population in particular, etc.

The prospects of further scientific research in this direction are outlined, which will be aimed at developing conceptual approaches to the prevention and counteraction of economic criminality in Ukraine under martial law and in the post-war period.

***Key words:*** *national security of Ukraine, state security, martial law, economic criminality, criminal offenses in the field of economic activity, criminal offenses related to the use of budget funds, criminal offenses in the field of official activity and professional activity related to the provision of public services, criminological characteristics, determinants, prevention.*

UDC 343.97
DOI: 10.31733/2078-3566-2024-5-28

**Eduard RYZHKOV**©
Ph.D. in Law, Professor
*(Dnipro State University of Internal Affairs, Dnipro, Ukraine)*

## COUNTERING CORRUPTION IN UKRAINE IN THE FIELD OF INFORMATIZATION UNDER MARTIAL LAW

**Едуард Рижков. ПРОТИДІЯ КОРУПЦІЇ В УКРАЇНІ У СФЕРІ ІНФОРМАТИЗАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ.** Досліджено актуальні проблеми протидії корупції у сфері інформаційної безпеки України в умовах воєнного стану.

Наголошено, що корупційні прояви в цьому секторі становлять загрозу не лише для ефективності функціонування державних інституцій, а й для національної безпеки загалом.

Вивчено ключові причини корупційних ризиків, що обумовлюють негативні наслідки, зокрема витоки критично важливої інформації, компрометацію державних реєстрів і зниження обороноздатності.

Особливу увагу приділено аналізу конкретних прикладів корупційних діянь у секторі інформаційної безпеки та викликів, пов'язаних зі впровадженням сучасних технологій, зокрема штучного інтелекту, як дієвого інструменту для боротьби з корупцією.

Акцентовано, що корупційні прояви в інформаційній сфері є критично небезпечними для функціонування державних інституцій та обороноздатності України, особливо в умовах воєнного стану. Такі діяння підривають довіру суспільства до державного управління, знижують ефективність роботи силових структур та можуть призводити до витоків стратегічно важливих даних.

Запропоновано комплекс заходів для мінімізації корупційних ризиків, як-от посилення правових санкцій, оптимізація функцій державних інституцій, розвиток міжнародної співпраці та запровадження технологій автоматизації.

Штучний інтелект та автоматизовані системи розглядаються як важливі інструменти мінімізації корупційних ризиків. Їх використання дозволить підвищити прозорість процесів, знизити ризики незаконного втручання та оптимізувати функціонування державного апарату.

Зроблено висновок, що ефективна протидія корупції в інформаційній сфері є невід'ємною складовою збереження національної безпеки та суверенітету України.

***Ключові слова:*** *корупція, сектор безпеки і оборони, кібербезпека, інформаційні технології, штучний інтелект, воєнний стан, ІТ-сфера, ІТ-коаліція.*

**Relevance of the study.** In Ukraine, as in many other countries, the functioning of state institutions responsible for information security is accompanied by corruption risks and negative manifestations. Corruption in this area not only undermines the efficiency of these structures but also poses significant threats to national security, especially during armed conflict. These negative phenomena require not only prompt responses from state authorities but also active public involvement in exposing, preventing, and combating corruption.

One of the key factors in ensuring the effectiveness of Ukraine's multi-tiered and complex information security management system is a comprehensive approach to minimizing


ORCID iD: https://orcid.org/0000-0002-6661-4617
eduard.ryzhkov@dduvs.edu.ua

corruption risks. This involves the clear identification, prevention, and eradication of corrupt practices within the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the Armed Forces of Ukraine, and other military formations and law enforcement agencies stipulated by the current legislation.

During martial law, when Ukrainian society has united to defend the country's territorial integrity and sovereignty, the fight against all forms of corruption in governance and national security systems becomes critically important. Particular emphasis must be placed on eradicating corrupt practices among leadership, military personnel, and law enforcement officers, as these structures ensure the country's defense capability and the stability of public institutions. Achieving this task is not only a component of national security strategy but also a guarantee of public trust in state governance and the effective functioning of the defense sector.

Well-documented cases of corruption in the country's information sector during martial law highlight the significant impact of such illegal actions on the nation's defense capability due to their societal danger.

Therefore, combating corruption in Ukraine's information security sector should become a priority area of state policy. This policy should involve scientifically grounded approaches, the implementation of information and technological innovations, active interagency cooperation, and public participation to achieve a high level of security and defense capability.

**Recent publications review.** The issue of combating corruption in the field of informatization under martial law is addressed in Ukrainian scientific literature in a limited and fragmented manner. In most cases, the legal aspects of anti-corruption efforts within law enforcement, the Armed Forces, the Security Service of Ukraine, the State Service of Special Communications and Information Protection, and other security and defense sector entities are only part of broader studies on national anti-corruption policy.

The topic of corruption in Ukraine has been explored in the works of scholars such as V. Averyanov, O. Bandurka, L. Zubkova, R. Kalyuzhny, Yu. Kovbasyuk, M. Kravchuk, I. Lavriv, M. Melnyk, A. Movchan, A. Moshnin, A. Novak, Ye. Pashchenko, S. Rohulsky, V. Fedorenko, M. Chaly, and others.

At the same time, the search for the causes of corruption in Ukraine's informatization sector under martial law requires separate scientific investigation.

**The article's objective** is to study the causes of corruption in Ukraine's informatization sector under martial law and to identify measures to counter it.

The article continues with detailed descriptions of: Legislative frameworks such as Ukraine's "Law on the Basics of Cybersecurity"; Critical issues specific to the IT sector, including restricted access classifications and state monopolization; Real-world examples of corruption cases and their consequences; Proposed solutions, including leveraging artificial intelligence and international collaboration to combat corruption.

The conclusion emphasizes the urgent need for systemic measures to combat corruption in Ukraine's information sphere, particularly during wartime, to safeguard national security and sovereignty.

**Discussion.** Ukraine's information sphere, according to current legislation, specifically the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine," is recognized as a priority area for state protection [1]. This sector is critically important due to several factors:

- The sensitivity of information containing data about citizens and the management of critical infrastructure;
- The significant volume of financial and material resources involved in its operation;
- The high level of responsibility required from users of information systems, which imposes special requirements on them.

For these reasons, the IT sphere is additionally protected by classifications of restricted access and confidentiality, given the nature of the information it processes. It has a limited circle of users, which, in turn, imposes specific restrictions on these individuals, including additional requirements.

The information sector is effectively under state monopoly, necessitating enhanced accountability for officials. Given the limited public oversight of this sphere, their level of responsibility before the law must be unconditional.

The international and domestic experience since 2014, supplemented by analytical insights into contemporary challenges, demonstrates that during martial law, corruption risks in the information sector can lead to severe societal consequences. These include: A decline in the

country's defense capability, particularly due to leaks of strategically important data; Reduced efficiency of key state institutions such as the Armed Forces of Ukraine, law enforcement agencies, and critical infrastructure facilities; The compromise of state registries and the banking system, posing threats to economic stability; The vulnerability of citizens due to data breaches, which can be exploited by adversaries for manipulation and destabilization.

Over the decade of Russian military aggression against Ukraine, the frequency of corruption cases in the security and defense sectors has shown a growing trend.

According to A. Moshnin, the general causes of increasing corruption in Ukraine include inefficient management, legislative deficiencies, societal moral decay, the rise of new moral values centered on personal success and enrichment, and the inefficiency of most state institutions [2, p. 107].

Corruption in the information sphere, as revealed through law enforcement investigations, reports by civil society organizations, journalists, and international partners, reflects a persistent negative situation marked by repeated illegal practices.

During martial law, this situation creates additional risks to national security and defense, beyond undermining the fundamental societal relations protected by law in the realm of public order.

Analysis of Key Examples of Corruption. The analysis of known corruption cases highlights the significant vulnerability of the information sector in the security and defense domains. Key incidents include:

1. The organization of a criminal group by a former head of the IT Department of the Ministry of Internal Affairs, involving the illegal use of information from the National Police's Information and Communication System Portal [3].
2. Embezzlement of budgetary funds by leaders of the State Service of Special Communications and Information Protection of Ukraine through criminal schemes [4].
3. The scandal surrounding the illegal enrichment of the Head of the Counterintelligence Protection Department in the Information Security Sector of the Security Service of Ukraine, which led to his dismissal [5].
4. Data leaks from the "Diia" application [6], the lack of public dialogue on this issue, and the failure to hold individuals accountable even after the acknowledgment of this fact by U.S. judicial authorities [7].
5. The absence of public accountability for individuals responsible for the inadequate protection of information in state registries, with breaches, damage, and destruction occurring following enemy cyberattacks in late 2024 [8].
6. Lobbying of legislative initiatives to strengthen the influence of the State Service of Special Communications and Information Protection of Ukraine in the information security sector, despite corruption scandals [9].
7. Exposure of a series of abuses in the implementation of information policies by a former Deputy Minister of Defense of Ukraine [10].

A common feature of these offenses is the conducive environment for their commission and the lack of enforcement of the principle of inevitable punishment for the perpetrators.

It is likely that the situation would improve if the proposal voiced by legal experts and society were implemented—corruption during martial law should be equated with acts of treason or, at the very least, collaboration with the enemy.

We support the view of Ye. M. Pashchenko and M. H. Chaly that there is a need to ensure full implementation of the principle of inevitability of punishment for individuals in uniform who commit acts of corruption [11, p. 216].

In any case, it is evident that during wartime, applying measures designed for peacetime to officials whose activities exhibit signs of corruption is insufficiently effective. This is especially critical for individuals involved in corrupt activities in the information sector, which, as previously noted, is highly vulnerable and has the potential to result in societal harm of a more destructive nature, up to and including the loss of statehood and sovereignty.

Under martial law, corruption in some cases is closely linked to treason or facilitates it in the most direct manner, given favorable conditions and prerequisites.

From our perspective, based on the moral and legal principles developed by humanity at the start of the 21st century, corruption by public officials in a country under martial law reflects a profoundly deficient level of personal awareness and legal consciousness. Such individuals should be stripped of their authority and punished in the most appropriate manner available in the state, taking into account the potentially dangerous societal consequences of their

actions.

A real alternative to subjective thinking and improper actions by individuals prone to corruption lies in artificial intelligence (AI) and machine learning tools, which are inherently the most effective instruments in the field of information technology.

Although AI technology still lacks clear legal regulation, Ukraine has already made initial steps toward its development [12, p. 123]. For instance, in 2020, Ukraine adopted the Concept for the Development of Artificial Intelligence, which outlines the main directions for its advancement in the country [13].

In any case, given the shortage of state resources caused by the war, AI represents perhaps the only truly effective tool capable of compensating for this factor and positively influencing the country's recovery during and after the war.

Moreover, artificial intelligence can be successfully utilized as an analytical tool for solving criminal offenses, including corruption-related crimes [14, p. 38].

Thus, what measures can a society under martial law take to combat corruption in the IT sector? In our opinion, the necessary measures should include the following:

1. Equate the qualifying characteristics of corruption crimes to those of treason during martial law, or expand the qualifying features of corruption offenses to allow for stricter sanctions.
2. Develop international cooperation through the creation of IT coalitions analogous to "Ramstein," uniting international partners in combating cyber threats and corruption in the information sphere.
3. Prevent the establishment of structures within the public sector that exhibit monopolistic influence on the IT services market or in performing state information functions.
4. Optimize the functions of public institutions by transferring non-core financial and economic functions to the private sector under strict regulation and supervision.
5. Legally oppose lobbying efforts aimed at introducing legislation to advance corrupt interests and monopolistic influence in IT-related societal relations.
6. Consider the possibility of introducing artificial intelligence in the informatization sphere at the level of state policy formation and implementation. Minimize the human factor in automation processes to optimize and enhance efficiency.

**Conclusions.** The main causes of corruption in the information sphere include the low accountability of officials, limited public oversight, legislative inefficiencies, and management shortcomings. Corruption is further exacerbated by monopolistic practices in the information security sector and inadequate anti-corruption mechanisms.

Corruption in the information sector during wartime acts as a catalyst for risks to national security and sovereignty. Implementing a systemic approach to combating such manifestations, including strengthening accountability, fostering international cooperation, and enhancing public oversight, is critically important for maintaining state stability.

The analysis of corruption causes and consequences during wartime requires further scientific research, particularly regarding the integration of advanced technologies into the national security domain. Strengthening legislation aimed at increasing accountability for corruption crimes is also a vital direction.

Combating corruption in the information sphere under martial law is not only a challenge but an essential condition for ensuring Ukraine's national security, territorial integrity, and sovereignty. A comprehensive approach encompassing legal, organizational, and technological measures is necessary to ensure the state's resilience against internal and external threats.

**Список використаних джерел**

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Мошнін А. Корупція у сучасній Україні: стан та напрями протидії. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління.* 2022. № 2 (62). С. 106–110. URL : https://doi.org/10.32689/2523-4625-2022-2(62)-16.

3. Поліція затримала групу осіб на чолі з колишнім посадовцем НПУ за несанкціоноване використання службової інформації. *Міністерство внутрішніх справ України.* URL : https://mvs.gov.ua/press-center/news/Policiya_zatrimala_grupu_osib_na_choli_z_kolishnim_posadovcem_NPU_za_nesankcionovane_vikoristannya_sluzhbovoi_informacii__18445.

4. Жирій К. Уряд звільнив голову Держспецзв'язку та його заступника через корупцію. *УНІАН.* URL : https://www.unian.ua/society/uryad-zvilniv-golovu-derzhspeczv-yazku-ta-yogo-

zastupnika-cherez-korupciyu-12461352.html.

5. Буняк В. Президент звільнив Іллю Вітюка з посади керівника Департаменту кібербезпеки. *Детектор медіа.* URL : https://detector.media/infospace/article/226230/2024-05-01-prezydent-zvilnyv-illyu-vityuka-z-posady-kerivnyka-departamentu-kiberbezpeky/.

6. У комітеті Ради хочуть покликати міністра Федорова на засідання через можливий витік даних із Дії. *New Voice.* URL : https://nv.ua/ukr/ukraine/politics/vitik-danih-diya-komitet-radi-hoche-poklikati-fedorova-na-zasidannya-50431845.html.

7. За що американці засудили Дію. *Espreso.* URL : https://espreso.tv/poglyad-za-shcho-amerikantsi-zasudili-diyu.

8. Проект Закону про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури від 29.09.2022 № 8087. URL : https://itd.rada.gov.ua/billInfo/Bills/Card/40553.

9. Дейнега В. Корупція в Держспецзв'язку. *Останній бастіон.* URL : https://bastion.tv/korupciya-v-derzhspeczvyazku_n59118.

10. Про корупцію у Держспецзв'язку та на проєкті «Армія дронів». Обговорюємо пост Віталія Дейнеги. *DOU.ua.* URL : https://dou.ua/forums/topic/46312/.

11. Пащенко Є. М., Чалий М. Г. Організаційно-правові засади протидії корупції в секторі безпеки і борони України на відомчому рівні. *Південноукраїнський правничий часопис.* 2022. Вип. 4. Ч. 3. С. 213–216. URL : https://doi.org/10.32850/sulj.2022.4.3.35.

12. Рижков Е. В., Синиціна Ю. П., Прокопов С. О. та ін. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посібник. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 181 с.

13. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02 грудня 2020 р. № 1556-р. URL : https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

14. Рижков Е. В., Писаренко Н. Ю. Штучний інтелект як аналітичний інструмент для розкриття кримінальних правопорушень. *Актуальні питання забезпечення діяльності органів і підрозділів системи МВС технічними засобами в умовах воєнного стану : матеріали II Всеукр. наук.-практ. конф.* (м. Київ, 25 квіт. 2024 р). Київ : ДНДІ МВС, 2024. С. 38–39.

*Надійшла до редакції 26.11.2024*
*Прийнято до опублікування 02.12.2024*

***References***

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity in Ukraine] : Zakon Ukrainy vid 05 zhovtnia 2017 r. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text. [in Ukr.].

2. Moshnin, A. (2022) Koruptsiia u suchasnii Ukraini: stan ta napriamy protydii [Corruption in modern Ukraine: the state and directions of counteraction]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia.* № 2 (62), pp. 106–110. URL : https://doi.org/10.32689/2523-4625-2022-2(62)-16. [in Ukr.].

3. Politsiia zatrymala hrupu osib na choli z kolyshnim posadovtsem NPU za nesanktsionovane vykorystannia sluzhbovoi informatsii [Police detained a group of people led by a former NPU official for unauthorized use of official information]. *Ministerstvo vnutrishnikh sprav Ukrainy.* URL : https://mvs.gov.ua/press-center/news/Policiya_zatrimala_grupu_osib_na_choli z kolishnim_posadovcem_NPU_za_nesankcionovane_vikoristannya_sluzhbovoi_informacii__18445. [in Ukr.].

4. Zhyrii, K. Uriad zvilnyv holovu Derzhspetszviazku ta yoho zastupnyka cherez koruptsiiu [Government dismissed the head of the State Special Communications Service and his deputy due to corruption]. *UNIAN.* URL : https://www.unian.ua/society/uryad-zvilniv-golovu-derzhspeczv-yazku-ta-yogo-zastupnika-cherez-korupciyu-12461352.html. [in Ukr.].

5. Buniak, V. Prezydent zvilnyv Illiu Vitiuka z posady kerivnyka Departamentu kiberbezpeky [The President dismissed Ilya Vityuk from the post of head of the Cybersecurity Department]. *Detektor media.* URL : https://detector.media/infospace/article/226230/2024-05-01-prezydent-zvilnyv-illyu-vityuka-z-posady-kerivnyka-departamentu-kiberbezpeky/. [in Ukr.].

6. U komiteti Rady khochut poklykaty ministra Fedorova na zasidannia cherez mozhlyvyi vytik danykh iz Dii [The Rada committee wants to summon Minister Fedorov to a meeting due to a possible data leak from Diya]. *New Voice.* URL : https://nv.ua/ukr/ukraine/politics/vitik-danih-diya-komitet-radi-hoche-poklikati-fedorova-na-zasidannya-50431845.html. [in Ukr.].

7. Za shcho amerykantsi zasudyly Diiu [What the Americans condemned Diya for]. *Espreso.* URL : https://espreso.tv/poglyad-za-shcho-amerikantsi-zasudili-diyu. [in Ukr.].

8. Proekt Zakonu pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo nevidkladnykh zakhodiv posylennia spromozhnostei iz kiberzakhystu derzhavnykh informatsiinykh resursiv ta obiektiv krytychnoi informatsiinoi infrastruktury [Draft Law on Amendments to Certain Laws of Ukraine Regarding Urgent Measures to Strengthen Cybersecurity Capabilities of State Information Resources and Critical

Information Infrastructure Facilities] vid 29.09.2022 № 8087. URL : https://itd.rada.gov.ua/billInfo/Bills/Card/40553. [in Ukr.].

9. Deineha, V. Koruptsiia v Derzhspetszviazku [Corruption in the State Special Communications Service]. *Ostannii bastion.* URL : https://bastion.tv/korupciya-v-derzhspeczvyazku_n59118. [in Ukr.].

10. Pro koruptsiiu u Derzhspetszviazku ta na proiekti «Armiia droniv». Obhovoriuiemo post Vitaliia Deinehy [About corruption in the State Service for Special Communications and the «Army of Drones» project]. *DOU.ua.* URL : https://dou.ua/forums/topic/46312/. [in Ukr.].

11. Pashchenko, Ye. M., Chalyi, M. H. (2022) Orhanizatsiino-pravovi zasady protydii koruptsii v sektori bezpeky i borony Ukrainy na vidomchomu rivni [Organizational and legal principles of combating corruption in the security and defense sector of Ukraine at the departmental level]. *Pivdennoukrainskyi pravnychyi chasopys.* Vyp. 4. Ch. 3, pp. 213–216. URL : https://doi.org/10.32850/sulj.2022.4.3.35. [in Ukr.].

12. Ryzhkov, E. V., Synytsina, Yu. P., Prokopov, S. O. ta in. (2024) Informatsiino-analitychne zabezpechennia pravookhoronnoi diialnosti [Information and analytical support of law enforcement activities] : navch. posibnyk. Dnipro : Dniprov. derzh. un-t vnutr. sprav. 181 p. [in Ukr.].

13. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini [On approval of the Concept of the development of artificial intelligence in Ukraine] : rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02 hrudnia 2020 r. № 1556-r. URL : https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text. [in Ukr.].

14. Ryzhkov, E. V., Pysarenko, N. Yu. (2024) Shtuchnyi intelekt yak analitychnyi instrument dlia rozkryttia kryminalnykh pravoporushen [Artificial intelligence as an analytical tool for revealing criminal offenses]. *Aktualni pytannia zabezpechennia diialnosti orhaniv i pidrozdiliv systemy MVS tekhnichnymy zasobamy v umovakh voiennoho stanu : materialy II Vseukr. nauk.-prakt. konf.* (m. Kyiv, 25 kvit. 2024 r). Kyiv : DNDI MVS, pp. 38–39. [in Ukr.].

**ABSTRACT**

The article explores the pressing issues of combating corruption in Ukraine's information security sector, particularly under martial law. It emphasizes that corruption in this sector threatens not only the efficiency of public institutions but also national security as a whole. The key causes of corruption risks are analyzed, along with their negative consequences, such as the leakage of critically important information, the compromise of state registries, and a decline in defense capability. Special attention is paid to specific examples of corruption in the information security sector and the challenges associated with implementing modern technologies, such as artificial intelligence, as effective tools for combating corruption.

The article highlights that corruption in the information sphere poses critical dangers to the functioning of public institutions and Ukraine's defense capability, especially during martial law. Such actions undermine public trust in state governance, reduce the efficiency of security structures, and can lead to the leakage of strategically important data.

A comprehensive set of measures is proposed to minimize corruption risks, including strengthening legal sanctions, optimizing the functions of state institutions, fostering international cooperation, and implementing automation technologies. Artificial intelligence and automated systems are considered essential tools for mitigating corruption risks. Their use will increase transparency, reduce the risks of illegal interference, and optimize the functioning of the state apparatus.

It is concluded that effective anti-corruption measures in the information sector are an integral part of preserving Ukraine's national security and sovereignty.

***Keywords:*** *corruption, security and defense sector, cybersecurity, information technologies, artificial intelligence, martial law, IT sector, IT coalition.*