Advances in Economics, Business and Management Research, volume 170
Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021)

Experience of Information and Analytical Activities in the Field of Border Protection of the European Union

Roman Liashuk* [0000-0003-0137-0989], Andrii Tsaruk [0000-0002-7871-0323]

National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine
**7roman@ukr.net*

ABSTRACT
This article presents the development trends in the global information environment in the near future. The concept of border security as a component of national security of Ukraine and regional border security of the European Union (hereinafter - the EU) is considered. Based on the analysis of regulatory legal acts of the European Union and Ukraine, the study of a number of scientific sources and works of leading scientists, the analysis of the best practices of the European Union was carried out and its implementation in the activities of the State Border Guard Service of Ukraine (hereinafter - SBGS) concerning the information and analytical activities (hereinafter - IAA) was suggested. The formation and development of joint protection of the EU's external borders is considered. The experience of information and analytical activities of the European Union in the protection of the EU's external borders is highlighted. Ways to improve the information and analytical activities of the State Border Guard Service of Ukraine in the context of the development of modern information technologies are proposed.

Keywords: *information and analytical activities, FRONTEX, EUROSUR, border security, European integration, State Border Guard Service of Ukraine, European Union.*

1. INTRODUCTION

Today's global information environment is extremely dynamic and diverse, and it is changing and transforming very quickly. Due to the development of information technology, it has become possible to transfer large amounts of information for short periods of time over long distances, to find almost any information, and to use it. As a result, threats and risks have appeared, as this information can be also used with the objective to organize cross-border crimes. The rapid development of technologies over the last decades, in particular information technologies, led to the fact that many information systems were created in the state authorities of Ukraine. In addition, these systems are mainly utilized to accumulate and use information in the activities of specific authorities and are not integrated into a single entity. In this regard, the exchange of information is complicated and time-consuming, which significantly affects the quality of the management process and, as a consequence, the state of border security, the national security of Ukraine and the regional security of the EU. It becomes obvious that the methods of searching, collecting, processing, storing, transferring and using information must be constantly improved, because technological progress, inventions and application of new ways for organizing cross-border crimes are forging ahead.

2. PURPOSE OF THE ARTICLE

The purpose of the article is to study the experience of information and analytical activities in the field of border protection in the European Union.

3. RESULTS OF THE RESEARCH

Border security is certainly a component of national security. The state of the EU's regional border security depends on the state of Ukraine's national security. As practice shows, these concepts are interrelated. The border security of Ukraine must be regarded both in national and regional and international scales. It is necessary to understand that the border security of Ukraine is interconnected with the trends of the regional and international security environment [1]. To ensure a high level of security in these spheres, clear and timely interaction of the subjects of integrated border management (hereinafter - IBM) at the national, regional and international levels is required. One of the main

Copyright © 2021 The Authors. Published by Atlantis Press B.V.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

conditions for productive cooperation in this direction is the quality IAA organization of IBM subjects at all levels.

The current state of border security (hereinafter - BS) of Ukraine should ensure the appropriate level of regional border security of the EU. It is logical that the states have imposed requirements for capabilities to protect the EU's external eastern border. Today, the introduction of European methods for protection of external borders is a prerequisite for full membership of Ukraine in the EU in the future. It is obvious that highquality interaction of the SBGS and other IBM subjects with European border guard agencies requires joint approaches to border protection, work with information files and development of analytical information that will be a proper basis for adequate management decisions in order to prevent cross-border crime, smuggling and human trafficking.

3.1. Formation and development of joint protection of the EU's external borders

In 2004, the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) (hereinafter referred to as the Agency or FRONTEX) [2] was established in the European Union to improve the integrated border management of the EU Member States.

In 2014, the Council of the EU adopted a Regulation [3], which regulates the protection of EU maritime borders. Scope of the Regulation is border surveillance operations carried out by Member States at their external maritime borders in the context of operational cooperation coordinated by FRONTEX.

In 2019, the provisions of the Regulation [4], which is still in force, reformed the European Border and Coast Guard Agency by providing the Agency with broader powers. A European Border and Coast Guard standing corps was established to effectively support Member States in protecting external borders [4]. Today's challenges, including such as the increase in smuggling, the increase in illegal migration and the development of cross-border crime, have necessitated to expand the powers of the Agency.

3.2. Characteristics of information and analytical activities in the field of protection of the EU's external borders

In accordance with the Regulation [2], FRONTEX developed a common integrated risk analysis model for EU Member States (CIRAM 2.0), according to which risk analysis is defined as a systematic study of threats, vulnerabilities and consequences, and the result of such analysis is documented in the form of risk assessment.

The Schengen Information System (hereinafter - SIS) was subsequently set up in accordance with the Convention [5]. In 2006, the Regulation [6] approved the second-generation SIS, which is designed to help maintain a high level of security in the area of freedom, security and justice of the European Union, to support the implementation of policies related to the movement of persons that are part of Schengen legislation. This system is designed to collect information on persons who have violated Schengen legislation in order to identify them. The system enabled to process biometric data in order to facilitate the reliable identification of persons. SIS II consists of: (a) The central system (‘Central SIS II’) composed of: - the technical support function (‘CS-SIS’) containing a database, the ‘SIS II database’; - a uniform national interface (‘NI-SIS’); (b) a national system (the ‘N.SIS II’) in each of the Member States, consisting of the national data systems which communicate with Central SIS II. The N.SIS II may contain a data file (a ‘national copy’), containing a complete or partial copy of the SIS II database; (c) a communication infrastructure between CS-SIS and NISIS (the ‘Communication Infrastructure’) that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux [6].

The Regulation further established the European Border Surveillance System (hereinafter - EUROSUR), which became a common basis for the exchange of information and cooperation between Member States and FRONTEX in order to improve their situational awareness and reaction capability at the external borders of the Member States of the Union for the purpose of detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants [7]. EUROSUR has developed in the Regulations [4]. According to Art. 19 of Regulation EUROSUR is used for border checks at authorised border crossing points and for external land, sea and air border surveillance, including the monitoring, detection, identification, tracking, prevention and interception of unauthorised border crossings for the purpose of detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants [4]. The EUROSUR system is designed to improve interaction and speed up the response to the situation between the state bodies of the EU member states on the protection of the external borders of the European Union.

EUROSUR consists of relevant components such as: national coordination centres (coordinate and exchange information between all responsible bodies at the national level and with other national coordination centres and the Agency); national situational pictures (a national coordination centre creates these pictures and maintains the relevant data to provide information to the relevant authorities); European situational picture (created by the Agency in order to provide the national coordination centres and the Commission with effective, accurate and timely information and analysis, covering the external borders, the pre-frontier area and unauthorised secondary

movements); specific situational pictures (the Agency and Member States may establish and maintain them in order to support specific operational activities at the external borders or to share information); EUROSUR fusion services (the Agency coordinates EUROSUR fusion services in order to supply the national coordination centres, the Commission and itself with information on the external borders and on the pre-frontier area); integrated planning (integrated planning process for border management and return, including operational planning, contingency planning and capability development planning processes) [4].

D. Kupriienko in his research emphasizes that the results of the regulation analysis, as well as a number of thematic reports and scientific publications indicate a crisis situation in the field of border security (hereinafter - BS) of the European Union. With this in mind, at EU level, FRONTEX set up three networks for joint risk analysis in the field of integrated border management: 1. FRONTEX Risk Analysis Network (FRAN) includes risk analysis units of border agencies of all EU member states on equal terms. 2. The Western Borders Risk Analysis Network (WB-RAN) is designed for cooperation with Western Balkan countries. 3. The Eastern Borders Risk Analysis Network (EB-RAN) is established to cooperate with the border guard services of Belarus, Ukraine, Russia and Moldova. The mechanism of information exchange and joint risk analysis was agreed at the level of the heads of the State Border Guard Service of Ukraine and the FRONTEX Agency [8]. The researcher also notes that the essence of reengineering the EU BS management system is to implement a common policy of security management at the external borders, to increase the capacity and expand the mandate of the supranational security structure - FRONTEX, to create European Border and Coast Guard Agency, and to further develop EUROSUR common information and communication platform [8].

As of today, 2 more regional risk analysis networks have been established and are operating: TurkeyFrontex Risk Analysis Network (TU-RAN) was established for cooperation with Turkey; Africa-Frontex Intelligence Community (AFIC) network was established to work with African countries. So, there are five of them. FRAN, WB-RAN, EB-RAN, TU-RAN and AFIC risk analysis networks are part of FRONTEX's strategic risk analysis.

It is clear from the above that the FRONTEX Agency pays considerable attention to IAA. IAA is one of the main and extremely important tools in the EU BS support system. Therefore, the capabilities and functionality of the EUROSUR information and communication platform and the FRAN, WB-RAN, EBRAN, TU-RAN and AFIC risk analysis networks will be further built up and developed.

In the research of D. Kupriienko, the operational procedure of the subjects of integrated border management of the EU is highlighted. In order to regularly exchange information on the situation in a near-real time mode, exchange intelligence and work closely with the subjects, the interaction of components of the EUROSUR system takes place at two levels: 1. At the national level, the authorities interact through a network of national coordination centres that monitor sectors of the national borders and exchange information 24/7. National situational pictures are formed and continuously specified. 2. At the European level, national coordination centres exchange information with each other and with the FRONTEX Agency. The European situational picture as well as the general intelligence picture in adjacent pre-frontier area are formed and continuously specified. Under these very conditions, a single mechanism of inter-institutional, national and international cooperation is formed in order to quickly and coherently respond to the situation in the border area on the basis of common standards. [9] In our opinion, such an approach is also relevant for Ukraine. The maximum result can be achieved only through coordinated work and joint approaches.

To provide strategic risk analysis products, FRONTEX collects information from a wide range of sources, including: border guard authorities of Member States and non-EU countries; EU partners (such as the European Commission, EASO, Europol, EEAS, EU SATCEN and Eurostat); international organizations (such as UNHCR, IOM, Interpol); own operational activity of Frontex; open sources, including social media. FRONTEX analyses the information gathered to establish and maintain a general situational awareness of the patterns and trends of illegal migration and crossborder criminal activities affecting the EU's external borders and so-called secondary movements within the Schengen area. Strategic risk analysis enables to make informed decisions about priorities and take appropriate measures to reduce risk. [10].

In our opinion, such approaches are also relevant for Ukraine. These technologies and methods need to be implemented today while considering Ukraine within the EU BS system as a full member of the European Union.

4. IMPLEMENTATION OF THE BEST EUROPEAN PRACTICES

At the end of the last century, Ukraine's foreign policy was aimed at European integration. The State Border Guard Service of Ukraine was one of the first to reform its activities and approaches to border protection management in order to bring them into line with EU standards. Given that Ukraine plans to become a member of the European Union in the future, the need to implement and use common approaches to border protection becomes obvious.

The norms of the European legislation are already partially implemented in the national legislation of

Ukraine and normative legal acts of the SBGS, but the Ukrainian legislation should correlate as much as possible with the European one, and these activities should be therefore continued.

Scientists O. Shynkaruk, O. Korystin, M. Lysyi, D. Kupriienko, Yu. Babii, A. Ihnatiev, O. Ananin claim that the solution to the problem of building an effective border security system, first of all, should be based on the analysis of the security environment, identifying the main trends of real and potential threats and forecasting their development. Today there is a discrepancy, on the one hand, between the need for timely detection of threats to Ukraine's border security [1] and effective response to them, and on the other hand, the presence of a significant number of diverse alternative approaches to task execution, regulatory conflicts, insufficient resources and other support etc. [11]

D. Kupriienko in his work [9] systematized the requirements for assessing the state of border security of Ukraine, and substantiated the need to develop a system for assessing the state of border security of Ukraine, which will create conditions for proper processing of information in this aspect and become part of two systems: national security of Ukraine and regional border security of the European Union. *In our opinion, it is expedient to implement this system in the activities of IBM subjects.*

It should be noted that in such a strategic planning document as the Integrated Border Management Strategy for the period up to 2025, the subjects of integrated border management are a number of state bodies of Ukraine that interact at the intra-agency, interagency, state and international levels to achieve the objectives of the state policy in the IBM sphere. The tasks of the risk analysis system are also defined, including: improving the regulatory framework and bringing risk analysis to the European model CIRAM 2.0; ensuring the capacity development for the units dealing with risk analysis and assessment, in particular the IT systems of integrated border management subjects to improve the exchange of information between them; implementing IT solutions to ensure automation of the risk analysis and profiling process. [12; 13]

The SBGS has the GART integrated information system, which is designed to ensure the exchange of information between the IBM subjects and to manage the subordinate bodies and units. But this system is outof-date and does not fully meet the requirements put forward to the European border protection.

Information and analytical activities of the SBGS and other IBM subjects require the latest methods and technologies for working with information. *We consider it appropriate to establish an integrated information system in Ukraine such as the EUROSUR European Surveillance System in order to exchange information between IBM subjects in real time. Such a system will significantly improve the level of border security and help to use available forces and facilities more rationally. It is also advisable to create a system in Ukraine similar to the Schengen Information System SIS II, which will be more functional than the existing GART integrated information system.*

Given the views of leading scholars and the fact that Ukraine in the near future should be ready to protect the external border of the European Union, there are good reasons to note the need to adopt the experience of European colleagues, accumulate, develop and implement it into the activities of the SBGS and other government agencies because of the peculiar geopolitical, economic, cultural and ethnic processes in Ukraine.

4.1. Innovative approaches to data protection in SBGS networks

Nowadays, there is an urgent need to protect data stored over networks and transferred between users. It is important that only verified users have access to the data. In order to protect data during their communication, it is necessary to use encryption algorithms [14] that ensure fast and secure data transfer. In our opinion, in order to implement data protection, it is advisable to use a hybrid scheme of secure routing and data transmission in wireless networks, proposed in [15], which combines both symmetric and asymmetric cryptographic techniques to ensure a high level of security. The system proposed by scientists will prevent unauthorized attempts to access information at two levels: encryption-decryption and hashing. In addition, this system offers improved security with less encryption-decryption time and the highest bandwidth.

As the number and variety of computer network attacks grows every year, an interesting method of detecting cyberattacks to protect computer networks is proposed in [16]. This method will increase the reliability of network protection by detecting anomalies that may indicate possible cyberattacks. Such timely information is useful for the network administrator.

In [17], it seems possible to detect an unauthorized user with the help of the proposed toolkit and confuse him by setting traps without giving him access to real network data.

The above studies present solutions for protecting computer networks from unauthorized access. *The proposed models are expedient to be used for protecting the information networks of the subjects of integrated border management, in particular, the SBGS and other public authorities to minimize unauthorized access to information resources of these authorities.*

The research [17] proposed a confidential mechanism for collecting information on the assessment of the course, which was taught to students using a vector

machine algorithm [18]. This mechanism makes it possible for management to better understand the effectiveness of teaching the material for better acquisition by students. *It seems appropriate to use this system in SBGS educational institutions to improve the educational process.* It is less expensive than its counterparts.

5. CONCLUSIONS

Under the conditions of the information society, the SBGS IAAs are a specific and necessary tool that enables managers at all levels to use analytical products to make adequate management decisions during border protection. Based on the analysis of research by national scientists and the IAAs of the EU Border Guard Agency, the implementation of the best European practices in Ukrainian legislation is proposed.

We consider it appropriate to amend the Action Plan [17] and include the following items:

to develop and implement a system for assessing the state of border security of Ukraine (the requirements for which are proposed in the research [8]);

to develop and implement systems similar to the European Border Surveillance System EUROSUR and SIS II;

to implement technological solutions proposed in the works [15, 16, 17].

In our opinion, the proposed measures will improve the functioning of the SBGS IAA and bring it closer to the requirements of EU standards. Future research in this area should be aimed at further finding ways to implement European legislation and best European experience in Ukrainian legislation.

REFERENCES

[1] Koval`chuk, T.I. Korystin, O.Ye. and Svyrydyuk, N.P. (2019), "Hybrid threats in the civil security sector in Ukraine", *Nauka i pravooxorona*, vol. 3 (45), pp. 69-79. DOI: doi.org/10.36486/np.2019308

[2] Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=OJ%3AL%3A2004%3A349%3ATOC

[3] Regulation (EU) No 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, available at: https://eur-lex.europa.eu/legalcontent/en/ALL/?uri=celex:32014R0656

[4] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1573722151667&uri=CELEX:32019R1896

[5] Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, available at: https://eur-lex.europa.eu/homepage.html

[6] 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), available at: https://eur-lex.europa.eu/legalcontent/en/ALL/?uri=celex:32014R0656

[7] Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), available at: https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2013.295.01.0011.01.ENG&toc=OJ:L:2013:295:FULL

[8] Kupriienko, D. “Analysis of current development trends of the border security management system of the European Union”, available at: http://chiz.nangu.edu.ua/article/view/138206/16676

[9] Kupriienko, D. “Definition of common requirements for assessing the state of border security of Ukraine in national and international security monitoring systems”, available at: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=sitsbo_2016_1_33

[10] FRONTEX, Strategic Analysis, available at: https://frontex.europa.eu/intelligence/strategicanalysis/

[11] Shynkaruk, O. Lysyi, M. Kupriienko, D. Babii, Yu. Ihnatiev, A. and Ananin, O. (2019), “Collection of

scientific works of Kharkiv National Air Force University", no. 3(61), pp. 135-145.

[12] On approval of the Integrated Border Management Strategy for the period up to 2025, Order of the Cabinet of Ministers Ukraine of 24.07.2019, No. 687-r, available at: https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#top

[13] Korystin, O.Ye. and Svyrydyuk, N.P. (2020), "Methodological principles of risk assessment in law enforcement activity", *Nauka i pravooxorona*, vol. 3, pp. 191-197. DOI: https: //doi.org/10.36486/np.2020.3(49).19

[14] Jamuna, S. Dinesha, P. Shashikala, Kp. and Kishore Kumar, K. (2020), "Design and Implementation of Reliable Encryption Algorithms through Soft Error Mitigation", *International Journal of Computer Network and Information Security*, Vol. 12, No. 4, pp. 41-50. DOI: 10.5815/ijcnis.2020.04.04

[15] Subedar, Z. and Araballi, A. (2020), "Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication", *I.J. Mathematical Sciences and Computing*, vol. 4, pp. 35-41.

[16] Zhengbing Hu, R. Odarchenko, S. Gnatyuk, M. Zaliskyi, A. Chaplits, S. Bondar, and V. Borovik (2020), "Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior", *I.J. Computer Network and Information Security*, vol. 6, pp. 113.

[17] Gokhale, S. Dalvi, A. and Siddavatam, I. (2020), "Industrial Control Systems Honeypot: A Formal Analysis of Conpot", *I.J. Computer Network and Information Security*, vol. 6, pp. 44-56.

[18] Mohammed Yousif, Ahmad Salim and Wisam K. Jummar (2021), "A Robotic Path Planning by Using Crow Swarm Optimization Algorithm", *International Journal of Mathematical Sciences and Computing*, Vol. 7, No. 1, pp. 20-25. DOI: 10.5815/ijmsc.2021.01.03

[19] Action plan for 2020-2022 for the implementation of the Integrated Border Management Strategy for the period up to 2025, available at: https://zakon.rada.gov.ua/laws/show/1409-2019-%D1%80#Text