e-ISSN 3083-6018

SOCIAL DEVELOPMENT: Economic and Legal Issues

https://www.eu-scientists.com/index.php/sdel

The Direction of the Activities of the Special Services of the Russian Federation as an Instrument of the State Policy of Aggression

Yurii Kanavets [1] *

[1] *National Academy of the Security Service of Ukraine (Ukraine). Senior Lecturer at the Department 4.*

* ***Corresponding Author,*** e-mail: samsung1503mk@gmail.com

ARTICLE INFO

Research Article

DOI: 10.70651/3083-6018/2025.10.06

ABSTRACT

The article is devoted to the analysis of the activities of the special services of the Russian Federation as a key tool for implementing the state policy of aggression, identifying their main directions and methods of influence, and assessing the consequences for national and international security. Special attention is paid to the development of recommendations for countering this activity. The purpose of the study is to analyze the strategies, methods, and instruments of the activities of the special services of the Russian Federation in the context of aggressive foreign policy and to develop recommendations for countering their actions. In the course of the scientific research, general scientific methods were used, in particular: analysis and synthesis to identify the essence and structure of the activities of the special services; comparative analysis to compare the methods of their influence at different stages of aggression; a systematic approach for a comprehensive consideration of the interaction of the special services with state and military structures; as well as the method of logical generalization for formulating conclusions and recommendations, generalization, and a systematic approach. The features of hybrid war and special services as an instrument of the policy of aggression are indicated. International legal norms on the prohibition of aggression and the responsibility of states are systematized. The ideological basis of the activities of special services in the context of the policy of the "Russian world" is considered. The main areas of activity of the Russian special services used in the implementation of the policy of aggression are identified: information and psychological operations, cyberattacks, sabotage, support for terrorist groups and proxy structures. Specific examples (cases) of the use of Russian special services in foreign policy operations are analyzed – in particular in the context of armed aggression against Ukraine, the annexation of Crimea, the war in Donbas and the full-scale invasion of 2022. The focus is on the consequences of the activities of the Russian special services for international and regional security, as well as for the sovereignty of Ukraine. Mechanisms for countering the activities of the Russian special services and ways to strengthen national security are identified. In particular, the international reaction and legal mechanisms of the Russian Federation's responsibility for aggression and the actions of its special services are analyzed. The system of counterintelligence and cyber-defense measures of Ukraine is presented. The role of international partnerships in countering hybrid threats is characterized. Proposals are made to improve the state security policy of Ukraine.

KEYWORDS

special services, armed aggression, hybrid threats, international organizations, cyberattack, sabotage, counterintelligence, protection.

e-ISSN 3083-6018

СОЦІАЛЬНИЙ РОЗВИТОК: економіко-правові проблеми

https://www.eu-scientists.com/index.php/sdel

Спрямування діяльності спецслужб Російської Федерації як інструменту державної політики агресії

Юрій П. Канавець [1]*

[1] *Національна академія Служби безпеки України (Україна). Старший викладач кафедри 4.*

* ***Автор-кореспондент,*** e-mail: samsung1503mk@gmail.com

СТАТТЯ

Дослідницька

DOI: 10.70651/3083-6018/2025.10.06

АНОТАЦІЯ

Стаття присвячена аналізу діяльності спецслужб Російської Федерації як ключового інструменту реалізації державної політики агресії, виявленню їхніх основних напрямів та методів впливу, оцінці наслідків для національної та міжнародної безпеки. Особлива увага приділяється розробці рекомендацій щодо протидії цій діяльності. Метою дослідження є аналіз стратегій, методів та інструментів діяльності спецслужб РФ у контексті агресивної зовнішньої політики та розробка рекомендацій щодо протидії їхнім діям. У ході наукового дослідження використовувалися загальнонаукові методи, зокрема: аналіз та синтез для виявлення сутності і структури діяльності спецслужб; порівняльний аналіз для зіставлення методів їхнього впливу на різних етапах агресії; системний підхід для комплексного розгляду взаємодії спецслужб із державними і військовими структурами; а також метод логічного узагальнення для формулювання висновків та рекомендацій, узагальнення та системний підхід. Зазначено особливості гібридної війни та спецслужб як інструменту політики агресії. Систематизовано міжнародно-правові норми щодо заборони агресії та відповідальності держав. Розглянуто ідеологічне підґрунтя діяльності спецслужб у контексті політики «русского мира». Визначено основні напрями діяльності спецслужб РФ, які використовуються у реалізації політики агресії – інформаційно-психологічні операції, кібератаки, диверсії, підтримка терористичних угруповань і проксі-структур. Проаналізовано конкретні приклади (кейси) застосування російських спецслужб у зовнішньополітичних операціях – зокрема в контексті збройної агресії проти України, анексії Криму, війни на Донбасі та повномасштабного вторгнення 2022 року. Зосереджено увагу на наслідках діяльності спецслужб РФ для міжнародної та регіональної безпеки, а також для суверенітету України. Визначено механізми протидії діяльності спецслужб рф та шляхи посилення національної безпеки. Зокрема, проаналізовано міжнародну реакцію та правові механізми відповідальності Російської Федерації за агресію та дії її спецслужб. Представлено систему контррозвідувальних і кіберзахисних заходів України. Охарактеризовано роль міжнародного партнерства у протидії гібридним загрозам. Надано пропозиції щодо удосконалення державної політики безпеки України.

КЛЮЧОВІ СЛОВА

спецслужба, збройна агресія, гібридні загрози, міжнародні організації, кібератака, диверсії, контррозвідка, захист.

1. Introduction

Since 2014, when Russia annexed Crimea and then unleashed a full-scale war against Ukraine in 2022, its actions have become an obvious example of armed aggression and a gross violation of the fundamental principles of international law. It is not only about the seizure of territory, but about a systematic attack on the political independence and integrity of the Ukrainian state. This position was confirmed by more than 70 resolutions and resolutions of international organizations, including key ones – the decisions of the UN General Assembly, which unequivocally qualify Russia's actions as an act of aggression. Russia's policy towards Ukraine has a clearly imperial character and is based on the concept of a "zone of influence", which has been outdated since the Cold War.

This is manifested in the use of a whole range of special tools – from open combat operations to discreet, but no less dangerous, hybrid actions. A special role in this system is played by the so-called special forces of the Russian Federation. Their activities go far beyond the usual military operations: they create an information environment, influence public sentiment, carry out targeted cyberattacks and psychological campaigns.

An equally significant component of the Russian strategy is the support of quasi-state formations and controlled groups created by it, which act as "local partners". Through them, Moscow embodies the tactics of controlled chaos – fueling instability, manipulating information flows, and legitimizing its own presence. This type of influence is an inherent feature of the modern form of neocolonial policy, when, instead of direct control, a network of subordinate structures is used.

The special services of the Russian Federation have become one of the leading links in the implementation of state policy. Their subordination to the highest political leadership guarantees complete coordination of steps with the Kremlin's strategic plans. It is thanks to this vertical supervision that intelligence organizations have become an effective instrument of state whim. Russian special services function not so much as a protective wall as an offensive platform, where military, diplomatic and media means are brought together into a single hybrid structure.

Their activities are characterized by secrecy and agility, which is confusing for the detect of measures and global legal analysis. Fourthly, thanks to the media and disinformation campaigns, intelligence agencies influence public opinion and political alignments in other countries, creating favorable circumstances for achieving Russia's strategic plans. Finally, the experience of conducting "active operations" in Soviet times allows the current intelligence services to skillfully combine the usual methods with the latest means of influence.

Thus, the work of the intelligence agencies of the Russian Federation is a consistent and coordinated lever that guarantees the implementation of the hostile policy of the state both openly and covertly, combining political, informational, cybernetic and military means.

2. Literature Review

The issue of directing the activities of the special services of the Russian Federation as an instrument of the state policy of aggression is not sufficiently studied in the domestic literature. An important contribution to the study of this issue was made by such scholars as V. Palyvoda [1], who analyzed the use by the Russian authorities of pseudo-public organizations formed to influence their own society, to convey to the world community narratives favorable to the Kremlin. such organizations. S. O. Sidchenko et al. [2, p. 106], focused on the fact that actions in the information space were accompanied by provocations and demonstration actions of armed formations and special services of the PMR and the Russian Federation. According to G. Wilde [3], the FSB/GRU/SVR coordinate external sabotage and information campaigns, collect intelligence, recruit agents, and use from state to semi-state and private actors (for example, PMCs) for operations outside the official front. V. Ilnytskyi et al. [4, p. 45] covered propaganda activities by the special services of the Russian Federation, which became an indicator of the preparation of the armed aggression of the Russian Federation against Ukraine. O. A. Melnichenko [5, p. 31] noted that to equip and implement destructive information and psychological operations against Ukraine in the information space, Russian special services are increasingly using the capabilities of IT giants (services and platforms of Google, LLC), thanks to the

technical resources of which disinformation is spread in order to exert a manipulative influence on Internet users.

I. H. Verkhovtseva [6, p. 213] emphasized the methods of information aggression and information pressure. She analyzed the key narratives of the Russian information war against Ukraine and the latest trends in public diplomacy in the context of the digitalization of the global information space. The work [7, p. 88] states that while continuing their destructive activities, special services recruit for secret cooperation those who, under the influence of anti-Ukrainian propaganda, have developed a hostile attitude towards the Ukrainian authorities, considering them criminal (illegally elected), and their work is useful for residents of Luhansk and Donetsk regions. In preparation for the unleashing of armed aggression against Ukraine, the special services of the aggressor country can carry out large-scale subversive activities aimed at persuading part of the population of a certain territory or district to collaborate, support their armed formations, or reconnaissance and sabotage groups.

H. I. Samarets [8, p. 12] considered the use of the special services of the Russian Federation to resume the armed phase of the confrontation in 1992, which led to the suspension of the four-party process of conflict settlement with the participation of the Republic of Moldova, Transnistria, Ukraine, Romania, and the removal of the latter from it. In a professional report [9, p. 45], according to the verdicts of cybersecurity experts, since 2014, Ukraine has served as a testing ground for Russian intelligence and groups of attackers controlled by them to test the latest methods of cyberattacks. Several types of attacks aimed at information and psychological pressure on citizens, illegal collection of information, immobilization of the work of central authorities, as well as causing financial damage to the country and people due to the shutdown of information and telecommunication networks at vital infrastructure facilities, were recorded.

K. Kononenko [10, p, 4] notes that the Russian Federation has significantly intensified its efforts to destabilize European countries, which it has declared “hostile”. The arsenal of Russian means aimed at achieving these goals includes attempts to influence political processes in European countries, the use of economic (including energy) pressure and the instrument of trade wars, threats to use military force, in particular nuclear weapons, the strengthening of the activities of Russian special services and the associated increase in cases of espionage, cyberattacks, the number of sabotages against the military and critical infrastructure of European countries, etc. In recent years, Russian special services have been actively recruiting citizens of European countries from among ethnic Russians and Russian-speakers for espionage, acts of sabotage and other subversive activities against their countries of residence [10, p. 8]. In its interference in the affairs of European countries, Moscow widely involves special services acting according to a clearly distributed list of tasks. The Foreign Intelligence Service of the Russian Federation performs traditional intelligence functions – obtaining information important for the Russian Federation on political and economic issues and other sensitive information. The Federal Security Service of the Russian Federation protects diplomatic missions and operational activities of Russian networks. In particular, Russian special services recruit the perpetrators of such crimes, “one-time” agents, through specialized groups on Telegram, without direct personal contacts (which further complicates their identification). Their target audience is people who are ready to cooperate for ideological or financial reasons, mainly migrants or low-income people who are used to casual “gray” earnings with low pay, Ukrainian refugees, and minors, who, in most cases, do not even realize that they work for Russian intelligence.

Modern research indicates: Russian aggression is a multi-layered war, where special services are the main catalyst for both “subversive” and covert military-political operations; counteraction requires comprehensive, interdisciplinary approaches and greater attention to the effectiveness measurements of non-quantitative operations.

3. Problem Statement

The purpose of the study is to thoroughly consider the functioning of the special services of the Russian Federation as a tool for implementing the militant policy of the state, outlining the main ways and methods of their pressure, assessing the consequences for state and world security, as well as forming proposals for effective resistance to their steps.

4. Methods and Materials

The study is based on a multifaceted approach to reviewing the activities of the special services of the Russian Federation as a means of the state policy of aggression. The methodological basis is a systemic concept that allows us to see the special services of the Russian Federation as a cohesive component of the political and military plan of the state and take into account the interaction of political, media, cyber and military levers of influence.

The study uses general scientific methods, in particular, analysis and synthesis to identify the essence, functions and ways of activity of special services, comparative analysis to compare methods and consequences of their influence at different stages of aggression, logical generalization to form conclusions and practical recommendations, as well as a systematic approach to in-depth consideration of the interaction of special services with state and military structures.

Methods that combine analytical depth with a proven empirical base are also used. One of the main tools is content analysis of open data – reports of international organizations, materials of leading think tanks, journalistic investigations and thematic publications. This approach makes it possible not only to organize disparate information but also to find patterns in the strategies and steps of the Russian special services.

The combination of quantitative indicators with deep qualitative analysis forms a reliable basis for reliable conclusions. This approach allows us to see not only the statistics of the activities of the Russian special services, but also the internal logic of their steps – motives, structure of influence, and coordination mechanisms. It is the symbiosis of empirical data and analytical interpretation that provides a true understanding of complex political processes, especially in situations of hybrid threats.

As a result, each method complements the other. This allows not only to assess the scale and nature of the actions of Russian intelligence agencies, but also to outline effective ways of protection – from strengthening cybersecurity to strengthening international mechanisms to deter the aggressor.

5. Results and Discussion

The modern Russian model of foreign policy influence is based primarily on the work of its special services – structures. They combine the functions of the army, diplomacy and propaganda. Their task is to create a controlled chaos in which you can promote your own interests while maintaining the appearance of "non-interference". In practice, this is manifested in the financing of pro-Russian parties, the launch of disinformation campaigns in the media space, pressure through energy resources, and even in the support of criminal networks that act as intermediaries. Such a multi-level system allows Moscow to act with high adaptability: "special services become not just executors, but architects of the political space of influence."

From 2014 to 2024, their activity went far beyond the usual espionage activities – it became the core of a hybrid war, where intelligence, financial transactions, cyberattacks, and propaganda work as a single mechanism. Thanks to this, the Russian security apparatus has turned into an autonomous force capable of implementing political decisions faster than official diplomatic channels. It can be seen that in the modern geopolitical reality, it is the special services of the Russian Federation that form the "strategic front" of the state – without public statements, without the march of tanks, but with tangible consequences for world security [1].

In the XXI century, the Russian Federation has made hybrid warfare its main weapon of influence on the world order. Its essence is in blurring the boundaries between peace and open conflict, when instead of fronts and armies, there are information campaigns, cyberattacks, economic blackmail and political destabilization. This format allows the state to achieve strategic goals without crossing the line of a formal declaration of war, which gives it room for maneuver and denial of its own involvement. Hybrid warfare has become a "new generation tool" that combines the logic of military strategy with methods of mind manipulation.

The basis of this system is the coordinated activities of special services. They act not just as executors of individual tasks, but as the think tank of a hybrid model that combines political, economic, cyber-technological and psychological operations. It is through intelligence that the Kremlin manages the hidden phases of the conflict – from spreading disinformation in the media to organizing sabotage groups on the territory of other states.

This creates the effect of constant uncertainty, when aggression looks like a set of local incidents, and not a purposeful strategy. This is the main strength of hybrid warfare – it deprives the enemy of the possibility of a quick response. Russia's special services, based on the experience of past decades, have learned to use information as a weapon no less effective than missiles or tanks. And it is this symbiosis of hidden methods and political pressure that makes hybrid aggression the most dangerous form of modern conflict [5, p. 31].

The special services of the Russian Federation, primarily the FSB, the GRU and the Foreign Intelligence Service, appear to be a key link in the implementation of operations aimed at destabilizing internal political processes in target countries, undermining the national security system and creating conditions for the implementation of the Kremlin's political interests. Their work includes cyberattacks, information and psychological operations, support for pro-Russian political and public structures, and organization of sabotage and intelligence operations. It is thanks to the capabilities of the special services that Russia carries out aggression against Ukraine not only on the battlefield, but also in the field of information, cultural and economic space.

Hybrid warfare involves minimizing the direct participation of regular troops and, at the same time, maximizing the use of non-linear means of influence. In this process, the security services act as an organizational and coordination cell, ensuring the coordination of actions between various components of the system of state aggression – military, diplomatic, informational and financial structures. This model allows Russia to maintain formal visibility at the wrong time, while using a wide range of hidden methods to achieve political goals.

The activities of special services within the framework of the hybrid war against Ukraine are systemic: from destructive influence on the information space to direct participation in military operations. They coordinate networks of agents, conduct cyber warfare, organize propaganda campaigns, and manipulate public opinion both inside Ukraine and internationally. All this indicates that it is the special services that are the core of the hybrid strategy of the Russian Federation – a tool that combines and embodies the political, military, and informational components of aggression.

In the current conditions, hybrid warfare is not only a form of confrontation, but also a strategy where special services act as decisive agents of influence. Their work allows the Russian Federation to pursue an aggressive policy against Ukraine and other states, while maintaining the appearance of the legitimacy of its own steps and avoiding direct responsibility for violations of international law.

After the beginning of the armed aggression of the Russian Federation against Ukraine, international organizations, including the UN, the International Criminal Court, the OSCE, and the Council of Europe, have been actively using legal mechanisms to condemn aggression, document crimes and determine the responsibility of the aggressor. The result was several resolutions of the UN General Assembly (2014-2025), which consistently record the position of the international community on the illegality of the actions of the Russian Federation, the demands for the cessation of aggression and the restoration of the territorial integrity of Ukraine.

A summary of these documents is given in Table 1, which systematizes the main international legal norms, their content and specific application to the case of Russian aggression against Ukraine.

The analysis of international legal acts shows that the aggression of the Russian Federation against Ukraine has all the signs of a gross violation of the UN Charter and the principles of international law. A set of norms – from the UN Charter and Resolution No. 3314 to the latest documents of 2024-2025 – forms a holistic system that not only condemns aggression, but also imposes legal, political, material and criminal responsibility on the aggressor state.

The decisions of the UN General Assembly in recent years confirm the steadfastness of the world's position: no state has the right to change its borders by force or occupy the territories of another country. Thus, the legal basis of the modern system of international security unconditionally defines the measures of the Russian Federation as an armed attack, and Ukraine as a victim of this act. This forms the legal basis for a future international court regarding the crime of aggression and compensation for damages.

The policy of the so-called "Russian world" has become the ideological framework of modern Russian statehood and a key tool for justifying external aggression, including the activities of the Russian special services. This concept, which arose at the intersection of political, cultural and religious narratives, is presented as "Russia's mission" to protect "compatriots" and "Orthodox civilization"

beyond its borders. In fact, it serves as a legitimation of expansionist policy, interference in the internal affairs of other states and undermining their sovereignty [6, p. 213].

Table 1. International legal norms on the prohibition of aggression and state responsibility

International legal act/document	Key provisions	The content of the norm (briefly)	Application to the Russian Federation
Charter of the United Nations (1945), Article 2(4)	Prohibition of the use of force or threat of force against the territorial integrity or political independence of any state	All states are obliged to settle disputes peacefully and not to use force to achieve political goals	The actions of the Russian Federation against Ukraine are a direct violation of Article 2(4), since the sovereignty and territorial integrity of Ukraine have been violated
UN General Assembly Resolution No. 3314 "Definition of Aggression" (1974)	Defines the concept of aggression and its forms	Aggression is the use of armed force, occupation, annexation, support for armed groups, blockade, etc.	The annexation of Crimea, the occupation of Donbas, the attack of 2022 – all these actions fall under the definition of aggression
Helsinki Final Act (1975)	Principles of inviolability of borders and non-interference in the internal affairs of states	Prohibits any actions aimed at changing borders by force	The principle of inviolability of borders and territorial integrity of Ukraine has been violated
Rome Statute of the ICC (1998), art. 8 bis (Kampala Amendments, 2010)	Defines the crime of aggression as an international crime	Heads of state bear individual criminal responsibility for planning, preparing or carrying out an act of aggression	The leadership of the Russian Federation may be prosecuted for the crime of aggression against Ukraine
Draft Articles on Responsibility of States for Internationally Wrongful Acts (UN International Law Commission, 2001)	Establishes the principles of international responsibility of states	The state is obliged to stop violations, compensate for damages and bear responsibility for aggression	The Russian Federation bears international responsibility for the occupation of Ukrainian territories and the damage caused
UNGA Resolution No. 68/262 (27 March 2014)	"Territorial integrity of Ukraine"	Condemns the annexation of Crimea and reaffirms the recognition of Ukraine's international borders	The world community does not recognize the annexation of Crimea, and calls on the Russian Federation to end the occupation
UN General Assembly Resolution ES-11/1 (2 March 2022)	"Aggression against Ukraine"	Recognizes the actions of the Russian Federation as armed aggression, demands an immediate cessation of hostilities	The first official international definition of Russia's war against Ukraine as an act of aggression
UNGA Resolution 77/1 (2022)	"Principles of the UN Charter for a Just Peace in Ukraine"	Demands the complete withdrawal of Russian troops and the restoration of Ukraine's sovereignty	Consolidates the international position on the need to end the occupation
UNGA Resolution No. 78/316 (11 July 2024)	"Safety and protection of nuclear facilities of Ukraine, in particular ZNPP"	Condemns Russia's military actions near nuclear facilities, demands their de-occupation	Highlights the threat to global nuclear security posed by Russia's actions
UN General Assembly Resolution ES-11/8 (24 February 2025)	"The Path to Peace"	Reaffirms Ukraine's sovereignty, calls for a just peace based on the UN Charter	The international community reaffirmed the qualification of the Russian Federation as an aggressor state and the need to bring it to justice

Source: Systematized by the author based on [11–15].

The origins of the ideology of the "Russian world" go back to the post-imperial and Soviet concepts of "great Russia" and "a single historical space". Its modern form was institutionalized in the 2000s through several state documents – primarily the Concept of Foreign Policy of the Russian Federation (2008, 2013, 2016, 2023), which proclaims the need to "protect the rights of Russian citizens and compatriots abroad." This message is used by the special services of the Russian Federation as an official justification for influence operations, destabilizing campaigns and subversive activities on the territory of neighboring states, primarily Ukraine, Moldova, Georgia and the Baltic States.

The ideological component of the "Russian world" is based on three main pillars:

1. The messianic idea of the special role of Russia as a "defender of traditional values" and the "civilizational center" of Eastern Orthodoxy.
2. The myth of a single people of Russia, Ukraine and Belarus, denying the right of Ukrainians to separate statehood.
3. The cult of victory in World War II, which is used as a tool for political mobilization and propaganda of the "anti-Nazi mission" of the Russian Federation.

The special services of the Russian Federation, primarily the FSB, the GRU and the Foreign Intelligence Service, are actively integrated into the mechanism for implementing this ideology. Their activities are not limited to intelligence or counterintelligence tasks: they perform ideologically colored functions of influence aimed at supporting the Kremlin's narratives and creating a "zone of Russian cultural and information control". Through controlled media, churches, public organizations and "cultural centers", special services form a favorable environment for spreading the ideas of the "Russian world" among Russian-speaking communities abroad.

A key component of the ideological toolkit is the fusion of Orthodoxy with government propaganda. The Russian Orthodox Church, closely associated with the FSB, essentially plays the role of an ideological unit, legitimizing foreign policy expansion under spiritual slogans. Thus, the special services use the religious and cultural factor as a "soft power" to justify aggression and form ways to influence public opinion in other countries.

In the context of the war against Ukraine, the "Russian world" has become the central ideological tool that united the political, military and intelligence structures of the Russian Federation. Under his cover, disinformation operations, cyberattacks, support for collaborationist groups, as well as efforts to destroy Ukrainian identity and national unity, are carried out.

Thus, the concept of the "Russian world" is not a cultural or humanitarian doctrine in the classical sense, but constitutes an integrated ideological platform of state aggression, in which the special services of the Russian Federation play a systemic role. It provides an ideological justification for expansion, legitimizes violence and creates pseudo-legal grounds for Russia's subversive activities under the guise of "protecting compatriots" [10].

The Russian Federation implements its policy of aggression against Ukraine and other neighboring states through the complex activities of special services that combine traditional intelligence tasks with modern means of hybrid influence. The main areas of this activity are information and psychological operations, cyberattacks, sabotage and providing support to terrorist groups and proxy formations. This approach makes it possible to achieve the Kremlin's strategic goals without officially declaring war, extending its control to the information, economic and military space.

Table 2 systematizes the main activities of the special services of the Russian Federation, methods of their implementation, key goals and characteristic indicators, which allows you to clearly assess the complexity and effectiveness of this toolkit of aggressive policy.

Analysis of Table 2 shows that the special services of the Russian Federation apply a multidimensional strategy, where different areas of activity act synergistically. Information and psychological operations prepare public opinion and demoralize the population, cyberattacks and sabotage disrupt critical infrastructure and management, and the support of proxy structures allows you to implement tactical tasks without the direct participation of regular forces.

The special services of the Russian Federation use a multidimensional strategy, where information and psychological operations, cyber operations, sabotage and the promotion of proxy formations work synergistically. This set of tools allows you to achieve strategic goals while reducing the risks of a direct military clash and complicating the process of international response. Effective resistance requires integrated national measures and close coordination with international allies [19].

Table 2. The main activities of the special services of the Russian Federation in the implementation of the policy of aggression

Direction of activity	Definition	Key methods	"Goals"	Performance indicators
Information and Psychological Operations (IPSO)	A set of measures to influence the information field to achieve political and strategic goals	Propaganda, fake news, troll farms controlled by NGOs, PSYOP	Demoralization of the population and troops, legitimization of aggression, polarization of society	Spikes in both activities, coordinated narratives, controlled movements, and organizations
Cyber-attacks and cyber intelligence	Using digital tools to undermine security, economics, and governance	Phishing, APT operations, DDoS, ransomware, SCADA/ICS attacks	Paralysis of critical infrastructure, collection of strategic data, and economic blackmail	Attacks on government/critical networks, coincident with political events, use of known APT tools
Sabotage and sabotage	Physical actions to undermine infrastructure and combat capability	Explosions, fires, destruction of objects, and coordination with proxies	Disruption of logistics, demoralization, and creation of conditions for control of territories	Man-made accidents, simultaneous sabotage, and activity of controlled groups
Support for terrorist groups and proxy structures	Provision of resources and coordination of the actions of illegal formations	Financing, armament, training, and use of PMCs	Achieving strategic goals without the direct participation of regular forces, destabilizing regions	Flows of weapons and personnel, PMC activity, connections of pro-Russian groups with special services
Integration of tools (system approach)	Integration of tools (system approach)	Integration of tools (system approach)	Achieving strategic goals while minimizing a direct military clash	Simultaneous operations of different types, a high level of coordination between directions

Source: Systematized by the author based on [16–19].

The operations of Russian special services and special forces units have become a central element in the implementation of the Kremlin's strategic interests in the Ukrainian direction. From the first days of the conflict, these structures acted not as an auxiliary force, but as the main mechanism of political, military and information pressure. They combined methods of forceful intervention with finely planned hybrid scenarios – sabotage, cyberattacks, manipulation of public opinion, support for local pro-Russian groups.

In 2014, it was the special forces of the "green men" that became a key tool for the annexation of Crimea, an operation carried out with almost laboratory precision. In parallel with the military control of the territory, a large-scale information campaign was unfolded aimed at legitimizing the occupation and creating the illusion of "popular support". A similar scenario was repeated in Donbas, where Russian agents organized armed formations, provided them with equipment and funding, while coordinating the political component – the creation of pseudo-republics and "people's councils".

After 2022, the activities of these structures reached a new level. Under the cover of a full-scale offensive, the special services focused on parallel tasks: reconnaissance of critical infrastructure, intimidation of civilians, undermining energy systems, and conducting psychological operations in the digital space.

Table 3 summarizes the most notable episodes of the use of these tools – from operations in Crimea to the latest forms of hybrid aggression. They demonstrate how Russia systematically combines classic intelligence operations with the tools of modern information warfare, turning its special services into the main lever for the implementation of foreign policy.

The interference of Russian special services in the implementation of the policy of aggression creates the effect of multi-level influence – from global processes to local crises. Their activities create not only security risks, but also deep political, economic and communicative deformations. In the international arena, Moscow's actions have caused an erosion of trust between states, strengthened militarization trends in Europe, and forced NATO to reconsider the concept of collective defense.

Table 3. The use of Russian special services in foreign policy operations against Ukraine

Event (period)	Actions of the Russian special services	"Goal"
Annexation of Crimea (2014)	Seizure of administrative buildings, blocking of airports, "green men" without identification marks	Ensuring control over Crimea, organizing a "referendum", and legalizing annexation
War in Donbas (2014–2015)	Support for pro-Russian groups, the presence of Russian special forces, the supply of weapons, and intelligence	Destabilization of the region, creation of Russian-controlled "republics"
Full-scale invasion (2022–2025)	Landing of sabotage and reconnaissance groups, participation in battles for strategic objects, and elimination of key targets	Advancing Russia's military goals, destroying Ukraine's defense capabilities
Hybrid warfare and information influence	Cyberattacks, disinformation, propaganda campaigns, and economic pressure	Formation of pro-Russian public opinion, undermining Ukrainian stability

Source: Systematized by the author based on [20; 21, p. 98].

The activities of the special services of the Russian Federation have systematic, long-term and complex consequences. At the international level, it undermines the principles of security and international law, creates hybrid threats and escalation risks. At the regional level, it destabilizes neighboring states, undermines trust and threatens critical infrastructure. For Ukraine, these actions directly violate sovereignty and territorial integrity, destroy governance and defense systems, and weaken socio-political stability. Effective counteraction requires integrated measures at the national and international levels, including informational, cybernetic, defense and diplomatic components (Table 4).

Table 4. Consequences of the activities of the special services of the Russian Federation for the security and sovereignty of Ukraine

Direction of activity of the special services of the Russian Federation	Implications for international security	Implications for regional security	Consequences for Ukraine (sovereignty and territorial integrity)
Information and Psychological Operations (IPSO)	Undermining the stability of the international order, the creation of global information threats	Polarization of society in the region; destabilization of the political situation	Demoralization of the population; discrediting state institutions; spreading pro-Russian narratives
Cyber-attacks and cyber intelligence	Threat to international cybersecurity; escalation of potential conflicts	Disruption of the functioning of critical infrastructure; Economic vulnerability of neighboring states	Disabling government systems; undermining defense and management structures; a Threat to critical infrastructure
Sabotage and sabotage	Undermining international trust and security	Destabilization of transport and energy infrastructure; Threat to regional stability	Damage to strategic facilities; undermining logistics and life support; Threat to civilians
Support for terrorist groups and proxy structures (PMCs)	Using the "gray zone" to avoid direct liability, the spread of international tensions	Destabilization of neighboring states; escalation of local conflicts	Undermining security in the frontline regions, strengthening of separatist sentiments, and increased risk of violence
Integration of tools (system approach)	Integration of tools (system approach)	Synchronized attacks on regional security and infrastructure	Complex violation of sovereignty; complication of management and defense; demoralization of the population

Source: Systematized by the author based on [22–24].

Consideration of Table 4 proves that the activities of the special services of the Russian Federation pose systemic dangers to international and regional security, as well as significantly violate the sovereignty and territorial integrity of Ukraine. Information and psychological operations, cyberattacks,

and sabotage multiply the destabilization of regional institutions and critical infrastructure, and sponsorship of proxy structures and PMCs allows the Russian Federation to achieve strategic goals without direct military intervention.

The activity of the Russian special services forms a long and systemic chain of consequences that covers all levels of international security. On the global stage, these structures undermine trust between states, undermine the principles of international law, and create a new type of threat – hybrid, blurred, and difficult to identify. Over the past decade, the number of recorded cyberattacks related to the activities of Russian intelligence networks has more than tripled, demonstrating the scale and sustainability of this strategy.

The international community is demonstrating a multidimensional response to the activities of the Russian special services, which increasingly go beyond the usual diplomatic procedures. At the UN level, violations of the fundamental principles of international law are emphasized, while the European Union is increasing pressure due to economic restraints and political sanctions that have already affected more than 70 major enterprises of the Russian Federation in the period from 2020 to 2024, reducing their integration into global supply chains. At the same time, NATO is strengthening the alliance's eastern border by investing in the renewal of defense mechanisms and providing Ukraine with technical and strategic assistance in countering hybrid challenges, which include cyberattacks, disinformation and financial sabotage [24].

In practice, this is manifested in the fact that the operations of the Russian special services are increasingly seen not only as local incidents but as a systemic threat to international security and stability in the region. In several cases, it is observed that coordinated actions of Western institutions allow not only to deter potential escalation, but also to increase the effectiveness of preventive measures. The dynamics of the last four years show that the combination of sanctions pressure, diplomatic channels and defense strategies creates a complex barrier that can minimize the risks of hybrid conflicts spreading to neighboring states.

Modern special operations are increasingly integrating technological and information tools, transforming traditional forms of influence into a multidimensional pressure strategy. In the light of these trends, it can be seen that the international response to Russia's actions is becoming not just reactive but gradually proactive, forming new approaches to ensuring security and stability in Europe [16].

In light of Russia's full-scale invasion of Ukraine, the functioning of an effective system of counterintelligence and cyber defense has become an important component of state defense. The enemy zealously uses hybrid methods: from an agent network and sabotage to large-scale cyberattacks and information pressure, creating direct dangers to state institutions, vital infrastructure and military formations of the state.

To address these challenges, Ukraine has developed a multi-layered defense system that includes state and military counterintelligence, cyber defense of critical infrastructure, and unity with international allies. The main purpose of this system is to find, neutralize and protect against pervasive dangers created by the activity of the Russian special services.

Table 5 shows key bodies, areas of their activities and examples of specific steps in the field of counterintelligence and cyber defense, which makes it possible to visualize information about the Ukrainian security structure and weigh the effectiveness of its response to modern challenges.

The assessment of the system of counterintelligence and cyber defense measures of Ukraine shows the complexity and multi-layered nature of the state's approach to countering threats from Russian special services and hybrid aggression. The connection between the work of the Security Service of Ukraine, military counterintelligence, the State Service for Special Communications and International Cooperation guarantees effective detection, neutralization and preventive protection against agent activities, sabotage, cyberattacks and information attacks.

The system makes it possible to respond to dangers in time, protect critical infrastructure and important state facilities, and increase the overall degree of cyber resilience of the region. The integration of world experience and intelligence sharing with NATO, EU and US allies strengthens Ukraine's ability to counter modern types of hybrid warfare. Thus, counterintelligence and cyber defense measures are a vital component of national security and the foundation for protecting the sovereignty and sustainability of the state.

Table 5. Systematization of counterintelligence and cyber defense measures of Ukraine

Direction	Body/Unit	Task	Examples of specific measures
Counterintelligence measures	Security Service of Ukraine (SBU)	Detection and neutralization of agent activities of foreign special services, protection of strategic objects, and control of information security	Checking civil servants for ties with the Russian Federation, blocking pro-Russian networks, and detaining sabotage groups
	Military counterintelligence (Ministry of Defense, SBU)	Protection of military facilities and units from espionage and sabotage	Detection of Russian agents at the front, inspection of ammunition and equipment, and access control to strategic facilities
	National Police	Countering sabotage, terrorist attacks, and pro-Russian organizations	Prevention of subversive actions, detention of agents and organizers of provocations
Cyber defensive measures	State Service for Special Communications and Information Protection (SSSZI)	Protection of critical infrastructure and state information systems	Monitoring cyberattacks, blocking malware, and responding to intrusions in government networks
	CERT-UA	Responding to cybersecurity incidents, detecting threats	Malware analysis, coordination with other authorities, and publication of recommendations for enterprises
	Ministry of Digital Transformation	Cyber protection of government agencies, digital services	Protection of government portals, development of cybersecurity standards, and staff training
International cooperation	NATO, EU, USA	Threat Information Sharing, Training, Cyber Resilience Support	Joint exercises, development of protocols for responding to cyberattacks, and consultations on cyber defense

Source: Systematized by the author based on [25, p. 222; 26–28].

Increasing the effectiveness of countering the aggressive activities of the special services of the Russian Federation requires a systematic combination of national resources, legal mechanisms and international partnership. At the national level, the primary task is to strengthen the counterintelligence capabilities of the state by improving the analytical, operational and technical base of the Security Service of Ukraine and related structures. cyber operations of the Russian Federation through the creation of an integrated system for collecting and analyzing intelligence information, which will combine data from public and private actors.

An important vector is the optimization of the legal regulation of activities in the field of counterintelligence and cyber defense. It is necessary to update the legislative framework in view of modern forms of hybrid aggression – cyber espionage, disinformation campaigns, influential operations, and information pressure. It is expedient to form a special interagency coordinating cell to counter the activities of foreign intelligence services, which will ensure rapid data exchange, coordination of operational actions and analytical support for government decisions.

At the international level, it is advisable to deepen cooperation with the intelligence structures of NATO and the European Union, in particular in the field of joint intelligence processing, participation in multilateral trainings and the development of standards for responding to information and cyber threats. Ukraine should actively participate in technology exchange programs in the field of cybersecurity and counterintelligence, and develop partnerships with NATO centers of excellence (for example, CCDCOE in Tallinn).

In addition, it is important to strengthen the information and diplomatic component of the resistance. It is necessary to increase the international publication of evidence of the aggressive activities of the Russian special services, forming political and legal pressure on the invading state. The

development of international sanctions against persons involved in espionage and computer attacks must become one of the levers of deterrence.

No less important is the training of new generation specialists who are able to act in the conditions of a multidimensional hybrid war. It is mandatory to create professional training programs for counterintelligence analysts, cyber operations and security intelligence specialists in cooperation with the main universities of the EU and the United States.

In general, effective counteraction to the aggressive activities of the special services of the Russian Federation is possible only if national and international efforts are synchronized, the technological potential of intelligence is strengthened, the level of interagency coordination is increased, and a joint system of strategic deterrence is formed. This approach will allow Ukraine not only to defend itself, but also to act proactively in the field of information and cybersecurity, ensuring the long-term stability of national statehood.

6. Conclusions

Thus, the activities of the special services of the Russian Federation go far beyond the typical internal security and become a central tool for the implementation of the Kremlin's foreign policy aspirations. They act as a hidden mechanism for promoting the state policy of aggression, capable of influencing world processes without open military steps. This is manifested in the use of hybrid methods – from financial and political pressure to disinformation and cyberattacks, which makes it possible to achieve strategic objectives with minimal visibility in the arena of hostilities.

It is indicated that such a practice creates a new kind of foreign policy, where special operations become a continuation of the state strategy and, at the same time, a means of demonstrating power in the world context. In several episodes, it is noticed that through the manipulation of information flows and technological platforms, the Russian Federation is able to create political pressure on nearby states while reducing the risks of a direct armed clash. This capability makes the Kremlin's intelligence services not just a body of stability, but a key lever of geopolitical influence, the effectiveness of which is constantly assessed by international experts and strategic institutions.

The arrangement of counterintelligence and cyber defense steps of Ukraine against the special services of the Russian Federation indicates a high degree of coordination and adaptability of the state security system. Counterintelligence measures are the main lever for eliminating the activities of Russian special services aimed at destabilizing state structures and undermining national defense.

Effective protection against Russian cyber operations is achieved by merging sustainable counterintelligence methods with modern digital tools. The organizational and legal framework and interagency coordination ensure the legality of actions and the rapid effectiveness of measures. Continuous updating of practices, improvement of technical equipment and training of specialists increase the deterrent potential of the country. Together, these steps form a holistic doctrine of protecting Ukraine's vital infrastructure, information field and strategic goals, serving not just as a way to respond, but as part of the state strategy to counter Russian aggression.

References

1. Palyvoda, V. (2024). *Rosiiski psevdohromadski orhanizatsii yak instrument vplyvu Kremlia na vlasne suspilstvo ta svitovu hromadsku dumku* [Russian pseudo-public organizations as a tool of the Kremlin's influence on its own society and world public opinion]. 22.01.2024. https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/rosiyski-psevdohromadski-orhanizatsiyi-yak-instrument-vplyvu (in Ukrainian).
2. Sidchenko, S. O., Zalkin, S. V., Khudarkovskyi, K. I., Revin, O. V., Bielimov, V. V., & Bieliaiev, P. V. (2023). Osnovni trendy informatsiinoi kampanii Rosiiskoi Federatsii proty Ukrainy na pochatku 2023 roku [Main trends of the Russian Federation's information campaign against Ukraine in early 2023]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy – Science and Technology of the Air Force of the Armed Forces of Ukraine*, *1*(50), 106–120. https://doi.org/10.30748/nitps.2023.50.13 (in Ukrainian).
3. Wilde, G. (2022). *Cyber Operations in Ukraine: Russia's Unmet Expectations. Cyber conflict in the Russia-Ukraine war.* Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/202212-Wilde_RussiaHypotheses-v2.pdf
4. Ilnytskyi, V., Starka, V., & Haliv, M. (2022). Rosiiska propaganda yak element pidhotovky do zbroinoi agresii proty Ukrainy [Russian propaganda as an element of preparation for armed aggression against Ukraine].

Ukrainskyi istorychnyi zhurnal – Ukrainian Historical Journal, (5), 46–53. https://doi.org/10.15407/uhj2022.05.043 (in Ukrainian).

5. Melnichenko, O. A. (2021). Osnovni napriamy destruktyvnoi diialnosti rosiiskykh spetssluzhb v informatsiinii viini proty Ukrainy [The main directions of destructive activity of Russian special services in the information war against Ukraine]. In *Hybrid warfare: Essence, challenges and threats: Proceedings of the Roundtable* (pp. 31–32). National Academy of the Security Service of Ukraine. https://duikt.edu.ua/uploads/p_293_46483431.pdf (in Ukrainian).
6. Verkhovtseva, I. H. (2024). Hlobalnyi kiberprostir ta opir informatsiinii ahresii: Kiberdyplomatiia Ukrainy u protydii rosiiskii informatsiinii invazii [Global cyberspace and resistance to information aggression: Ukraine's cyber diplomacy in countering the Russian information invasion]. In *Mizhnarodne spivtovarystvo ta Ukraina v protsesakh ekonomichnoho ta tsyvilizatsiinoho postupu: Aktualni ekonomiko-tekhnolohichni, resursni, instytutsionalni, bezpekovi ta sotsiohumanitarni problemy* [The international community and Ukraine in the processes of economic and civilizational progress: Current economic-technological, resource, institutional, security, and socio-humanitarian problems] (pp. 213–243). Baltija Publishing. https://doi.org/10.30525/978-9934-26-480-1-9 (in Ukrainian).
7. Maliuk, V. V. (Ed.). (2023). *Zlochynna kolaboratsiia v umovakh zbroinoi ahresii: Praktychnyi poradnyk z kryminalno-pravovoi otsinky ta rozmezhuvannia* [Criminal collaboration in conditions of armed aggression: A practical guide to criminal legal assessment and demarcation]. Alerta. https://dspace.nlu.edu.ua/bitstream/123456789/19713/1/Zlochinna_kolaboraciya.pdf (in Ukrainian).
8. Samarets, H. I. (2020). Polityka rosiiskoi federatsii shchodo prydnistrovskoho konfliktu. ukrainskyi vymir [The policy of the Russian Federation regarding the Transnistrian conflict. Ukrainian dimension]. *Politychne zhyttia – Political Life*, (2), 125–131. https://doi.org/10.31558/2519-2949.2020.2.17 (in Ukrainian).
9. *Hibrydni zahrozy Ukraini i suspilna bezpeka. Dosvid YeS i Skhidnoho partnerstva* [Hybrid threats to Ukraine and public security. Experience of the EU and the Sikh partnership]. (2018). Ukrainian Center for European Policy.https://geostrategy.org.ua/analityka/doslidzhennya/gibrydni-zagrozy-ukrayini-i-suspilna-bezpeka-dosvid-yes-i-shidnogo-partnerstva/zavantazhyty-pdf (in Ukrainian).
10. Kononenko, K. (2025). *"Hibrydna" stratehiia Rosiiskoi Federatsii shchodo krain Yevropy: formy, zmist i mozhlyvi zasoby protydii* [The "hybrid" strategy of the Russian Federation towards European countries: forms, content and possible means of counteraction]. Konrad Adenauer Stiftung. https://www.kas.de/documents/d/ukraine/kononenko_hybrid_strategy_of_russia_ukr (in Ukrainian)
11. Statut Orhanizatsii Obiednanykh Natsii [Charter of the United Nations]. (1945). United Nations. https://zakon.rada.gov.ua/laws/show/995_010/stru (in Ukrainian).
12. Popravky do Rymskoho statutu Mizhnarodnoho kryminalnoho sudu shchodo zlochynu ahresii [Amendments to the Rome Statute of the International Criminal Court regarding the crime of aggression]. (2024). International Criminal Court. https://zakon.rada.gov.ua/laws/show/995_004-10#Text (in Ukrainian).
13. United Nations General Assembly. (2022). Aggression against Ukraine: Resolution ES-11/1. United Nations Digital Library. https://digitallibrary.un.org/record/3965290?ln=ru&v=pdf
14. United Nations General Assembly. (2024). Resolution A/RES/78/316. United Nations Press. https://press.un.org/en/2024/ga12614.doc.htm
15. United Nations General Assembly. (2025). Resolution A/RES/ES-11/8. United Nations Documents. https://docs.un.org/en/A/RES/ES-11/8
16. Calle, M. (2025, August 30). *Cyber warfare in Russo-Ukrainian war. International Relations Review*. https://www.irreview.org/articles/2025/8/28/cyber-warfare-in-russo-ukrainian-war
17. Russian cyber-attacks against NATO states up by 25% in a year, analysis finds. (2025, October 16). *The Guardian*. https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds
18. Brown, W. (2025, October 22). *The bear and the bot farm: Countering Russian hybrid warfare in Africa*. https://ecfr.eu/publication/the-bear-and-the-bot-farm-countering-russian-hybrid-warfare-in-africa/
19. Beznosiuk, M. (2025, June 5). Russian hybrid warfare: Ukraine's success offers lessons for Europe. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/russian-hybrid-warfare-europe-should-study-ukraines-unique-experience/
20. Boi za DAP, potuzhnyi spysok operatsii, pershyi koreiskyi polonenyi: Boiovyi keis znamenytoho 8-ho polku SSO [Battles for DAP, a powerful list of operations, the first Korean prisoner: A combat case of the famous 8th SSO Regiment]. (2025, October 1). *Vechirniy Kyiv*. https://vechirniy.kyiv.ua/news/117966/

21. Khudarkovskyi, K.I., Sidchenko, S.O., Zalkin, S.V., Bielimov, V.V., Revin, O.V., Shyhimaha, N.V. (2025). Osoblyvosti hibrydnoi viiny rosiiskoi federatsii proty Ukrainy [Features of the Russian Federation's hybrid war against Ukraine]. *Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl – Collection of Scientific Papers of the Kharkiv National Air Force University*, *1*(83), 98-105. https://doi.org/10.30748/zhups.2025.83.12 (in Ukrainian).
22. Countering disinformation with facts – Russian invasion of Ukraine (2025). *Global Affairs Canada*. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng
23. Colling, J. (2024, January 8). Recapping "cyber in war: Lessons from the Russia-Ukraine conflict". *Lieber Institute West Point*. https://lieber.westpoint.edu/recapping-cyber-war-lessons-russia-ukraine-conflict/
24. Jones, S. G. (2025, March 18). Russia's shadow war against the West. *Center for Strategic and International Studies*. https://www.csis.org/analysis/russias-shadow-war-against-west
25. Myrhorod, V. V. (2024). Diialnist sluzhby bezpeky ukrainy v konteksti natsionalnoi bezpeky [Activities of the Security Service of Ukraine in the context of national security]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu – Scientific Bulletin of Uzhhorod National University*, *82*(2), 222–227. https://doi.org/10.24144/2307-3322.2024.82.2.35 (in Ukrainian).
26. *Derzhspetszviazku: Yak CERT-UA reahuie na kiberintsydenty – vid povidomlennia do likvidatsii naslidkiv* [State Special Communications Agency: How CERT-UA responds to cyber incidents - from notification to elimination of consequences]. (2025, Fabruary 10). Government of Ukraine. https://www.kmu.gov.ua/news/derzhspetszviazku-iak-cert-ua-reahuie-na-kiberintsydenty-vid-povidomlennia-do-likvidatsii-naslidkiv (in Ukrainian).
27. Pitsun, I.D. (2023). Sutnist i zmist kontrrozviduvalnoho zabezpechennia Syl TrO ZSU: aspekty teorii ta praktyky [The essence and content of counterintelligence support of the Armed Forces of the Armed Forces of Ukraine: aspects of theory and practice]. *Akademichni vizii – Academic visions*, (15). http://dx.doi.org/10.5281/zenodo.8369123 (in Ukrainian).
28. Stender, S. V., Froter, O. S., Snitko, Yu.M. (2023). Tsyfrova intehratsiia ta kiberzakhyst ekonomiky Ukrainy: pravovi aspekty ta innovatsiini stratehii [Digital integration and cyber protection of the Ukrainian economy: legal aspects and innovative strategies]. *Akademichni vizii – Academic visions*, (26). http://dx.doi.org/10.5281/zenodo.10389831 (in Ukrainian).