Шумен, ВТС, 2008.
11. Андреев А., Андреева П. "Локално моделиране на геоида за територията на Североизточна България", Научна конференция с международно участие МАТТЕХ 2010, ШУ "Епископ Константин Преславски", 2010 г.
12. Андреев А., Андреева П. "Анализ на системите височини от гледна точка на физическата геодезия и приложението им в Р. България.", Научна конференция с международно участие МАТТЕХ 2010, ШУ "Епископ Константин Преславски", 2010 г.

Author's name: Chief Assistant eng. Evgeni Stoykov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Geodesy
E-mail: e.stoykov@shu.bg

ANALYSIS OF THE METHODS FOR TRANSFORMING SPATIAL CARTESIAN COORDINATES (X, Y, Z) OBTAINED FROM GNSS MEASUREMENTS, IN ELLIPSOIDAL COORDINATES AND HEIGHT (B, L, H)

Evgeni Gr. Stoykov

ABSTRACT: *There are many solutions to transform spatial Cartesian coordinates (X, Y, Z) coordinates and ellipsoid height (B, L, H), which generally can be grouped into three groups: formulas for iterations B, formulas with differential corrections to B (tgB) and closed formulas. Will examine methods of the first and third group whose formulas are used to solve this issue.*

KEYWORDS: *Geodesy, GPS, Transformations.*

Reference (official) system of GPS is the World Geodetic System 1984 (WGS - 84). Received from GPS measurements dimensional rectangular geocentric coordinates (*X, Y, Z*), in practice can not always be directly put into service users. Since the resulting coordinates of ground points using GPS to obtain a global geocentric system (WGS - 84), and we care about the earth points are referred to the local coordinate system (Geodetic - ellipsoidal or plane coordinates), which is not geocentric must perform the appropriate transformations [2]. Or put another way, it is necessary first to be transformed into ellipsoidal geographic coordinates (*B, L, H*), and from them a suitable geodetic projection.

For GNSS measurements more important is the transformation from the spatial rectangular geocentric coordinates (*X, Y, Z*) in the ellipsoidal geographic coordinates (*B, L, H*). There are many different ways to address this issue, the main difficulty comes in finding the ellipsoid latitude *B*. Finding the ellipsoid longitude L is done much easier [1].

Assigning a Cartesian coordinate of a point in space *X, Y, Z*, and assuming a rotational ellipsoid having the same point on the Cartesian coordinate system, the point can also be given, with elliptical coordinates *B, L, H* (Fig.1) [2].

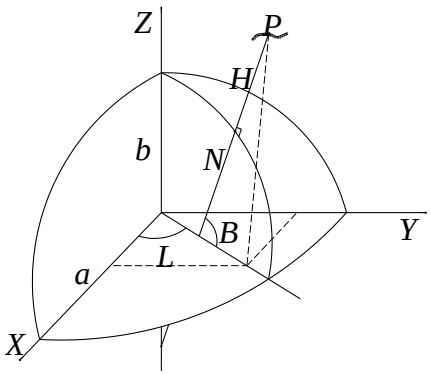

Fig.1.

The relationship between Cartesian and elliptical coordinates is given by the well-known formulas:

$$\begin{aligned} X &= \left(N+H\right).\cos B.\cos L \\ Y &= \left(N+H\right).\cos B.\sin L \\ Z &= \left(\frac{b^2}{a^2}N+H\right).\sin B, \end{aligned} \qquad (1)$$

where N is a transverse radius of curvature and is obtained by the following formula

$$N = \frac{a^2}{\sqrt{a^2.\cos^2 B + b^2.\sin^2 B}} \quad \text{or} \quad N = \frac{a}{\left(1-e^2.\sin^2 B\right)^{1/2}}, \qquad (2)$$

a and b are respectively the large and the small semi-axis of the ellipsoid.

In the considered formula (1) is transformed elliptical coordinates B, L, H in Cartesian coordinates X, Y, Z. As noted above for GPS applications more important is the reverse transformation as Cartesian coordinates are known, and elliptical coordinates are looking for. In this connection, the aim is to calculate the elliptical coordinates B, L, H of the spatial coordinates X, Y, Z. In the literature this problem is solved by iterations, but there is a possible

solution in closed form [2]. Of *X* and *Y* coordinates can calculate the radius of the parallel

$$p = \sqrt{X^2 + Y^2} = \left(N + H\right).\cos\varphi. \qquad (3)$$

From the above equation after transformation we get the ellipsoid height *H*:

$$H = \frac{p}{\cos B} - N \qquad (4)$$

From the formula for the first eccentricity can be given to the relationship $\frac{b^2}{a^2} = 1 - e^2$, which upon substitution in the equation for *Z*, the result is obtained

$$Z = \left(N + H - e^2.N\right).\sin B, \qquad (5)$$

equivalent which can be given by the equation

$$Z = \left(N + H\right)\left(1 - e^2.\frac{N}{N + H}\right).\sin B \qquad (6)$$

If we divide the resulting expression of equation (3), we get

$$\frac{Z}{P} = \left(1 - e^2.\frac{N}{N + H}\right).\tan B, \qquad (7)$$

where we can express the ellipsoid width *B*

$$\tan B = \frac{Z}{P}\left(1 - e^2.\frac{N}{N + H}\right)^{-1} \Rightarrow B = \arctan\frac{Z}{p}\left(1 - e^2.\frac{N}{N + H}\right)^{-1} \qquad (8)$$

From equations (1), by dividing the first to the second equation is the equation of the ellipsoid obtained length L

$$\tan L = \frac{Y}{X} \Rightarrow \quad L = \arctan \frac{Y}{X} \ . \qquad (9)$$

In connection with the above will be considered several methods of calculation.

For the ellipsoid WGS 84, the following parameters:

$a = 6378137m$ - semimajor axis of the ellipsoid

$f = 1/298.257223563$ - flatness, $e^2 = 2f - f^2$ - first eccentricity

$e'^2 = \frac{e^2}{\left(1-e^2\right)}$ - second eccentricity , $e^2 = \frac{(a^2-b^2)}{a^2}, e'^2 = \frac{(a^2-b^2)}{b^2}$,

$b = a\sqrt{1-e^2} = 6356752.31424518m$, $e^2 = 0.00669437999014132$,

$e'^2 = 0.006739496742276$, $\left(1-e^2\right) = 0.993305620009859$,

$\left(1-e'^2\right) = 1.006739496742276$

1. First method through iteration.

1.1 Calculation of secondary value $-p = \sqrt{X^2 + Y^2}$.

1.2 Calculate the approximate value of B_0 – $B_0 = \arctan \frac{Z}{p}\left(1-e^2\right)^{-1}$.

1.3 Calculate the approximate value of N_0 (transverse radius of curvature of the ellipsoid-like) – $N_0 = \frac{a^2}{\sqrt{a^2.\cos^2 B_0 + b^2.\sin^2 B_0}}$.

1.4 Calculating the ellipsoidal height – $H = \frac{p}{\cos B_0} - N_0$.

1.5 Calculation of the improved value of the width – $B = \arctan \frac{Z}{p}\left(1 - e^2 . \frac{N_0}{N_0 + H}\right)^{-1}$.

Checking for the necessary next iteration: if $B = B_0$, then the iteration is completed, otherwise it is applied $B_0 = B$ and continued in a third step (i.e., repeat steps 1.3, 1.4 and 1.5 while $B_i = B_{i-1}$).

1.6 Ellipsoid length is obtained from the equation $-\tan L = \frac{Y}{X} \Rightarrow$

$L = \arctan \frac{Y}{X}$.

Example:
X = 4113656.8739 m, Y = 2170479.9823 m, Z = 4350140.6014 m

Solution: $p = 4651145.6900$, $B_0 = 43.27676606$, $N_0 = 6388193.4497$,
$N_1 = 6388193.4463$, $N_2 = 6388193.4463$, $H_0 = 297.120m$,
$H_1 = 296.182m$, $H_2 = 296.185m$, $B_1 = 43.27675710$, $B_2 = 43.27675713$,
$B_3 = 43.27675713 \left(43^0 16`36.3257``\right)$, $L = 27.81737779 \left(27^0 49`02.5600``\right)$

For the first method of calculations shows that it takes at least three iterations to get the value of elliptical coordinates *B* and *H*.

2. Second method iterates through.

2.1 Calculation of secondary value – $p = \sqrt{X^2 + Y^2}$.

2.2 Calculate the approximate value of B_0 – $B_0 = \arctan\left(\frac{Z}{p}\left(1 + \frac{e^2}{1 - e^2}\right)\right)$.

2.3 Calculate the approximate value of N_0 (transverse radius of curvature of the ellipsoid-like) – $N_0 = \frac{a}{\left(1 - e^2.\sin^2 B_0\right)^{1/2}}$.

2.4 Calculation of the improved value of the width – $B = \arctan\left(\frac{Z}{p}\left(1 + \frac{e^2.N_0.\sin B_0}{Z}\right)\right)$.

Again checks the next iteration needed, as in the previous method: if $B = B_0$, then the iteration is completed, otherwise it is applied $B_0 = B$ and continued in a third step (i.e., repeat steps 1.3 and 1.4 while $B_i = B_{i-1}$).

2.5 Calculating the ellipsoidal height [3] – $H = D\cos B + \left(Z + e^2 N \sin B\right)\sin B - N$.

2.6 Calculation of the ellipsoid length [3].

a) If $X \neq 0$, calculated utility value $-\overline{L} = \arctan\frac{Y}{X}$, then determine the quadrant and the final value of the ellipsoid length.

- if $X > 0$, $Y \geq 0$, it $L = \overline{L}$
- if $X > 0$, $Y < 0$, it $L = 360^0 - \overline{L}$
- if $X < 0$, $Y < 0$, it $L = 180^0 + \overline{L}$
- if $X < 0$, $Y \geq 0$, it $L = 180^0 - \overline{L}$

б) If $X = 0$, the ellipsoid length is determined as follows:

- if $Y > 0$, it $L = 90^0$
- if $Y < 0$, it $L = 270^0$

Example: We use the same values of *X, Y* and *Z* of the top section.

Solution: $p = 4651145.6900$, $B_0 = 43.27676606$, $N_0 = 6388193.4497$,

$N_1 = 6388193.4463$, $N_2 = 6388193.4463$, $B_1 = 43.27675716$,

$B_2 = 43.27675713$, $B_3 = 43.27675713\ \left(43^0 16`36.3257``\right)$, $H = 296.185m$,

$L = 27.81737779\ \left(27^0 49`02.5600``\right)$

For the second method of calculations shows that are also needed at least three iterations to get the value of the ellipsoid width *B*, while the height *H* is obtained directly with the final width *B*.

3. A third method without iteration, but with the inherent approximation.

3.1 Calculation of the ellipsoid width $-B = \arctan \frac{Z + e^{`2}.b.\sin^3 \theta}{p - e^2.a.\cos^3 .\theta}$,

where $p = \sqrt{X^2 + Y^2}$ and

$\theta = \arctan \frac{Z.a}{p.b}$ are secondary value.

3.2 Ellipsoid length is obtained from the equation $-L = \arctan \frac{Y}{X}$.

3.3 Calculate the approximate value of N (transverse radius of curvature of the ellipsoid-like) – $N = \frac{a^2}{\sqrt{a^2.\cos^2 B + b^2.\sin^2 B}}$.

3.4 Calculating the ellipsoidal height – $H = \frac{p}{\cos B} - N$.

Example: Using the same values of *X*, *Y* and *Z* of the point 1.
Solution: $p = 4651145.6900$, $\theta = 43.18073761$,
$B = 43.27675713 \left(43^0 16`36.3257``\right)$, $L = 27.81737779$, $\left(27^0 49`02.5600``\right)$
$N = 6388193.4463$, $H = 296.185m$

In the third method elliptical coordinates *B* and *H*, are obtained by visibly less computing activity as precision achieved coincides with the third iteration of points 1 and 2.

4. Decision without iterations (method of Prof. Valev).
This method is used for items in the near-Earth space. Used formulas provide sufficient accuracy for practical purposes [1].

$N = \sqrt{X^2 + Y^2 + Z^2.\left(1 + e^{`2}\right)^2}$ ; $A = \sqrt{X^2 + Y^2 + Z^2.\left(1 + e^{`2}\right)}$ - semi major axis of the ellipsoid like. Calculated $H = \frac{\left(A - a\right).A}{N}$.

Calculated $\tan B = \tan B_0.K_1$, where $\tan B_0 = \frac{Z.\left(1 + e^{`2}\right)}{\sqrt{X^2 + Y^2}}$ and $K_1 = \frac{1}{1 + \frac{H.e^{`2}}{N}}$.

Calculated $B = \arctan\left(\tan B_0.K_1\right)$ and $L = \arctan\frac{Y}{X}$.

Example: Using the same values of *X, Y* and *Z* of the point 1.
Solution: $N = 6388490.5694$, $A = 6378433.6520$, $H = 296.185m$
$\tan B_0 = 0.9415870093$, $K_1 = 0.9999996875$
$B = 43.27675713\ \left(43^0 16`36.3257``\right)$, $L = 27.81737779$, $\left(27^0 49`02.5600``\right)$

This method is equivalent to the third, the achieved accuracy coincides with that obtained by the three methods.

To check the precision achieved, as well as control of computing activity is recommended to make the reverse transformation.

5. Conversion from *B, L, H* in *X, Y, Z.*
Use of formulas (1) and (2).

Example: $B = 43^0 16`36.3257``$, $L = 27^0 49`02.5600``$, $H = 296.185m$
Solution: $N = 6388193.4463$,
$X = 4113656.8739\ m$, $Y = 2170479.9823\ m$, $Z = 4350140.6014\ m$

To obtain the same coordinates *X, Y, Z* as above, necessary values for the *B* and *L* are calculated with four decimal places.

REFERENCES:

1. ст.н.с. I ст. д-р инж. Г. Милев, проф. дтн инж. Г. Вълев, доц. д-р инж. М. Минчев, М. Матова, К. Василева, П. Гъбенски – Европейската референтна система в България, София, 2006.
2. Б. Хофман-Веленхоф, Х. Лихтенегер, Дж. Колинс – Глобална система за определяне на местоположение, Теория и практика, 2002.
3. 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".
4. Иванов С., Методика за решаване на права засечка по измерени хоризонтални ъгли и права засечка по посочни ъгли, Научна конференция с международно участие MATTEX 2018, Шумен.
5. Михайлов Пл., Янчева К., Изследване и оценка на точността на планово-височинни мрежи, трансформирани от координатна система 1970 г. в КС2005 – кадастрална с лицензирания софтуер BGSTrans, Научна конференция с международно участие MATTEX 2018, Шумен.
6. Иванов С., Извод на формула за изчисляване на началния посочен ъгъл, при решаване на обратна засечка чрез синусите и косинусите на измерените хоризонтални ъгли, научна сесия с международно участие MATTEX 2016, ШУ "Епископ Константин Преславски".
7. Иванов С., Сравнителен анализ на геодезически системи БГС 2000 и БГС 2005, научна сесия с международно участие MATTEX 2014, ШУ "Епископ Константин Преславски".
8. Михайлов Пл., Петров Д., "Съвременни технически средства и технологии за събиране на геопространствени данни за местността", ШУ "Епископ Константин Преславски", монография, 2014.
9. Михайлов Пл., "Ръководство за упражнения по геодезични мрежи" – Учебно пособие; Шуменски университет „Епископ Константин Преславски", 2007.
10. Андреев А., Съвременни методи за локално моделиране на геоида. 162 с. НВУ "В.Левски" – Шумен, ВТС, 2008.
11. Андреев А., Андреева П. "Локално моделиране на геоида за територията на Североизточна България", Научна конференция с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски", 2010 г.
12. Андреев А., Андреева П. "Анализ на системите височини от гледна точка на физическата геодезия и приложението им в Р. България.", Научна конференция с международно участие MATTEX 2010, ШУ "Епископ Константин Преславски", 2010 г.

Author's name: Chief Assistant eng. Evgeni Stoykov, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Geodesy
E-mail: e.stoykov@shu.bg

ESTIMATING THE AREA OF THE IRREGULAR DUNG-HILLS IN SHUMEN MUNICIPALITY BY USING UNMANNED AERIAL VEHICLES

Monika B. Bedzheva, Stefan D. Dobrev

ABSTRACT: *The effective waste management is one of the primary trends in reducing the negative effect on the environment caused by humans. Considering this in the paper the dependence between the number of population in settlements in Shumen municipality and the area of their irregular dung-hills has been estimated using unmanned aerial vehicles (UAV) and photogrammetry. The obtained results can be used for more precise planning, organization and execution of irregular dung-hills recultivation.*

KEYWORDS: *Irregular dung-hills, Photogrammetry, Unmanned aerial vehicle (UAV).*

1. Introduction

Preservation of the environment is one of the most important problems that human society is facing. It is determined by two factors: the boom in the industrial branch and the society's culture of consumption (fig. 1).

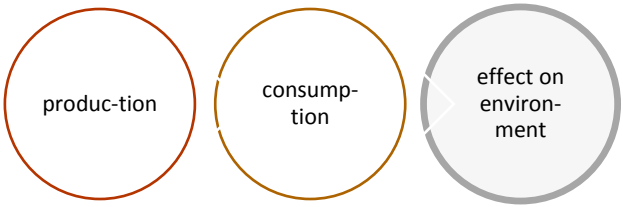

Fig.1. Factors that cause negative effect on environment

In one hand, the production causes effect by releasing hothouse gases, soot and small dust particles in the atmosphere and also with the huge expense of water integrated in production cycle.

On the other hand, many goods are made of materials that after going out of use slowly and difficult decompose in natural way. Unfortunately, many of them do not reach the recycling works or waste depots but are thrown away by the road, in the fields, riverbeds, gullies – the so called irregular dung-hills.

This leads to the conclusion that for reducing the negative effects on environment caused by humans the effective waste management is one of the main directions to follow. Assuming this, the aim of the paper is to estimate the dependence between the number of population in settlements in Shumen municipality and the area of their irregular dunghills so that more precise planning, organization and execution of recultivation is being made.

2. Estimating the area of irregular dunghills in Shumen municipality using unmanned aerial vehicles

The analysis of dependence between the number of population in the settlements and the area of their irregular dunghills is made difficult by the following shortcomings of the classical methods of surveying.

First, it is quite expensive and the surveyors work in potentially risky environment for their health.

Second, the irregular dunghills usually are located so that their existence is being concealed. For this reason, about 30% of the irregular dunghills are never investigated.

At this stage of the remote sensing's development the listed problems can be overcome by using unmanned aerial vehicles (UAVs). Indeed, this approach reduces repeatedly the expensiveness of initial surveying of large land areas. Besides, the health risks are practically excluded.

Considering this technology's advantages in September 2018, irregular dunghills near 6 villages in Shumen municipality had been examined using UAV. The study was carried out in three steps.

On the first (in the field) step 6 villages in Shumen municipality were overflown with UAV. In addition, by field surveying the average height of the irregular dunghills are estimated at

$$\boldsymbol{h = 0,05\ [m]}. \tag{1}$$

On the second step the aerial photographs were processed with Agisoft PhotoScan. As a result digital elevation models (DEM) and orthophoto mosaics from them have been generated. Some of the irregular dunghills happened to be located out of cellular communication systems' coverage. For this reason ground control points (GCPs) were not placed on them and for models' orientation was used only the board GPS data. This

circumstance does not question the reliability of the conducted surveying because only the absolute values of areas and volumes are of interest.

On the third (main) step the orthophoto mosaics were imported in Global Mapper so that irregular dunghills' areas and volumes were measured. The obtained results are presented in table 1. In the first column, the villages are indicated with numbers from 1 to 6 according their flying row. The data in the second column is according [1].

Table 1: Main results from the photogrammetry

Village	Population count of village i N (i)	Dunghill area near village i S (i) [m^2]	Dunghill volume near village i V (i) [m^3]	Volume garbage per citizen of village i [m^3/citizen] $\bar{v}_{av}(i)$
Village 1	1543	5666,2	283,31	0,18
Village 2	555	1857	92,85	0,17
Village 3	195	1596	79,80	0,41
Village 4	374	1916,8	95,84	0,26
Village 5	1019	7350	367,50	0,36
Village 6	254	3217	160,85	0,63
Total	$N_s = 3940$	$S_s = 21603$	$V_s = 1080$	

As of mathematical statistics' point of view the presented results are a statistical excerpt with size equal to the total number of citizens N_s of all villages

(2) $$N_s = \sum_{i=1}^{n} N(i) = 3940.$$

Besides, the statistical excerpt consists of $n = 6$ groups and their sizes are equal to the number of village citizens $N(i), i = 1, 2, \dots, 6$.

From table 1 we can see that all N_s citizens have "generated" garbage with volume

(3) $$V_s = \sum_{i=1}^{n} V(i) = 1080\ [m^3].$$

Since the statistical excerpt consists of $\boldsymbol{n = 6}$ groups, the mean garbage volume generated form one citizen for one year has to be estimated for each single group (i.e. each village)

(4) $$\overline{\boldsymbol{v}}_{\boldsymbol{av}}(\boldsymbol{i}) = \frac{\boldsymbol{V(i)}}{\boldsymbol{N(i)}},\ \boldsymbol{i = 1, 2, \dots, n},\ \boldsymbol{n = 6},$$

and for the entire statistical excerpt

(5) $$\overline{\boldsymbol{V}}_{\boldsymbol{av}} = \frac{\boldsymbol{V_s}}{\boldsymbol{N_s}} = \boldsymbol{0,274}\ [\boldsymbol{m^3}].$$

In previous studies [2] it has been specified that $\boldsymbol{1}\ [\boldsymbol{m^3}]$ weights $\boldsymbol{218,2}\ [\boldsymbol{kg}]$. Therefore *the volume transformation coefficient of garbage in garbage weight is*

(6) $$\boldsymbol{k_{w/v} = 218,2}\ [\boldsymbol{kg/m^3}].$$

As of this fact and from (4) and (5) it is clear that the mean garbage weight generated by one citizen for one year for every single group and for the entire statistical excerpt is

(7) $$\bar{\boldsymbol{t}}_{\boldsymbol{av}}(\boldsymbol{i}) = \boldsymbol{k_{w/v}}\overline{\boldsymbol{v}}_{\boldsymbol{av}}(\boldsymbol{i}),\ \boldsymbol{i = 1, 2, \dots, n},\ \boldsymbol{n = 6},$$

(8) $$\overline{\boldsymbol{T}}_{\boldsymbol{av}} = \boldsymbol{k_{w/v}}\overline{\boldsymbol{V}}_{\boldsymbol{av}} = \boldsymbol{59,8}\ [\boldsymbol{kg}].$$

The mean garbage volume $\overline{\boldsymbol{V}}_{\boldsymbol{av}}$ and the mean garbage weight $\overline{\boldsymbol{T}}_{\boldsymbol{av}}$ generated by one citizen for one year for every single group and for the entire excerpt are illustrated in fig. 2 with blue and red colour respectively. From fig. 2 one can clearly see that the efficiency of the conducted by the government, local authorities and ecological organizations explanatory campaigns aimed at improving the culture of consumption is better for villages 1, 2 and 4.

In order to achieve good accuracy of planning and organization of irregular dunghills recultivation activities it is necessary also to determine the statistical reliability of the statistical estimations (5) and (8). It is appropriate to use the following random variable [3]

(9) $$\boldsymbol{T} = \frac{\overline{\boldsymbol{V}}_{\boldsymbol{av}} - \boldsymbol{E}[\boldsymbol{V}_{\boldsymbol{av}}]}{\boldsymbol{\sigma}\sqrt{\boldsymbol{N_s}}},$$

Whose possible (particular) values will be marked with *t* in the sequel.

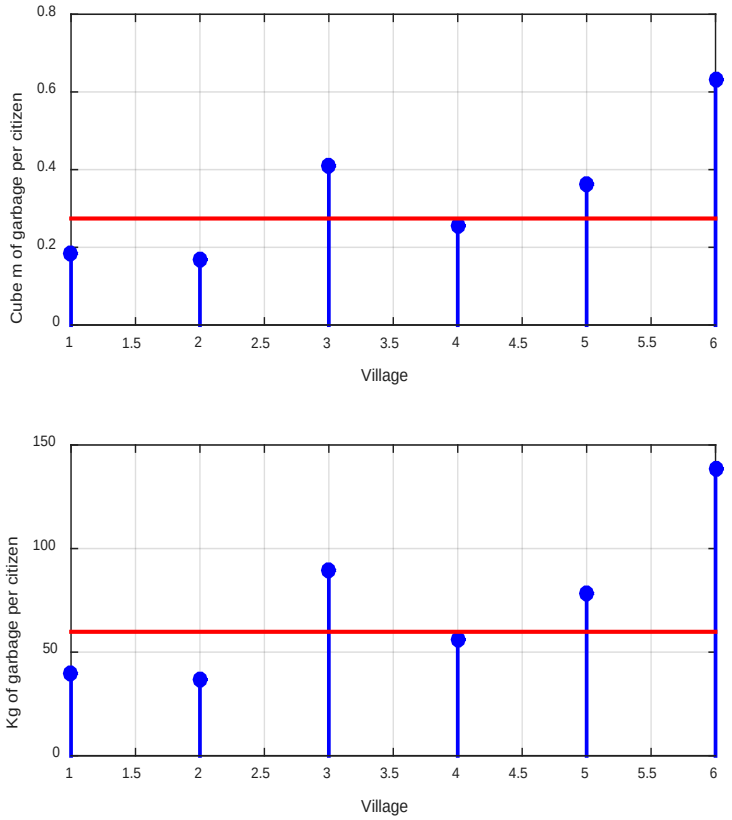

Fig.2. Mean garbage volume and mean garbage weight generated by one citizen for one year

In (9) $\boldsymbol{E[V_{av}]}$ is the mathematical expectation of the random variable "garbage volume generated by one citizen for one year", σ is the corrected value of the root mean square (RMS)

(10) $$\boldsymbol{\sigma = \sqrt{\frac{N_s - 1}{N_s} D_g}},$$

and $\boldsymbol{D_g}$ is the general variance of the whole statistical excerpt

(11) $$\boldsymbol{D_g = \frac{1}{N_s}\sum_{i=1}^{n} N(i)[\overline{v}_{av}(i) - \overline{V}_{av}]^2}.$$

In the beginning of twentieth century British scientist-statistician William Sealy Gosset, who worked under the pen name Student [4], had proved that the random variable (9) has a *Student distribution* with $\boldsymbol{k = N_s - 1}$ degrees of freedom.

Student's density of distribution is [3]

(12) $$\boldsymbol{f(t, N_s) = B_{N_s}\left(1 + \frac{t^2}{N_s - 1}\right)^{-\frac{N_s - 1}{2}}},$$

as here

(13) $$\boldsymbol{B_{N_s} = \frac{\Gamma(N_s)}{\sqrt{\pi(N_s - 1)}\Gamma(\frac{N_s - 1}{2})}},$$

and $\boldsymbol{\Gamma(*)}$ is *the gamma function*.

As it can be seen Student's distribution depends only on excerpt's volume $\boldsymbol{N_s}$ and does not depend on unknown parameters $\boldsymbol{E[V_{av}]}$ and $\boldsymbol{\sigma}$. This characteristic is its big merit. Considering that $\boldsymbol{f(t, N_s)}$ is even function of $\boldsymbol{t}$ the probability the value of the random variable (9) to belong to the interval $\boldsymbol{(-t_\gamma, t_\gamma)}$ is

(14) $$\boldsymbol{P\left(\left|\frac{\overline{V}_{av} - E[V_{av}]}{\sigma\sqrt{N_s}}\right| < t_\gamma\right) = 2\int_0^{t_\gamma} f(t, N_s)dt = \gamma}.$$

Here $\boldsymbol{\gamma}$ is so called *confidence probability* or *reliability of interval estimation*. The meaning of these two terms gets clear after the inequality in the left part of (14) is replaced with its equivalent double inequality

(15) $$\boldsymbol{P\left(\overline{V}_{av} - t_\gamma\sigma\sqrt{N_s} < E[V_{av}] < \overline{V}_{av} + t_\gamma\sigma\sqrt{N_s}\right) = \gamma}.$$

Equation (15) means that with probability $\boldsymbol{\gamma}$ the mathematical expectation $\boldsymbol{E[V_{av}]}$ is in the interval

(16) $$\boldsymbol{\left(\overline{V}_{av} - t_\gamma\sigma\sqrt{N_s}, \overline{V}_{av} + t_\gamma\sigma\sqrt{N_s}\right)},$$

calculated using the results from the measurements.

From (14) one can see that having $\boldsymbol{N_s}$ and $\boldsymbol{\gamma}$ the parameter $\boldsymbol{t_\gamma}$ should be calculated from equation

(17) $$\int_0^{t_\gamma} \boldsymbol{f(t, N_s)dt} = \frac{\gamma}{2}.$$

Finding a solution for (17) is relatively difficult computing task. Fortunately, today in the Internet can be found websites with "calculators" or with detailed tables using which the parameter $\boldsymbol{t_\gamma}$ can be defined by given excerpt volume N_s and confidence probability $\boldsymbol{\gamma}$. For example, from [5] we can see that by $\boldsymbol{N_s = 3940}$ and $\boldsymbol{\gamma = 0,90}$

(18) $$\boldsymbol{t_\gamma = 1,645}.$$

From (10), (11) (18) it is determined that

(19) $$\boldsymbol{D_g = 0,0160[(m^3)^2]}, \qquad \boldsymbol{\sigma = 0,1265[m^3]},$$

$$\boldsymbol{t_\gamma \sigma \sqrt{N_s} = 0,0033[m^3]}.$$

As we can see the estimation is very accurate because

(20) $$\frac{\boldsymbol{t_\gamma \sigma \sqrt{N_s}}}{\boldsymbol{\bar{V}_{av}}} = \frac{\boldsymbol{0,0033}}{\boldsymbol{0,274}} = \boldsymbol{1,2}\%.$$

Therefore, with probability $\boldsymbol{\gamma = 0,90}$ the mathematical expectation of garbage volume generated by one citizen for one year lies in the confidence interval

(21) $$(0{,}274 - 0{,}0033,\ 0{,}274 + 0{,}0033)[m^3],$$

Whose relative width is only 2,4%.

3. Conclusion

In this paper using data obtained from UAV the dependence between number of population in six villages in Shumen municipality and their irregular dung-hills' size is statistically estimated. The usefulness of the obtained results for government, local authorities and ecological organizations ensues from the following two facts.

First, they allow precise planning, organization and execution of irregular dunghills recultivation in the entire area of Shumen municipality.

Second, they give the opportunity for objective conclusions about conducted explanatory campaigns' efficiency aimed at increasing society's culture of consumption.

REFERENCES:

1. Population register towards year 2011, NSI: http://www.nsi.bg/bg/content/3078/%D0%BD%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BF%D0%BE-%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D0%B8-%D0%BE%D0%B1%D1%89%D0%B8%D0%BD%D0%B8-%D0%BD%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8-%D0%BC%D0%B5%D1%81%D1%82%D0%B0-%D0%B8-%D0%B2%D1%8A%D0%B7%D1%80%D0%B0%D1%81%D1%82-%D0%BA%D1%8A%D0%BC-01022011-%D0%B3
2. Final report according to contract "Analysis of morphological content of daily waste generated in Shumen municipality for one year – four seasons", October 2016 (in Bulgarian).
3. V. E. Gmurman, Theory of probabilities and mathematical statistics, Academic school, Moscow, 1977, 477 pp. (in Russian)
4. https://ru.wikipedia.org/wiki/%D0%93%D0%BE%D1%81%D1%81%D0%B5%D1%82,_%D0%A3%D0%B8%D0%BB%D1%8C%D1%8F%D0%BC_%D0%A1%D0%B8%D0%BB%D0%B8
5. https://www.kontrolnaya-rabota.ru/s/teoriya-veroyatnosti/tablica-studenta/?n=3940&p=0.90.
6. Andreev A., Markov M. Geographic information systems. NMU-Shumen, 2009, ISBN: 978-954-9681-46-8, p. 189.
7. Andreev A., Markov M. Guide to exercises in geographical information systems. NMU-Shumen, 2009, ISBN: 978-954-9681-47-5, 222 p.
8. Andreev A., Geo-information technologies for modeling of security disaster. Collection of scientific works, MATTEX Shumen's university "Bishop K. Preslavski "2012.

Author's name: PhD student eng. Monika Bedzheva
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Geodesy"
E-mail: m.bedzheva@shu.bg

Author's name: PhD student eng. Stefan Dobrev
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Geodesy"
E-mail: st.dobrev@shu.bg

NEW CATEGORIES OF RISK

Donika V. Dimanova

ABSTRACT: *The changes that have occurred in the geostrategic situation in Europe and the world lead to changes in the nature and the meaning of the destabilizing risk factors and the threats for security. New categories of risk appear in contemporary society. Unlike the situation in the past, at the moment the existing risks are multiple and multi-directional and for that reason they are difficult to predict and assess. At the expense of the reduced risk for military conflicts the share of the potential reasons for emergence of risk, resulting from serious economic, social and political difficulties, has grown.*

KEYWORDS: *Risk, Risk management, Risk factors, Types of risk.*

1. Introduction

Risk is a chance event that develops dynamically in the course of human evolution and the accompanying development of technologies, technique, society and nature. For a comparatively short period of time there has been a remarkable evolution regarding risk understanding. It is difficult to find sustainable solutions of new global and asymmetrical in their nature risks arising from: international terrorism and the distribution of weapons for mass destruction; cyber crime and cross-border organized crime; illegal migration and migrant flows; distribution of harmful technology; information manipulation; as well as financial and economic crises; poverty, natural disasters and large-scale ecological, industrial accidents and environmental disasters.

The tendencies for security in the global and regional environment have shown that the development of such processes will continue to be highly dynamic, difficult to determine, ambiguous and complex to predict.

In this context the aim of the research report is to analyze the new risks that have emerged.

2. Research report

The global society faces the risks related to human decisions. The changes in the nature of wars, as well as the detailed research on the risk in the global post-modern violence, are of exceptional interest.

The risk of terrorism is a new type of violence, having a growing scope. Its global nature, detrimental consequences and the possibility for the terrorists to be recruited through radicalization and dissemination of propaganda on the Internet turn it into a great risk for the society. The

possibilities for using radioactive materials, toxic substances and biological agents for the purposes of terrorism are increasing.

Undoubtedly, the study of the risks of terrorist acts is a complex task. It can only be noted that the threats for terrorist acts, not only for Bulgaria but also worldwide, are highly probable and can cause instability in the world at the beginning of the 21th.

The risks related to the distribution of nuclear and other weapons for mass destruction (WMD) are growing. One of the basic reasons for the above fact is the increasing interest in their acquisition on the part of different countries. WMD can be used for physical destruction and for causing outbreaks of epidemics among large groups of people. The risks for using the WMD against international contingencies working on peace-keeping, rescue or other missions in different regions of the world are increasing.

The existence of regions of increasing or prolonged conflict enhances the risk for acquisition of weapons, products or technology for double use by countries in risk or extremist organizations [6].

The risk of cross-border (international) organized crime involves activities related to corruption, economic crime, production and traffic of drugs, traffic and exploitation of people, smuggling, production and distribution of counterfeited or forged currency and documents, cyber crime, money laundering, etc. Such acts are illegal and they lead to quick and large-scale profit. In most cases the profit from such activities can occupy a substantial part of the resources of a country and thus the political stability and the sustainable development of the affected country can be threatened.

Figure 1 shows assessment of the share of key illegal markets in Bulgaria for the period 2016 – 2017.

Many of the crime networks in Bulgaria control legal business structures which eases the process of money laundering. It can be said that the degree of penetration of the organized crime in the legal economy of Bulgaria is considerably greater than the level in Western Europe. The overall value of the researched criminal markets in 2017 amounts to almost 2.5 billion lv or 2.5% от GDP [4].

Organized crime groups use corruption as an instrument for making their criminal acts easier and for avoiding legal punishment. As far as corruption is concerned, there have been various tendencies in different criminal activities in Bulgaria over the last few years [4]. As for the drug market and the market of sex services, there is a tendency for restriction of the corruptive influence. This is due to the increased use of the Internet for finding clients, which reduces the contacts with officers from the Ministry of Interior. Thus, the corruptive pressure upon the former is reduced. The

influence of corruption in trafficking is declining because of the decline in migration pressure.

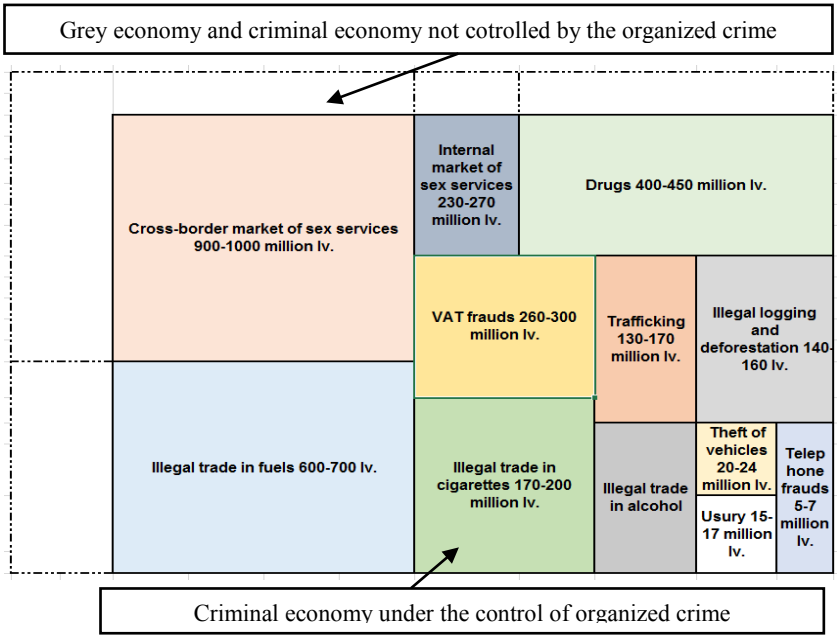

Fig.1. Assessment of the volume of key illegal markets in Bulgaria (2016 – 2017)

Many of the crime networks in Bulgaria control legal business structures which eases the process of money laundering. It can be said that the degree of penetration of the organized crime in the legal economy of Bulgaria is considerably greater than the level in Western Europe. The overall value of the researched criminal markets in 2017 amounts to almost 2.5 billion lv or 2.5% от GDP [4].

Organized crime groups use corruption as an instrument for making their criminal acts easier and for avoiding legal punishment. As far as corruption is concerned, there have been various tendencies in different criminal activities in Bulgaria over the last few years [4]. As for the drug market and the market of sex services, there is a tendency for restriction of the corruptive influence. This is due to the increased use of the Internet for finding clients, which reduces the contacts with officers from the Ministry of Interior. Thus, the corruptive pressure upon the former is reduced. The

influence of corruption in trafficking is declining because of the decline in migration pressure.

According to the assessment made by the Center for the Study of Democracy, regarding the threats by the organized crime in Bulgaria, there are new increasing threats forming:

• The share of the market for illegal fuel trade is growing. This fact is alarming because of the importance of petrol products in many key branches of the economy;

• The market and the use of cannabis is considerably growing. The trade in drugs is an important source of finance for criminal and some terrorist groups and organizations. The profit is used for growing corruptive activities, for destabilizing the economy, for infiltration in legal businesses, for creation of new 'grey areas' in the economy, etc. The battle against drug trafficking is getting more complex because of the use of modern communication media and transport, the development of modern technology, the free movement of goods and services, as well as the broadening of the areas where drug substances are produced;

• The introduction of crypto currency creates additional chances for money laundering;

• The frequency, the range and the diversity of cyber crimes in Bulgaria are growing;

• The integration of information technology in market functioning, related to people trafficking, the offer of sex services, the distribution of illegal goods and services adds to the efficiency of crime groups.

Risk of telephone frauds. Since the beginning of 2010 there has been a stable growth in the number of telephone fraud victims. According to data of The Ministry of Interior and The Prosecutor's office on that kind of crime has been observed and has become socially important.

According to the data based on a national research on crime, conducted in 2018, every fourth Bulgarian (27%) was a target of telephone fraud over the last 5 years, while the share of the actual victims was under 1% of the population [4].

There is still no official statistics of the volume of the profit from telephone frauds. As the data from the Prosecutor's office show [2] the amount of the profit from such frauds is gradually growing. It was 2.4 million lv. in 2012 and reached 6.7 million lv. in 2015. The amount of the damages for 2017 was 8 million lv.

Not only elderly people but also young people and children were victims of this type of fraud. The areas where such campaigns occur are broadening. Despite the fact that phone frauds are public, the number of the registered victims is continually growing. Very often investigations do not

reach the organizers of the criminal groups but end in catching 'mules' or mediators. It can be said that the percentage of revealed crimes of that type is very low (about 10%) and there have been no trials against organized crime groups.

The difficulties in revealing such crimes are various:

• The crime groups are quite flexible, mastering different logistic approaches and they successfully exploit the fears and trust of predominantly elderly people;

• Most victims are ashamed of their naivety and do not report the fraud;

• The fragmentary structures of such crime activities make it difficult to prove who was involved in a phone fraud and the income is guaranteed at a low risk of arrest and punishment.

Risk of corruption. As it has already been pointed out, organized criminal groups use corruption as an instrument for making their criminal acts easier. However, corruption is realized in a more comprehensive way – through the conquest of the state. This refers to the practice of many influential figures to ensure a preferential attitude from the state through complex corruptive schemes, bargains and other acts of trespassing. Such practices are achieved through influencing the functioning and the policy of the state institutions in order to satisfy private interests at the expense of the social welfare [1].

The risk of corruption significantly affects the social environment, the economic development and the international image of the country. As it has already been pointed out, the risk of corruptive activities in the high levels of power is greater as it is more difficult to prove. The disclosure of corruption is very often related to particularly great interests and is accompanied by severe resistance. In most cases corruptive activities create prerequisites for other crimes and violations. Some of the most often affected structures are those of the legal institutions, the legal system and the state administration on a local level. The analysis shows that a great part of the corruptive practices in the structures of the executive power are related to procedures of public procurement. Considerable criminal financial flows are generated also by:

- Abuse of grants in the agriculture;
- Abuse of finance for health services;
- Parallel export of pharmaceutical products;
- Illegal logging and trade with timber, etc.

Since 2000 the share of the IT-risk (cybercrime) has gained particular importance. It is also a global and anonymous threat for the information systems of the private companies and the state institutions alike. The quick growth of computer technology and the industrial globalization creates

prerequisites for the emergence of risk of penetration, manipulation and destruction of information systems. Malicious influences upon information systems and networks can lead to hindrances and blockings of the normal functioning of systems that are important for the economy, the financial area and the state government.

The enhanced risk of cybercrimes is determined by:

• The great number of users, having access to the information systems of banks, companies, organizations and institutions;

• The growing number of financial transactions, done through the Internet, with low reliability and protection of the information networks;

• The vast range and volume of administrative, legal, financial and other services and products those are offered and provided through the Internet;

• The used passwords, codes and biometric identifications that are complex for many users but not reliable enough against hackers, pirates, viruses, etc.

According to data by experts [4], over the last few years the fishing attacks have been dominating and becoming more often, as well as the "Compromised business e-mail" (CBE), ransomware, denial of services and Internet-based frauds in the trade of financial products and services. Figure 2 shows the types of registered cyber accidents for the period 2014-2017.

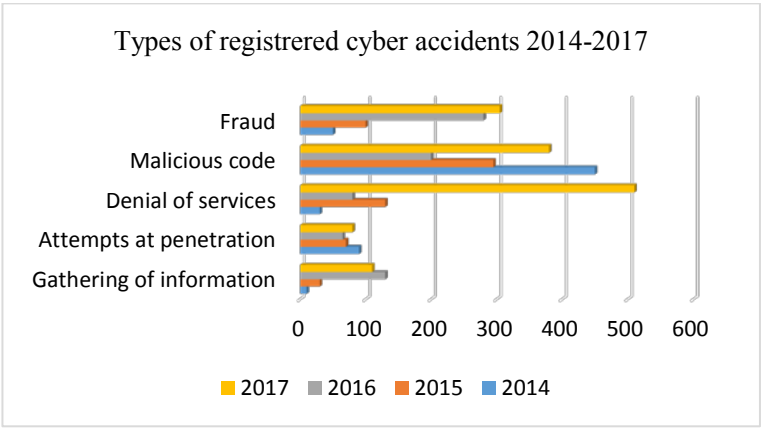

Fig.2. Types of registered cyber accidents (2014 – 2017)

Over the last few years there has been a stable tendency for growing of most types of cybercrime in Bulgaria. The research shows that in 2016 about 24% of the Bulgarian business was affected by cybercrime, compared

to 10% in the preceding year [10]. According to data from a national representative research for 2017, the most common accidents in the context of business are related to viruses, affecting about 8% of the victims of cyber-attacks, as compared to 1% in 2011 [3].

Our country is frequently mentioned in world rankings related to the measurement of cybercrimes. This means that the Bulgarian ICT infrastructure is actively used by international organized cyber criminals who carry out different types of cyber-attacks worldwide.

The traditional understanding of the nature of information is developing in a new trend. The information in the electronic media, having advantages over the rest of the media for communication, can be used as an instrument for causing conflicts and contradictions that create a risk of information manipulation. Mass media can have a negative psychological effect upon the population and in a global aspect (through the use of different ways for disinformation and intentional twisting of information arrays) can be used for the purposes of propaganda.

The risk of having disallowed access to classified information presents a potential threat for the security of the country. It is expressed through [5, 6]:

- Loss or deletion of classified information;
- Violating the principle „necessary to be known";
- Incorrect or ungrounded classification, etc.

The growing vulnerability due to unregulated access or destructive influence is determined by the quick development of information technology and its turning into a necessary resource for effective carrying out of the functions of the governmental body and the local self-regulation. In that manner, the possibility for information acquisition by foreign special services, people or groups and its use against the national security is increased.

The systematic risk for the classified information suggests the necessity for control of the range, the goals, the purposes and the ways and rules for the building of communication-information systems of all the bodies.

Migration risk. Since 2014 as a result of the total opening of the labour market of the EU for Bulgarian citizens, the net migration has been increasing to 4-15 thousand people per year. Increased migration pressure is observed, mainly from Syria. Afghanistan and Iraq. The territory of Bulgaria is used as a transition point for the illegal migration to Western European countries.

The existence of conflict areas in Afghanistan, the Middle East and Northern Africa, the emergence of Islamic State in Iraq and Syria, as well as

social and economic problems, political instability and internal conflicts leads to the appearance of great groups of refugees. The share of those who emigrate for economic reasons and seek a better life is not to be underestimated.

According to data by Directory „Migration“ at the Ministry of Interior during the period 2013-2015 the number of the detained migrants entering the Bulgarian-Turkish border was much higher in comparison to the period 2016-2017 (most refugees were detained at the exit, Fig. 3). This is due to the agreement signed in 2016 between Turkey and the EU for stopping the migration flow and strengthening the border control along the Bulgarian border.

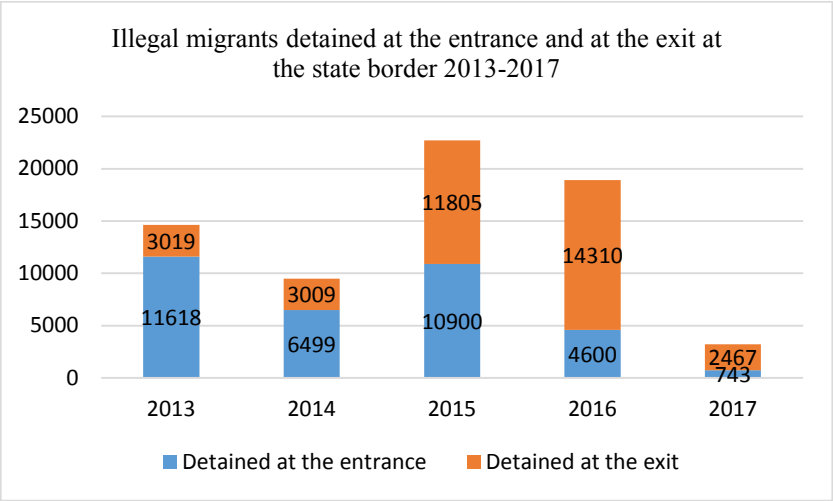

Fig.3. Illegal migrants detained at the entrance and at the exit at the state border (2013 – 2017)

The increase in the migration flows can lead to a lasting change in the demographic and ethno-religious structure of the population of the accepting country. As a result of this the immigrants can cause alarm among the population, as well as social tension, protests against the settling of refugees; they can create conditions for the rise of xenophobic and extreme nationalist organizations.

The migration processes create risks related to [6]:

• Penetration, passing or staying (on our territory) of people creating risk for the national security, including people associated with the activities of terrorist formations, organized crime groups and foreign special services;

• The search for forged Bulgarian documents for identity and other official types of documents;

• The corruptive pressure on the border controlling bodies can create conditions for discrediting of the country, considering the obligations for protection of the outer border of the EU and the international priorities for inclusion in Schengen area;

• A direct threat to the life and health of the people involved in trafficking. The greatest risk is related to the possibility of coercion and exploitation in different forms (sexual exploitation, pick-pocketing, begging).

Risks for the financial security [5, 6]. They are related to:

• Tax frauds;

• Legalizing of the funds that have been acquired in an illegal way;

• Criminal assaults against financial institutions, financial assets of people and legal entities or against the assets of such institutions;

• Occurrence of liquidity problems in certain institutions, which can destroy the stability of the financial and crediting system;

• Doubtful operation through the stock exchange, including non-transparent operations with shares, money laundering etc.;

• Illegal financial activities (usury);

• Risks related to internet banking, creation of forged documents and the abuse of companies, etc.

The tax frauds with VAT are considered to be some of the most significant crime markets in the EU. According to a report by the European Commission [9], the potential annual losses due to organized VAT frauds are estimated to be about 150 billion Euros. Based on expert evaluations [4] at the moment it is suggested that the current loss in Bulgaria amounts to 250-300 million lv. annually.

Vat frauds usually pursue one of the following goals [4]:

• Necessity for documentation of smuggled goods or goods imported through customs frauds, as well as goods produced in the grey economy sector (the frauds in the trade in agricultural products, fuel, imported Chinese and Turkish cargo);

• Necessity for documentation of supplies (expenses) which were actually performed. However, the invoices in accordance with Bulgarian law (frauds in building) are missing;

• Documented realization of expenses that were not real. The goal is to reduce the amount of the VAT that is to be paid;

• Unlawful reimbursement of amounts of money from the budget in the form of VAT.

A typical feature of the VAT frauds is that they are easily adapted to the changing circumstances; start to change into more complex schemes and more legal entities from many countries participate in them. At the same time the main instrument against organized tax frauds provided by the law to the National Revenue Agency is the deregistration of companies related to people presenting risk. The facilitation of that type of frauds is associated with the offer of diverse electronic payment services, the introduction of digital technology in storing and exchange of information, the use of crypt technology, the use of electronic banking and appliances for secure access to internet-based services.

Some of the tools for legalization of finance, acquired in a criminal way are: the money laundering, smuggling and customs frauds. An increase in the risk of smuggling of excise goods is observed. As a result of this, quick profit is realized with a minimal investment and relatively low risk for the participants involved in the criminal acts. The introduction of crypto currency creates additional possibilities for money laundering of illegally acquired funds.

Unlawful finance activities are: usury, loans from pawnshops, loans from companies for quick credits and racketeering. The data from a national representative survey among the population, done by the Center for the Study of Democracy in 2017 show that 40.4% of the families have had at least one loan from a financial institution or private persons. 1.1% of the people pointed out that they had drawn a loan from a private person (usurer), 1% - from a pawnshop and 5.9% - from a company for quick credits (Fig. 4). It can be summed up that about 23 thousand families used loans from usurers and the same number – from pawnshops.

Over the last two decades the unlawful provision of credits had a continuous presence in the regional center towns and cities. The unlawful provision of credits is of two types: usurers, using legal companies as a cover and usurers against the law. A new trend is the formation of companies collecting debts or the so called collector companies. Another type of risk is related to the new organized types of coercion and racketeering, practiced by officials usually on a local level. The lack of a precise regulation frame for the work of such companies suggests that the abovementioned types will create risk in the coming years.

Risks for the economy. Economic activities have a serious impact on the quality and basic characteristics of social life. The inability of the economy to provide growth of the real income of the people or keep the level of the standard of living can put all the social systems, including the political one, under pressure.

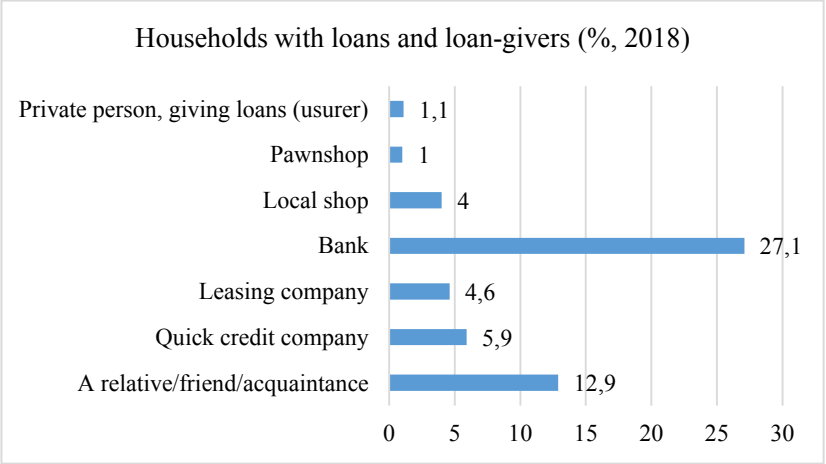

Fig.4. Households with loans and loan-givers (%, 2018)

The deepening of economic and social differences in Europe and the region are prerequisites for insecurity and new threats for stability. The unstable economic situation, the weak role of the state and the low standard of living reduce the chances for protection of national interests and increase the risk of foreign financial, technological, raw material and other type of dependency.

Ecological risks are risks for the environment, creating threats for the life and health of the population. These are: the polluted air, soil and waters and they can be of cross border nature. The consequences of such risks can lead to diseases, destruction of material or natural resources, great financial and economic losses.

Ecological risks stem from [6, 7]:

• The pollution of air, water, coastline, caused by industry or industrial accidents with harmful emissions;

• Transport accidents, related to the transport of dangerous cargoes, including the transportation of petroleum products by ships;

• Terrorist activities using substances that are particularly dangerous for the environment;

• Deliberate causation of accidents resulting from diversions related to oil pipelines, gas pipe lines, electricity network, thefts and traffic of radioactive materials;

• Natural disasters resulting from anthropogenic and technology-related factors;

• Changes in climate;

• The lack of investment for building wastewater treatment systems and abatement equipment to treat the emissions in the air and water;

• Imperfections and omissions in the regulation system, ineffective control and cooperation between the law-enforcement institutions.

The main sources of ecological risk are the big power plants, metallurgy, extractive and food industry, as well as certain small and medium factories in most regions of the country. Consequently, 'risky' are those establishments that produce, recycle, use and store or transport pathogenic, toxic, radioactive, fire hazardous and explosive substances and materials, or are engaged in activities that are potentially dangerous for the personnel, the population and the environment.

Ecological risk can be examined as part of the problem of the global insufficiency of resources. The dependency of the countries on vital resources such as energy, water, raw materials and food, enhancing the risk of a crisis, is deepening. The problems in that area are turning into one of the most serious risks for all countries, no matter what the degree of their economic development and resource security is.

Ecological risk can be regarded as part of the problem of the climate change. The climate changes can lead to famine, diseases and natural disaster, the appearance of large refugee flows and severe conflicts in the future.

Risk of natural disasters, industrial accidents and catastrophes. This type of risk is increasing recently and has to be reported.

The events, resulting from natural disasters include: space cataclysms, earthquakes, floods, drought, landslides and collapses, severe winds, hurricanes, tsunami, dust storms, forest and plane fires, hail, snowfalls and icing, sources of contagious diseases and epidemics of people, animals and plants. Any of the abovementioned events can occur on the territory of Bulgaria. Most of them – snowfalls and snowstorms and icings, landslides and collapses, hails and some others happen annually or are in a constant process of development.

The events arising from human activities can be: accidents in establishments with risky production, vehicle crashes, terrorist activities, mass trespassing of legal order in the country, financial, economic or political events that threaten the normal existence of large groups of people.

Economic damages caused by floods, fire fires, hot air waves, drought and other extreme natural and climate events over the recent decades have considerably grown in number in comparison with the victims and the

damages caused by military conflicts. The probability of this tendency to deepen is high and there is a necessity for the creation of efficient management bodies.

3. Conclusion

Over the recent decades there have been risks for two types of dangers [7, 8]:

• Generally recognized threats for ecology caused by negative, anthropogenic influences combined with the impact of the global natural processes of climate change;

• The quick development of top technology in the civil and military sector of a limited number of countries causes disruption between the continuously growing threats of natural and technology-based character and the ability of the world community to counter the former in an adequate manner.

The following threats can be added to the above mentioned ones: threats of military conflict, great industrial accidents, dangerous pollution, migration, the building of social, economic, resource and cultural and civilization disharmony between the different regions and states in the world.

The global society faces risks related to human decisions. That is why it cannot be said that there exist universal solutions for risk prevention that can be applied equally for every single occasion by the people making management decisions. Despite the above fact, the analysis and risk evaluation are expected to provide an exact decision that can provide an answer to the questions for risk reduction.

REFERENCES:

1. Conquering the state. Countering the administrative and political corruption. Center for the Study of Democracy. 2016.
2. European Commission: European Commission proposes far-reaching reform of the EU VAT system Brussels, Press Release, 4 October 2017.
3. Evaluation of the threats by organized crime in Bulgaria. Center for the Study of Democracy. 2018.
4. Hristov, P., The End of the Concepts of National Security// Military journal, 1997/vol.1.
5. National representative study of business. Center for the Study of Democracy.2018
6. Popchev, I., Strategies for Risk Management, a Lecturer's Notes. Sofia, 2014.
7. PWC, Global Economic Crime Survey, 2016 – Bulgaria Country report.
8. Research on the crime of fraud by telephoning for the period 2011-1015. Prosecutor's office of Republic of Bulgaria.
9. Security environment – risks and threats for the national security for 2010. Summary of the annual report by the State agency 'National security' for the state of the national security for 2010.

10. Tomov, V., Hristov, P., Nenova, A., Ecological Security. Varna. Varna Free University “Ch. Hrabar”, 2007.

Author’s name: assoc. prof. eng. Donika V. Dimanova, PhD
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems“
E-mail: d.dimanova@shu.bg

PRESENT APPROACHES TO THE DEVELOPMENT OF RADARS FOR UNMANNED AERIAL VEHICLES

Borislav Y. Bedzhev

ABSTRACT: *Today the radars, based on unmanned aerial vehicles, have great importance for large number of projects and applications. The analysis of the positive features of these radars shows that they are result of applying of specific modes of transmission and ultra-high frequency hardware. Accounting this situation, our paper aims to give a systematical description of the present approaches to development of radars for UAVs, providing their effectiveness.*

KEYWORDS*: Radars based on unmanned aerial vehicles, complex phase manipulated signals.*

1. Introduction

Today the unmanned aerial vehicles (UAVs) are widely used in many areas such as: traffic control, exploration of natural resources, observation of ecological situation, reconnaissance of the wild nature and so on. In order to perform their missions, the UAV are typically equipped with light and infrared cameras. Unfortunately, in cases of fog, rain and/or smoke the efficiency of the optical sensors is small. Due to this reason often the UAVs have to possess radio ranging sensors (radars), because the radio waves provide ability for tracking of the objects in hostile optic environment.

With regard to the important role of the radars for UAVs, they are object of intensive scientific and technical researches, aiming improvement of their abilities. The scrutiny of the materials, published in the scientific and technical literature or presented in the specialized conferences, shows that the radars, developed for usage in UAVS, will possess the following peculiarities:

- processing of the received signals directly in the antenna output without any amplification and demodulation (i.e. directly on the carrier frequency);
- usage of quasi continuous complex phase manipulated (PM) ultra wide band signals with very small spectral density;
- practically 100 - percents effective signal processing;
- excluding of any frequency converters and intermediate frequencies from the receivers;
- easiness of the modification and the adaptation of the devices to solving different problems;

- small volume and weight;
- high level of automation of the process of their manufacturing;
- flexible structure due to the usage of large number of specialized or universal modules;
- significant reliability and working readiness.

The analysis of above listed positive features shows that they are result of the applying of the so-named ultra wide band radio technologies [1], [2], [3], [4], [5], [6]. More specifically, the radio signals, exploited in present radars, have complex inner structure, containing great number of phase manipulated very short elementary pulses (chips) with duration τ_0. In the radar receivers the long signals with duration $N\tau_0$ are compressed during the processing. In fact, the signal processing of complex phase manipulated signals brings a significant improvement of the *signal-to-noise ratio* (SNR), named processing gain. This feature of complex signals is used in the development of present radars, used in UAVs, in order to ensure both very large range of observation and high resolution of the objects.

Unfortunately, in general the effectiveness of the radars is limited by the contradictions among the following main factors [1], [2], [3], [4], [5], [6]:

- the enhancement of the resolution requires the duration of the elementary pulses (chips) to be shortened, but it cannot be smaller than the time of the performance of operations during the signal processing in the radar transmitters and receivers;
- the usage of a single antenna allows the volume and weight of the radars to be reduced but this construction leads to an undesirable interference of the transmitter over the receiver.

With regard to this situation, our paper aims to give a systematical description of the present approaches to development of radars for UAVs, used to solve the above mentioned contradictions.

The paper is structured as follows. First, the general block scheme of the advanced radars, developed for usage in UAVs, is considered. After that, the so-named quasi continuous mode of operation of radars, is clarified. At the end, some important conclusions are given.

2. Present Approaches to the Development of Radars for Unmanned Aerial Vehicles

The scrutiny of the materials, published in the scientific or technical literature or presented in the specialized conferences shows that the usage of the so-named quasi continuous mode of transmission satisfies simultaneously the main requirements, which have to meet the radars of UAVs. This approach will be explained in more details [5], [6] by means of the Fig. 1, Fig. 2 and Fig. 3.

Namely, on Fig. 1 the general block scheme of advanced radar, developed for implementation in UAVs, is depicted. It consists of two equal *digital solid-state radars* (DSSR1 and DSSR2), presented on Fig. 2.

In order to diminish the volume of the equipment, the DSSR1 and DSSR2 use alternatively a single antenna (A) during every base cycle, which duration is $2\tau_0,\ \tau_0 \leq 1[\eta S]$ (Fig. 3). The DSSR1 sends sound signals with duration τ_0 during the first half of the base cycle and DSSR2 sends sound signals with duration τ_0 during the second one (Fig. 3b). In order to avoid the undesirable mutual interference between DSSR1 and DSSR2, their transmitters use different carrier frequencies f_{c1} and f_{c2}, separated by appropriate protective frequency band. The *filters* (F1 and F2 respectively) and the *commutating device* (CD) ensure a deep decoupling (about 180÷200 [dB]) of DSSR1 and DSSR2. The proper work of the elements of the radar is provided by the *clock-pulses*, generated by the *synchronizer* (S) (Fig. 3b). The signals, processed in DSSR1 and DSSR2, are combined in a device of *hardware logic* (HL). A micro computer ($\mu Comp$), equipped with specialized peripheral devices, performs all control functions over the radar, including the visual presentation of radar images and their storage.

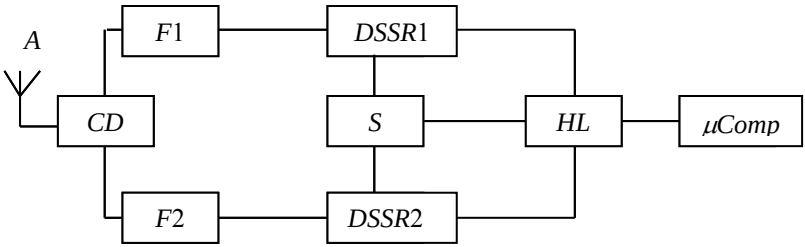

Fig.1. A general block scheme of advanced radar, developed for implementation in UAVs

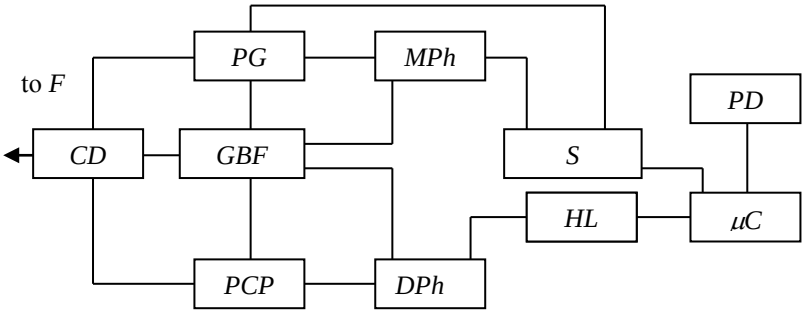

Fig.2. A general block scheme of digital solid-state radars (DSSRs), which are counterparts of advanced radar, developed for implementation in UAVs

The so-named *generator of the base frequency* (GBF) produces a very highly stabilized frequency f_0, which is practically free of phase noise. By means of filters the n-th adjacent frequency (nf_0) is selected and used as carrier frequency in other elements of the DSSRs, i.e.:

(1) $$f_{ck} = n_k f_{ck}, \;\; k = 1, 2.$$

The carrier frequency is amplified by the so-named *parametric generator* (PG). It is a special type of electrical microcircuit, which comprises a resonator camera and an active element (called parametric diode). The *modulator of the phase* (MPh) controls the duration of the generations of the PG and their phase. In fact, the MPh:

- allows PG to generate the frequency $f_{ck}, k = 1, 2$ only in respective time frames (with duration τ_0) during the base cycle (with duration $2\tau_0$);

- changes the phase of the carrier frequency from $0\ [rad]$ to $\pi\ [rad]$ in accordance with 0s and 1s of the *characteristic sequence* during the active periods of PG.

As a result, the scheme, depicted on Fig. 2, provides:

- generating of a very long quasi continuous sound radio signal with duration $2\tau_0 N, \;\; N > 10^3$, containing N elementary phase manipulated pulses (chips) (Fig. 3a);

- very low level of the short-term instability of the carrier frequency (10^{-8} instability for $150\ [\mu S]$).

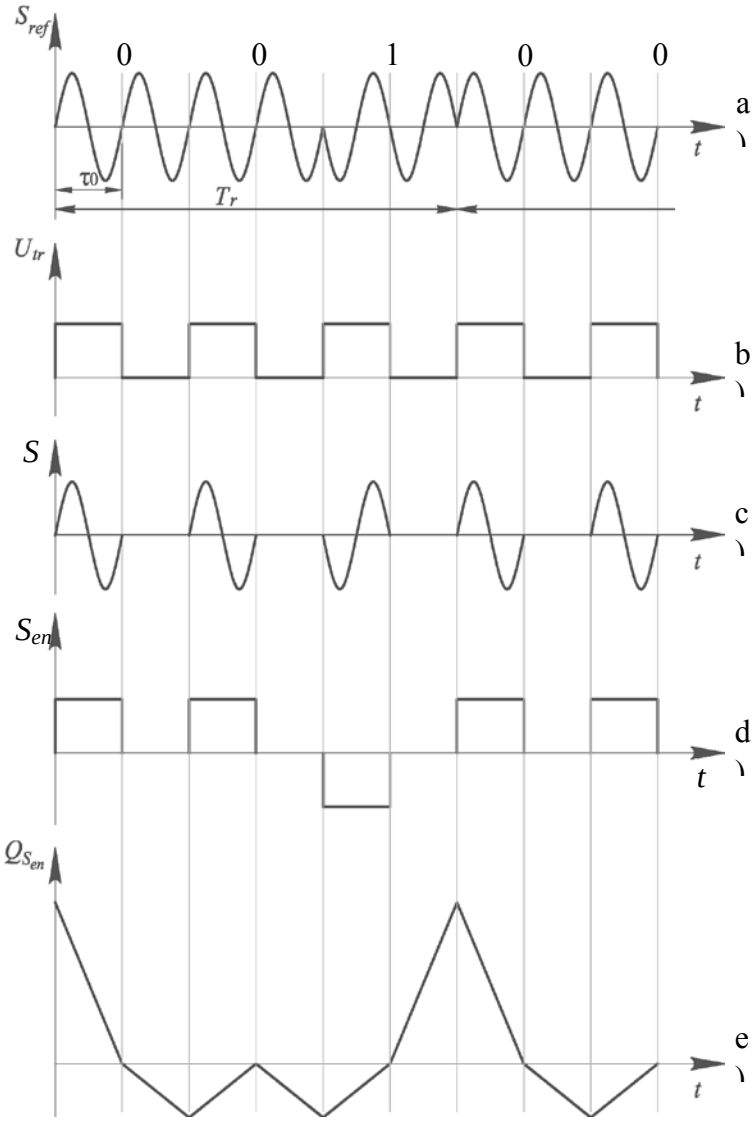

Fig.3. Quasi continuous mode of transmission of DSSR 1

Due to the extremely large duration of the sound signals, an average power of 1 $[W]$ of the radar transmitter is equivalent to N $[W]$ impulse

(instant) power. So, the improvement of SNR (processing gain) is greater than $30\ [dB]$. Consequently, exploitation of complex radiosignals enhances significantly the range of operation of the radars in a mode of low average consumption of the electrical power [5], [6].

The filtered frequency of the GBF is used not only in the PG, but also in the so-named *parametrical converter of the phase* (PCP). The construction of the PCP is very similar to the construction of the PG, but it mixes the echo-signals with a low power pattern signal, which frequency is $f_{ck}, k = 1, 2$. The PCP is a very sensitive device, which can work properly even if the echo-signals are weaker with about $120\ [dB]$ than the sound signals. It produces radio pulses (chips) which phase is proportional to the phase difference between echo-signals and pattern signal. This difference is processed by a *detector of the phase* (DPh) and after that - by *hardware logic* (HL). At the end, a *microcontroller* (μC) selects and storages the information for observed objects.

Now we shall clarify the peculiarities of the quasi continuous mode of transmission, proposed for exploitation in the advanced radars, developed for usage in UAVs.

First of all, we shall point out that the characteristic sequence can be: *maximal length sequence* (M-sequences), *Legendre sequence* or any other binary (or $\{0, 1\}$) sequence, which respective *phase manipulated* (PM) radio signal has *periodic auto-correlation function* (PACF) with small level of side-lobes [1], [2], [3], [4], [5], [6]. For instance, M-sequences are created by means of a linear recursive procedure which general form is:

$$v(i) = d_{n-1}v(i-1) + d_{n-2}v(i-2) + \cdots + d_0 v(i-n), \tag{2}$$

where:

- $v(i)$ is the new i-th element of the M–sequence;
- $v(i-1) = 0, v(i-2), \ldots, v(i-n)$ are elements of the considered M-sequence, obtained during the previous steps of the recursive procedure (2) (it is assumed that the initial elements $v(0), v(1), \ldots, v(n-1)$ are known);
- $d_{n-1}, d_{n-2}, \ldots, d_0$ are coefficients, belonging to a limited algebraic field (named *Galois Field* (GF)) and all algebraic operations in Eq. (2) are performed in GF(p) (i.e. modulo p, where p can be an arbitrary prime integer);
- the left side of the characteristic equation of (2) (noted often as "connection polynomial" of the *linear feedback shift register* (LFSR) hardware which realizes the recursive procedure (2)):

(3) $$x^n - d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \cdots + d_0,$$

is a primitive irreducible polynomial over GF(p).

It is known that the period of a M-sequence is $N = p^n - 1$. Their wide implementation in communication devices can be explained as follows. Let a PM signal $\{\zeta(i)\}_{i=0}^{N-1}$ uses a M-sequence $\{v(i)\}_{i=0}^{N-1}$ as characteristic sequence. This means that complex envelopes of the chips of the PM signal are generated by the rule

(4) $$\zeta(i) = e^{j\frac{2\pi l}{p}v(i)}, j = \sqrt{-1}, i = 0, 1, \ldots, N-1, 0 < l < p\ ,$$

In order to maximize the SNR, the receivers of the DSSR1 and DSSR2 evaluate the PACFs of the echo-signals. Unfortunately, side-lobes of the PACFs of the powerful objects can mask the main peaks of the PACFs of the weaker ones. In other words, when the contrast between the main lobe and the side-lobes of the PACF of the exploited signal is small then it is possible to miss objects during the radar observation. Due to this reason PM radio signals, which PACFs have small side-lobes, are the most favorable signals from implementation point of view. The PM signal (4) belong to the class of preferred signals, because its PACF is:

(5) $$Q_{\zeta\zeta}(r) = \sum_{i=0}^{N-1} \zeta(i)\zeta^*\langle i + r\rangle = \begin{cases} N, & r = 0, \\ -1, & r \neq 0. \end{cases}$$

In (5) the symbol "$\langle\ \ \rangle$" means "summing modulo p" and the symbol "$*$" – "complex conjugation".

As seen, all the side lobes of the PACF of the PM signal (4) are only -1 and the contrast between the main lobe and the side-lobes of the PACF is $(N + 1)/1$.

It ought to be emphasized that due to the simplicity of their processing, the binary M-sequences are most widely used (i.e. sequences, defined over the GF(2)) [4], [5], [6], [7], [8].

The usage of quasi continuous mode of transmission is explained in more details on Fig. 3, where for simplicity the shortest M-sequence with length $N = 2^2 - 1 = 3$ is presented. It is created by the linear recursive procedure

(6) $$v(i) = d_1 v(i-1) + d_0 v(i-2),$$

where $d_1 = d_0 = 1$ and $v(0) = v(1) = 1$.

All algebraic operations in Eq. (6) are performed in GF(2) and the characteristic equation of (6)

$$x^2 + x + 1, \tag{7}$$

is a primitive irreducible polynomial over GF(2).

It easy to verify that

$$\{v(i)\}_{i=0}^{2} = \{1, 1, 0\}. \tag{8}$$

For simplicity in Fig. 3a the "inverse" version of the characteristic sequence (8) is used

$$\{\bar{v}(i)\}_{i=0}^{2} = \{0, 0, 1\}. \tag{9}$$

The complex envelopes of the chips of the respective PM signal (Fig. 3c), generated by the rule

$$\zeta(i) = e^{j\frac{2\pi l}{2}\bar{v}(i)}, j = \sqrt{-1}, i = 0, 1, 2, l = 1, \tag{10}$$

are the samples of the digital signal

$$\{\zeta(i)\}_{i=0}^{2} = \{1, 1, -1\}. \tag{11}$$

The complex envelopes of the chips of the PM signal (11) and its PACF are presented on Fig. 3d and Fig. 3e respectively.

The DSSR1 sends sound signals with duration τ_0 during the first half of the base cycle (Fig. 3b) just as shown on Fig. 3. Analogously, the DSSR2 sends sound signals with duration τ_0 during the second half of the base cycle. As a result, the quasi continuous signal does not introduce additional side lobes in the PACF of a "classical" continuous signal, phase manipulated according to the 0s and 1s of a M-sequence, Legendre sequence and so on.

3. Conclusion

From all above stated it can be concluded that the usage of new ultra-high frequency hardware and the quasi continuous mode of transmission simultaneously provide the following valuable features of radars for UAVs:

- large range of observation;
- high accuracy of the measurements of the coordinates and high resolution of the objects;
- diminishing of the volume and the weight of the radars.

REFERENCES:

1. T. S. Trifonov, Ts. S. Tsankov, N. R. Nikolov, and S. P. Velchev, A hardware realization of composite generator of pseudorandom sequence, using irreducible polynomials over the fields GF(2) and GF(5) and program control of the feedbacks, The 2nd international jubilee scientific conference „50 years since the flight of Yuriy Gagarin“, Shumen, 2011, ISBN 978-954-8557-11-5 (in Bulgarian).
2. N. R. Nikolov, Ts. S. Tsankov, T. S. Trifonov, and V. A. Dacheva, A summing generator with 2 bits of memory, controlled by Lorenz chaos attractor, National conference with international participation „40 years of Shumen University 1971-2011“, Shumen, 2011, ISBN 978-954-577-620-5 (in Bulgarian).
3. N. R. Nikolov, Ts. S. Tsankov, T. S. Trifonov, and V. A. Dacheva, A study of composite generator of pseudorandom sequences, using Lorenz chaos attractor, National conference with international participation „40 years of Shumen University 1971-2011“, Shumen, 2011, ISBN 978-954-577-620-5 (in Bulgarian).
4. Ts. S. Tsankov and T. S. Trifonov, An algorithm for evaluating of the linear complexity of signals, International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, Vol. 10, Liepaya, 2014, ISBN 978-9934-10-573-9 (in Russian).
5. Ts. S. Tsankov, T. S. Trifonov, and L. Staneva, A survey of phase manipulated signals with high structural complexity and small loses after processing with mismatched filters, Journal Scientific & Applied Research, Vol. 4, 2013, ISSN 1314-6289.
6. Ts. S. Tsankov, T. S. Trifonov, and L. Staneva, An algorithm for synthesis of phase manipulated signals with high structural complexity, Journal Scientific & Applied Research, Vol. 4, 2013, ISSN 1314-6289.
7. M. P. Iliev, N. R. Nikolov, Ts. S. Tsankov, Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences, Journal "Electrotechnica & Electronica", Vol. 46, 2011, ISSN 0861-4717.
8. Ts. S. Tsankov, Computer laboratory for automated synthesis of signals with high structural complexity, Scientific Conference with international participation MATTEX 2012, Shumen, 2012, ISSN 1314-3921 (in Bulgarian).

Author’s name: prof. eng. Borislav Bedzhev, PhD, DSc
Workplace: Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department „Management of security systems“
E-mail: bedzhev@abv.bg, bedzhev@shu.bg

ANNUAL

OF

KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN

FACULTY OF TECHNICAL SCIENCES

VOL. VIII E

Format 16/80/84

ISSN 1311-834X