Salud, Ciencia y Tecnología. 2025; 5:1793
doi: 10.56294/saludcyt20251793

ORIGINAL

Risk-based approach for protecting critical infrastructure facilities: specifics of application by law enforcement agencies

Enfoque basado en el riesgo para la protección de instalaciones de infraestructuras críticas: particularidades de su aplicación por las fuerzas del orden

Khoronovskyi Oleg[1], Drozd Oleksii[2], Shevchenko Tetiana[3], Semeniuk Oleksandr[4], Samorai Oleh[5]

[1]Candidate of Legal Sciences, Doctoral Student of the National Academy of the State Security Service of Ukraine, Kyiv, Ukraine.
[2]Doctor of Legal Sciences, Professor, Honored Worker of Science and Technology of Ukraine, Professor of the Police Law Department, National Academy of Internal Affairs, Kyiv, Ukraine.
[3]Ph.D in Law, Associate Professor, National Academy of Internal Affairs, Kyiv, Ukraine.
[4]Candidate of Legal Sciences, Associate Professor of the Department of Law of the European University, Kyiv, Ukraine.
[5]Lecturer at the Department of Cybersecurity of the European University, Kyiv, Ukraine.

Citar como: Oleg K, Oleksii D, Tetiana S, Oleksandr S, Oleh S. Risk-based approach for protecting critical infrastructure facilities: specifics of application by law enforcement agencies. Salud, Ciencia y Tecnología. 2025; 5:1793. https://doi.org/10.56294/saludcyt20251793

Enviado: 26-12-2024 **Revisado:** 10-04-2025 **Aceptado:** 11-06-2025 **Publicado:** 12-06-2025

Editor: Prof. Dr. William Castillo-González

ABSTRACT

Introduction: the purpose of this article is to examine the specifics of the use of risk-based approach by some law enforcement agencies of Ukraine, in particular, when protecting critical infrastructure, and to develop recommendations for improving this process.
Method: the following methods were used in the course of the research: method of theoretical generalization; monographic; methods of induction and deduction; methods of structural, logical and semantic analysis; system and structural; dialectical.
Results: it is proved that the risk-based approach always deals with probable categories, calculations of possible impact and works to prevent the threat from materializing, minimize its impact or minimize the consequences. The authors offer their own vision of the model for applying a risk-based approach in protecting critical infrastructure facilities, which consists of the indicated stages. In their view, the very idea, main goal, and content of RBA in ensuring CI security presuppose its application in 3 interconnected spheres (the security sphere; counterintelligence and operational-search activities; pre-trial investigation system) of law enforcement activity to form a complete system.
Conclusions: the advantages of applying RBA in fighting the threats to critical infrastructure are highlighted.

Keywords: Critical Infrastructure, Law Enforcement Agencies; Risk; Risk-Based Approach; Threat.

RESUMEN

Introducción: el objetivo de este artículo es examinar las particularidades del uso del enfoque basado en el riesgo por parte de algunos organismos encargados de hacer cumplir la ley de Ucrania, en particular, a la hora de proteger infraestructuras críticas, y elaborar recomendaciones para mejorar este proceso.
Método: en el curso de la investigación se utilizaron los siguientes métodos: método de generalización teórica; monográfico; métodos de inducción y deducción; métodos de análisis estructural, lógico y semántico; sistémico y estructural; dialéctico.
Resultados: se demuestra que el enfoque basado en el riesgo siempre se ocupa de categorías probables, cálculos del posible impacto y trabaja para evitar que la amenaza se materialice, minimizar su impacto o reducir al mínimo las consecuencias. Los autores ofrecen su propia visión del modelo de aplicación de un enfoque basado en el riesgo en la protección de instalaciones de infraestructuras críticas, que consta de las etapas indicadas. En su opinión, la idea misma, el objetivo principal y el contenido del enfoque basado en el

riesgo para garantizar la seguridad de las IC presuponen su aplicación en 3 esferas interconectadas (la esfera de la seguridad; las actividades de contrainteligencia y de búsqueda operativa; el sistema de investigación previa al juicio) de la actividad policial para formar un sistema completo.
Conclusiones: se destacan las ventajas de aplicar la RBA en la lucha contra las amenazas a las infraestructuras críticas.

Palabras clave: Infraestructuras Críticas; Fuerzas del Orden; Riesgo; Enfoque Basado en el Riesgo; Amenaza.

INTRODUCTION

In global practice, the category "RBA" (Risk-Based Approach) was first applied in the field of preventing and combating the laundering of proceeds obtained through criminal means. The Recommendations of the Financial Action Task Force on Money Laundering (FATF), which establish general conditions for the application of these measures, were already partially based on the application of RBA in their 2003 version. In 2012, after another revision of the Recommendations, the application of RBA became a necessary prerequisite for the effective implementation of the recommendations.

According to the FATF Recommendations, the application of RBA by the States (their authorized bodies, banks) involves identifying, assessing, and understanding the risks of legalization (laundering) of proceeds from crime, terrorist financing, and taking measures (including determining an authorized body or mechanism for coordinating risk assessment measures) to effectively minimize those risks. Based on such an assessment, RBA is applied so that response measures are adequate to the level of possible risk. In other words, RBA is aimed at the effective use of resources for responding to risks. If a higher risk is identified, an appropriate response must be ensured; for a lower risk level, simplified minimization measures can be applied.[1]

The risk-oriented approach in the activities of law enforcement and prosecutors is already a standard in EU countries. In Ukraine, there is also a shift from a formalistic to a risk-based approach to customer due diligence. In 2023, a new focus was placed on checking counterparties for ties to the aggressor country. The risk-based approach (RBA) is becoming a key element for the successful implementation of the international standards for combating money laundering, terrorist financing and the proliferation of weapons of mass destruction.

The purpose of this article is to examine the specifics of the use of this approach by some law enforcement agencies of Ukraine, in particular, when protecting critical infrastructure, and to develop recommendations for improving this process.

Literature review

Standardization has begun in the 1990s. Starting from this time, various organizations have been working on creating national and international standards. For example, the FERMA standard is a joint development of The Institute of Risk Management (IRM), UK, The Association of Insurance and Risk Management (AIRMIC), and The National Forum for Risk Management in the Public Sector (ALARM). The purpose of creating this standard was to maximize profitability and reduce unplanned losses. Despite the fact that it can be implemented in the risk management system of any business entity, it is largely aimed at the manufacturing sector, or the real sector of the economy.[2]

The COSO standard "Enterprise Risk Management — Integrated Framework" was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), USA. The main objectives of this document are: to determine the level of risk that corresponds to the chosen development strategy; to improve decision-making processes taking into account emerging risks; to reduce losses from economic activity; to use capital rationally. This standard is more suitable for corporations involved in stock exchange activities. Among its shortcomings, the insufficiency of methodological approaches to quantitative risk assessment methods should be highlighted.[3]

ISO 31000 is an international risk management standard developed by the International Organization for Standardization (ISO). It provides principles and guidelines for effective risk management in any organization, regardless of its size or industry. The provisions of ISO 31000 can be applied to any type of risk, regardless of its origin, that has positive or negative consequences. ISO 31000 can be used in the organization as a whole or in its individual parts and in various activities, including strategies and decisions, operations, processes, functions, projects, goods, services and assets. The scope of the standard applies to any public and commercial enterprises, associations, groups and individuals. The purpose of ISO 31000 is to harmonize risk management processes in existing and future standards, as well as to provide a unified approach to support and implement the requirements of the standards for specific risks and/or industries.[4]

However, risk management practices used until recently have become outdated for addressing modern challenges and countering threats. For this purpose, the ISO revised the ISO 31000 standard "Risk management

– Guidelines" and published a new version – ISO 31000:2018. The updated version of the well-known standard. The updated document – ISO 31000:2018 "Risk management – Principles and guidelines" – highlights risk management principles for improving planning and making effective decisions. The aim of revising the standard was to make it more accessible for understanding by all interested parties.[5]

Changes introduced in the new edition of the ISO 31000 standard include:

- Revised risk management principles, which are key success criteria in the field of risk management.
- Focus on the use of leadership qualities by top management, who must ensure the integration of risk management into all organizational activities.
- Thorough consideration of the iterative nature of risk management, taking into account new experience, knowledge, and analysis results used to revise elements of the risk management process, actions, and controls at each stage of the process.
- Streamlining of content with a greater focus on supporting an open systems model, which has regular feedback with the external environment to meet multiple needs and form correlations.

In Ukraine, Mokhor et al. made an attempt to interpret the terms and interpretations of ISO/IEC Guide 73:2009 in accordance with the traditions of the scientific and technical Ukrainian language and in accordance with the requirements of DSTU 3966-2000 "Terminology. Principles and rules for developing standards for terms and definitions of concepts". According to this guideline, risk identification is considered as a process of identifying, researching and describing (descriptive) risks. Risk identification involves identifying sources of risks, studying events, their causes and possible consequences.[6] Kulyk analyzed the terms of existing risk management standards and identified the possibility of their adaptation to the Ukrainian government's activities.[7]

Risk-based approach (RBA) in the in the activities of law enforcement agencies was examined by Vyacheslav Nekrasov and Hrigol Katamadze. The authors believe that the process of forming a modern law enforcement officer (detective, investigator, operative, analyst) requires in-depth knowledge of the methodology of risk analysis and management, the complex system "law enforcement officer – criminal phenomenon" as a modern security management tool that takes into account the impact of the human factor, system reliability, external hazards on the integral level of security. Security management is based on a systematic approach to identifying sources of danger and controlling risk factors in order to minimize human casualties, material damage, as well as financial, environmental and social losses.[8]

ISO standards have been adopted as national standards by more than 50 national standardization bodies and some UN organizations. Ukraine also joined this process starting in 2009. To date, the following standards have been implemented and are in effect in Ukraine: ISO Guide 73:2009; IEC/ISO 31010:2009; ISO 31000:2018; ISO/TR 31004:2013.

METHOD

The theoretical and methodological basis for this article is the research by Ukrainian and foreign scientists on conceptual approaches to risk management, understanding their nature and phenomenology, developing methods for analyzing and assessing risks and mechanisms for managing them. To achieve the defined goal of the article, the following general scientific methods were used to ensure the reliability of the results and conclusions obtained: the method of theoretical generalization was used to formulate the understanding of the essence of risk-based approach in protecting critical infrastructure facilities. Monographic method helped to examine the documents enshrining the concept of RBA, its principles and guidelines for effective risk management, as well as to systematize scientific approaches of domestic and foreign scientists to the theoretical aspects of this phenomenon. The methods of induction and deduction contributed to determining the directions of legal regulation of using risk-based approach by law enforcement agencies. The methods of structural, logical and semantic analysis made it possible to clarify the conceptual and categorical apparatus of the research. The method of analysis was applied for analyzing the status, dynamics and practices of using RBA by law enforcement agencies in protecting criminal infrastructure objects. System and structural method was useful in defining the stages of RBA application in counteracting risks to CI. Dialectical method helped in highlighting the advantages of applying RBA in fighting the threats to critical infrastructure.

RESULTS AND DISCUSSION

In Ukraine, the application of RBA as the main principle of financial monitoring is not a "know-how" of the new Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction".[9] Thus, according to the requirements of the previous Law of Ukraine No. 1702-VII, primary financial monitoring entities were obliged to independently assess the risk of their clients, taking into account, in particular, risk criteria defined by the Ministry of Finance, and to take precautions against clients at high risk.[10] In this case, the application of RBA

was most often carried out by banking institutions in the course of financial monitoring. In particular, according to the requirements of the Procedure for Banks to Conduct Financial Monitoring approved by the National Bank of Ukraine (NBU) Board Resolution No. 65, the bank shall apply a risk-based approach in its activities, which shall be proportionate to the nature and scale of its activities. The continuous application of a risk-based approach is essential for detecting, identifying, and assessing all current and potential ML/FT risks linked to the bank's activities (its risk profile) and customers. This approach must also ensure the prompt development of measures to effectively manage and minimize these identified ML/FT risks. The bank shall document the process of applying the risk-based approach in such a way as to be able to demonstrate its essence (in particular, the difference in approaches), the decisions made by the bank in the course of its application and the validity of such decisions.[11]

With the adoption of the Law of Ukraine "On Currency and Currency Transactions", a new system of currency supervision based on RBA was also introduced. The obligation to conduct direct currency supervision during currency operations was assigned to authorized institutions, namely: banks, non-bank financial institutions, and postal operators.[12] According to the requirements of the "Regulation on the Procedure for Authorized Institutions to Analyze and Verify Documents (Information) on Currency Operations", it is the authorized institution that is obliged to ensure a comprehensive analysis and verification of documents (information) on currency operations. Thus, authorized institutions were tasked with supervising currency operations using RBA. In case of violation of currency legislation requirements by currency supervision agents, the NBU applies enforcement measures to such agents.[13]

The new Law of Ukraine No. 361-IX enshrined the definition of RBA and expanded its scope, extending the obligation of its application to all primary financial monitoring entities (hereinafter – PFMEs). According to it, risk-oriented approach is identifying (determining), assessing (reassessing) and understanding the risks of money laundering, terrorist financing and/or financing of proliferation of weapons of mass destruction, and taking appropriate risk management measures in a manner and within the scope minimizing such risks depending on their level.[9]

PFMEs must develop internal documents on financial monitoring, taking into account the recommendations of state financial monitoring entities, defining the procedure for applying RBA. Risk criteria are determined in such documents independently, but taking into account the criteria established by the NBU (for the entities, for which state regulation in the field of financial monitoring is carried out by the NBU) or the Ministry of Finance (for other entities), as well as typological studies of the SFMS (State Financial Monitoring Service), the results of the national risk assessment, and recommendations of state financial monitoring entities.[9]

Considering the definition of the list of such criteria by the NBU and the Ministry of Finance and their establishment as a guideline for PFMEs, the latter, in their internal documents on financial monitoring, provide a similar list or supplement it with other criteria at their own discretion. Despite the fact that the application of RBA is based on the independent determination and assessment of risks by PFMEs, the Law establishes a list of cases in which the PFME is obliged to establish a high risk or an unacceptably high risk of establishing business relations or conducting a financial transaction without establishing business relations.

Assigning a high risk to a client is, in turn, grounds for enhanced due diligence measures regarding the client, and an unacceptably high risk is justification for refusing to establish (maintain) business relations and conduct a financial transaction.

Thus, high risk must be established for:

- Clients from high-risk jurisdictions: Individuals residing in or registered in states/jurisdictions non-compliant or inadequately compliant with international AML/CFT/CPF recommendations (list determined by the CMU and published by the SFMS).
- Clients linked to terrorism or sanctions: Persons listed for terrorist activities or under international sanctions, their representatives, or entities owned/beneficially owned by such listed persons (list published by the SFMS).
- Certain foreign financial institutions: Those with established correspondent relationships, excluding institutions registered in EU/FATF member states (unless they are aggressor states against Ukraine).
- Politically Exposed Persons (PEPs) and associates: Foreign public officials, their family members, close associates, and clients where such PEPs are ultimate beneficial owners.
- Sanctioned clients: Individuals or entities (or their ultimate beneficial owners) subject to special economic or other restrictive measures.
- Clients from offshore zones: Individuals residing in or registered in states classified as offshore zones by the CMU.

Unacceptably high risk must be established for clients in case of:

- impossibility to perform the duties defined by the Law or to minimize the identified risks associated with such a client or financial transaction;

- reasonable doubt that client's activity may be fictitious (based on the results of an investigation).

Accordingly, for clients whose business relations risk is low, PFMEs (Primary Financial Monitoring Entities) may apply simplified due diligence measures.[9]

Therefore, the study of operations using RBA in this area allows for the timely detection of risky operations and the termination of business relations with such a client, meaning RBA works to prevent operations with dubious purposes and, as a consequence, makes it impossible to commit illegal acts aimed at legalizing criminal proceeds.

An interesting fact is that in 2014, 2 years after the Recommendations revision, FATF stated that the introduction of RBA led to the emergence of the practice of "risk avoidance". The essence of this phenomenon is that financial institutions terminate or restrict business relations with clients to avoid risks altogether, rather than managing them using RBA. FATF noted that terminating or restricting business relations due to "risk avoidance" strategy may encourage businesses and citizens to use less transparent channels for the movement of funds. At the same time, the movement of funds through traceable and regulated channels enables to implement measures to combat the laundering of criminally obtained funds.[14]

At the same time, a better alternative to RBA in the field of combating laundering of proceeds from crime has not yet been invented, as RBA allows for effective counteraction to the legalization of illegal property while simultaneously rationally allocating the resources necessary for such counteraction.

In the context of this research, it is also worth mentioning the creation and launch of the ESBU's (Economic Security Bureau of Ukraine) operation on November 24, 2021. According to the Law of Ukraine "On the Economic Security Bureau of Ukraine" the ESBU applies RBA in its analytical activities, which is interpreted as the identification, assessment, and determination of risks of committing criminal offenses in the economic sphere, as well as taking appropriate risk management measures in a manner and to an extent ensuring the minimization of such risks depending on their level. It should be noted that the application of RBA in this case is limited to the scope of analytical activities.[15]

The application of RBA in the ESBU's practical activities occurs as follows: the institution applies RBA to identify potential risks of criminal offenses in the budgetary, tax, customs, monetary, credit, and investment spheres. This approach is used by its information and analytical units to perform tasks defined by the Law of Ukraine No. 1150-IX, RBA involves:

- detection, assessment (reassessment), and determination of risks of committing criminal offenses in the economic sphere;
- taking risk management measures;
- periodic recording of the results of RBA application;
- maintaining up-to-date information on risk assessment.[15]

The implementation of the risk-based approach involves analyzing and comparing information from ESBU databases with data obtained from automated information and reference systems, registers, and databases of state and local government authorities. Access to these latter sources is provided in accordance with the provisions of Article 7 of Law No. 1150-IX. This process also incorporates structured and unstructured data from other sources[15]

The following levels of RBA application are distinguished within the ESBU activities:

- strategic, which involves identifying risk zones, the impact of which leads to the shadowing of the economy at the national level and the weakening of the state's economic security; risk assessment, as well as determining priority areas for developing and implementing risk management measures to minimize or eliminate them;
- operational, which lies in identifying risks in a specific sector (sectors) of the economy and/or by territorial characteristics, developing and implementing measures to manage such risks to minimize or eliminate them;
- tactical – identifying risks of committing criminal offenses based on the analysis of the activities of state bodies, local self-government, business entities, or individuals, developing and implementing measures to manage such risks to minimize or eliminate them.[16]

The establishment of risks is carried out through the following sequential stages:

1) risk detection, the purpose of which is to monitor sectors of economic activity and identify potential threats that may affect the economic security of the state;

2) risk assessment: determining the level, other characteristics of the identified threat, analyzing the causes and conditions of its occurrence, possible risk forecasting (if necessary), potential or actual consequences, as well as determining possible measures to respond to this threat in order to minimize or eliminate it;

3) risk determination that includes the identification and documentation of the obtained results.[16]

Risk management measures are enacted based on the findings from risk detection, assessment, and determination. The core of these measures is a prompt response designed to reduce or remove the factors causing or potentially causing the risks, and to deal with the aftermath if such risks manifest.
The risk management process involves the following sequential stages:

- selection of response measures based on risk assessment results;
- implementation of the determined measures;
- monitoring this process;
- analyzing the effectiveness of the incorporated measures.

Response measures include:

- providing recommendations to state bodies to improve the effectiveness of their managerial decisions in regulating economic relations;
- submitting proposals for amending legal acts on the issues of eliminating the prerequisites for creating schemes of illegal activity in the economic sphere;
- providing ESBU detective units with analytical products and informational documents for making procedural decisions in the manner prescribed by criminal procedural legislation or for conducting detective activities.[16]

Consequently, ESBU contributes to protecting critical infrastructure by analyzing financial and economic activities of enterprises that are part of CI to identify risks of economic crimes. Besides, the ESBU's activities aim to prevent or minimize economic crimes that could negatively impact the functioning of CI. For example, preventing the theft of funds allocated for CI equipment ensures that this equipment is of proper quality and installed.

It is worth noting that these ESBU's performance indicators are in no way related to the results of pre-trial investigations (number of reports of suspicion; reports of indictments to court; value of seized property transferred to ARMA (Asset Recovery and Management Agency) management, etc.), which may indicate the real effectiveness of applying RBA in the ESBU law enforcement activities.

Despite the fact that the RBA principles have not yet been widely integrated into the practice of combating crime within the law enforcement system of Ukraine, they have gained recognition in developed countries in addressing social security problems. In our opinion, the widespread incorporation of this practice in the activities of all law enforcement agencies is a manifestation of the state's ability to solve problems of a systemic nature. In this case, the implementation of the preventive function in the activities of law enforcement agencies, aimed at minimizing criminal risks, becomes a completely realistic project.

At the current stage, in our view, it is important to establish a law enforcement model in the critical infrastructure (CI) protection area based on RBA, which is due to a number of factors. Firstly, risk is a foundational component of Critical Infrastructure (CI) security; consequently, risk analysis serves as a tool for studying complex social systems under conditions of uncertainty. Secondly, the components of risk include threats, defined as potential dangers with the intent and capability to harm CI facilities. Threats are characterized by their scale (impact) and the probability of their occurrence. This implies that the mere presence of certain forces, phenomena, or factors necessitates action by authorized entities, even during the formation of intent and capabilities. Concurrently, identifying system vulnerabilities (such as problems, flaws, or shortcomings) in CI security—which create or increase susceptibility to the negative impacts of threats—provides an opportunity to determine ways to enhance the system's overall capacity. Thirdly, when applying a Risk-Based Approach (RBA), we consistently deal with probabilistic categories, calculations of potential impact, and efforts to prevent a threat's realization or minimize its impact and consequences. Fourthly, based on the principles of complex systems like CI security, it is practically impossible to make a satisfactory forecast of a complex system's behavior over a sufficiently long period relying solely on personal experience and intuition.

Therefore, the risk analysis toolkit that law enforcement officers should apply is based on processing large amount of information precisely by artificial intelligence (software that allows for the automatic analysis of large volumes of data according to specified parameters).

In our view, the very idea, main goal, and content of RBA in ensuring CI security presuppose its application in 3 interconnected spheres of law enforcement activity to form a complete system. The first one is the security sphere, which aims to use tools of preventive intervention in the processes influencing the formation of risks to CI security. Any legislative acts, in particular, the future Law of Ukraine "On the Security Service of Ukraine" (currently draft law No. 3196-d, hereinafter – the Draft Law), except for the Criminal Procedure Code of Ukraine, can serve as the legal basis for its application. The use of criminal procedure takes place only when all possible preventive measures have been exhausted.

The Draft Law defines the concept of "state security risk" as a quantitative and/or qualitative measure of danger caused by a threat to the state security, and "state security risk management" as the process of making and ensuring the implementation of managerial decisions on the identification, assessment, monitoring, and controlling state security risks, aimed at their neutralization or minimization. In addition, the Draft Law identifies such tools of preventive impact on state security risks as a recommendation and reservations from the Security Service of Ukraine.[17]

The second one is a paradigm shift in counterintelligence and operational-search activities, in which case they are used not only as an appendage to pre-trial investigation but also as a tool of preventive influence to neutralize the threats to CI functioning and ensure the mechanisms of operational control over them, etc.

The third one is the pre-trial investigation system. It covers issues regarding the introduction of a risk assessment procedure for initiating or terminating criminal proceedings (conducting investigative search actions; introducing a system for prioritizing the investigation of criminal proceedings, etc.). In this context, it is appropriate to cite the example of the federal laws package called RICO ("Racketeer Influenced and Corrupt Organizations Act"), approved back in 1970 in the USA, which allows for avoiding opening of proceedings in each individual case.[18] Therefore, investigation of criminal proceedings should be a last resort when all possible preventive tools have been exhausted, and compensation for the damage caused is impossible without criminal coercion.

In general, the correct implementation of RBA in the operational and service activities of the SSU in the field of CI protection will contribute to solving systemic problems, is able to keep the level of competence up-to-date at all times, as well as prevent any harm to the state.

Considering the foregoing, we offer our own vision regarding the model of the SSU's application of RBA in counteracting the risks to critical infrastructure. The purpose of applying RBA in this area is identifying such threats, as well as developing and implementing measures to minimize and eliminate such them based on their assessment.

The application of RBA will be carried out by analyzing and comparing data on the threats to critical infrastructure facilities, contained in the SSU unified information system, and data obtained from automated information and reference systems, registers, banks (databases) of state authorities, local self-government bodies, as well as from other sources, in particular:

- materials of the SSU obtained during counterintelligence, operational-search, and information-analytical activities, pre-trial investigation, as well as the performance of other tasks stipulated by current legislation;
- materials received from state bodies, local self-government, non-governmental organizations, competent authorities of other states, international, intergovernmental organizations within international cooperation in accordance with the legislation and international treaties of Ukraine;
- mass media and other open sources.

To ensure the application of RBA (conducting automated analysis of large amount of information), a specialized software product (information and analytical system) may also be created, which, if necessary, can be integrated into the SSU unified information system, as well as information (reference) systems, registers, banks (databases) of other state authorities and/or local self-government.

The application of RBA in counteracting risks to critical infrastructure can be conditionally divided into several stages:

1) detection of the named threats, which lies in monitoring critical infrastructure sectors and searching for threats affecting their security, and is carried out by studying information sources, analyzing them, and comparing them with risk criteria for committing offenses to the detriment of CI (a risk criterion is a sign, characteristic, parameters, or their combination allowing for the detection of the transnational organized criminal groups activities). Such criteria may be specific individuals and/or legal entities that are participants in criminal activity, countries (jurisdictions), their individual territories where such activity is performed, a certain type of goods, works, services that are illegally moved across the state border, relevant typologies of criminal schemes, etc.

OSINT (Open-Source Intelligence) technologies and specialized software products (information and analytical systems) allowing for the analysis of large amount of information according to the established criteria for its search and selection can also be used to ensure risk detection. OSINT technologies are categorized according to the following principle: OSINT (Open-Source Intelligence), HUMINT (Human Intelligence, also known as "agent intelligence"), and TECHINT (technologies and information resources used to gather intelligence on an adversary, which includes IMINT, SIGINT, MASINT).[19] Simultaneously, new directions in the development of OSINT technologies are also distinguished, such as CYBERINT (Cyber Intelligence) and SOCMINT (Social Media Intelligence).[20]

2) Risk assessment (re-assessment). This stage establishes the level, other characteristics of the

identified threat, the causes and conditions of its occurrence, risk forecasting (if necessary), potential or existing consequences, as well as determining possible ways to respond to such a risk in order to minimize or eliminate it. The risk level is determined based on qualitative and quantitative assessments of possible negative consequences that may be caused by the absence of a response or untimely response to an identified threat. To verify the presence or absence of previously identified risks, a risk reassessment may be conducted.

3) Risk determination. At this stage, risks are identified in a specific area of legal relations, and the obtained results are properly recorded.

4) Risk management. At this phase, the measures, which lie in timely response to risks by minimizing or eliminating factors that have led or may lead to their occurrence, as well as the consequences of the manifestation of such risks, are taken.

These measures include:

- submitting recommendations (mandatory for consideration) to state bodies, local self-government, military formations, enterprises, institutions, organizations regardless of ownership, and officials (employees) concerning CI security issues, elimination of causes and conditions that may contribute to the realization of threats to CI or increase them, ways to minimize and/or neutralize the negative consequences of such risks;
- sending an official warning (an explanation) to an individual or legal entity, informing that their actions (acts or omission) create conditions for the emergence or realization of threats to CI security or increase such risks, and are therefore unacceptable;
- initiating a counterintelligence and/or operational-search activities if it is necessary to use special forces and means to obtain additional data on identified risks and take measures to minimize or eliminate them;
- directing relevant materials to pre-trial investigation bodies for initiating a pre-trial investigation if it is impossible to prevent the occurrence of negative consequences;
- monitoring the implementation of risk management measures.

Control over the incorporation of such measures and analysis of their effectiveness is carried out through exchange of information (orally or in writing) with the implementers of recommendations and official warnings, as well as investigators (detectives, prosecutors) who are investigating criminal proceedings based on relevant materials.

The data obtained through the application of risk-based approach by the Security Service of Ukraine in counteracting the risks to critical infrastructure facilities can be used for: 1) keeping information on risk assessment and methods of their identification up-to-date; 2) filling of a single information system of the Security Service of Ukraine with a view to further use of this information in operational and service activities of other state security bodies.

CONCLUSION

The implementation of the risk-based approach in crime prevention in Ukraine was largely driven by the adoption of the Law of Ukraine “On Prevention and Counteraction to Legalization (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction”. The further entrenchment of these principles in the Law of Ukraine “On the Economic Security Bureau of Ukraine” and the Decree of the President of Ukraine “On the Introduction of the National Resilience System” further underscored the urgency of applying the RBA in the activities of law enforcement agencies.

The risk-based approach (RBA) serves as one of the most important instruments for establishing effective programs to counter criminal offenses. A comprehension of these risks and their associated factors facilitates the implementation of more effective and efficient measures to prevent criminalization. Due to the dynamic nature of threats, the risk management process necessitates continuous execution. It is imperative that the assigned risk levels align with the actual risks, reflect the true state of affairs, and represent a valid method of assessment.

The application of RBA in fighting the threats to critical infrastructure, in our conviction, will significantly contribute to: 1) ordering large arrays of operational information regarding such risks; 2) a clear understanding of the essence of the identified threats, the methods of their minimization and neutralization; 3) optimization of operational and service activities through the economy and rational allocation of forces and means; 4) identifying gaps and conflicts in legislation, as well as the causes and conditions that contribute to illegal activities; 5) rapid and adequate response to any criminal manifestations to prevent material damage and eliminate the very causes and conditions contributing to them; 6) the fastest possible mastery of techniques and methods for counteracting the named risks.

https://doi.org/10.56294/saludcyt20251793

REFERENCES

1. FATF. FATF Recommendations; 2025. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

2. Federation of European Risk Management Associations. About us; 2025. https://ferma.eu/about-ferma/

3. Committee of Sponsing of the Treadway Commission. About us; 2025. https://www.coso.org/about-us

4. LLC "INTERSERT-UKRAINE". ISO 31000 series of standards. Risk management; 2025. https://intercert.com.ua/articles/regulatory-documents/311-iso-31000-risk-management

5. ISO. ISO 31000:2018 Risk management — Guidelines; 2018. https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf

6. Mokhor V, Bogdanov O, Kruck O, Tsurkan V. An attempt to localize ISO Guide 73:2009 "Risk Management-Vocabulary". Ukrainian Scientific Journal of Information Security. 2012; 2 (18): 12-22. https://doi.org/10.18372/2225-5036.18.3421

7. Kulyk H. Standardization of risk management: public administration aspect. Theory and practice of public administration. 2012; 2 (37): 103 – 111.

8. Nekrasov V, Katamadze H. Risk-based approach (RBA) in the activities of law enforcement agencies. In: Realization of the philosophy of "intelligence-led policing" in the criminal analysis system of the National Police of Ukraine. Kyiv: "Vait"; 2024: 311 – 341. 10.36486/978-966-2310-66-5-25

9. Law of Ukraine of December 06, 2019 No. 361-IX "On Prevention and Counteraction to Legalization (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". https://zakon.rada.gov.ua/laws/show/361-20#Text

10. Law of Ukraine of October 14, 2014 No. 1702-VII "On Prevention and Counteraction to Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction" (expired). https://zakon.rada.gov.ua/laws/show/1702-18#Text

11. Resolution of the Board of the National Bank of Ukraine of May 19, 2020 No. 65 "Procedure for Banks to Conduct Financial Monitoring". https://zakon.rada.gov.ua/laws/show/v0065500-20#Text

12. Law of Ukraine of June 21, 2018 No. 2473-VIII "On Currency and Currency Transactions". https://zakon.rada.gov.ua/laws/show/2473-19#Text

13. Resolution of the Board of the National Bank of Ukraine of January 2, 2019 No. 8 "Regulation on the Procedure for Authorized Institutions to Analyze and Verify Documents (Information) on Currency Operations". https://bank.gov.ua/ua/legislation/Resolution_02012019_8

14. FATF clarifies risk-based approach: case-by-case, not wholesale de-risking. FATF; 2024. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Rba-and-de-risking.html

15. Law of Ukraine of January 28, 2021 No. 1150-IX "On the Economic Security Bureau of Ukraine". https://zakon.rada.gov.ua/laws/show/1150-20#Text

16. Order of the Economic Security Bureau of Ukraine of January 02, 2023 No. 36 "On the approval of the Procedure for the application of a risk-oriented approach in the Bureau of Economic Security of Ukraine". https://zakon.rada.gov.ua/laws/show/z0350-23#Text

17. Draft Law of Ukraine of October 26, 2020 No. 3196-d "On Amendments to the Law of Ukraine "On the Security Service of Ukraine" to Improve the Organizational and Legal Framework of the Security Service of Ukraine". http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243

18. Racketeer Influenced and Corrupt Organizations Act (RICO). Wex Definitions Team; 2023. https://www.law.cornell.edu/wex/racketeer_influenced_and_corrupt_organizations_act_(rico)

19. Hwang Y-W, Lee I-Y, Kim H, Lee H, Kim D. Current Status and Security Trend of OSINT. Wireless Communications and Mobile Computing. 2022; 2022: 1–14. https://doi.org/10.1155/2022/1290129

20. Șandor A. An Intelligence Perspective on Privacy and Data Protection Risks in social media. International conference KNOWLEDGE-BASED ORGANIZATION. 2020; 26(1): 151–156. https://doi.org/10.2478/kbo-2020-0023

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Khoronovskyi Oleg, Drozd Oleksii.
Data curation: Orlean Andriy.
Formal analysis: Semeniuk Oleksandr, Samorai Oleh.
Research: Khoronovskyi Oleg, Drozd Oleksii, Orlean Andriy.
Methodology: Semeniuk Oleksandr, Samorai Oleh.
Project management: Orlean Andriy.
Resources: Orlean Andriy, Semeniuk Oleksandr, Samorai Oleh.
Supervision: Khoronovskyi Oleg, Drozd Oleksii.
Display: Semeniuk Oleksandr, Samorai Oleh.
Writing – original draft: Khoronovskyi Oleg, Drozd Oleksii, Shevchenko Tetiana, Semeniuk Oleksandr, Samorai Oleh.
Writing – review and editing: Khoronovskyi Oleg, Drozd Oleksii, Shevchenko Tetiana, Semeniuk Oleksandr, Samorai Oleh.