

participation in the upbringing of a child, the place of his residence, the appointment of alimony, the establishment of guardianship/care, adoption, deprivation of parental rights or removal of a child without depriving parents of parental rights, etc.

Keywords: *child, child rights, child protection, administrative and legal protection of children, juvenile justice, juvenile prevention, foreign experience.*

UDC 341.3

DOI 10.31733/2078-3566-2022-5-55-60



Eduard RYZHKOV[©]
Ph.D. (Law), Professor
(Dnipropetrovsk State University
of Internal Affairs, Dnipro, Ukraine)

PROBLEMATIC ISSUES OF STAFFING CYBER TROOPS OF UKRAINE UNDER MARTIAL LAW

Едуард Рижков. ПРОБЛЕМНІ ПИТАННЯ КАДРОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРВІЙСЬК УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ. У статті розглянуто передумови створення кібервійськ Міністерства оборони України, появи первинних правових документів, що повинні у майбутньому сприяти розробці відповідного закону та підзаконних актів з цього питання. Наголошується, що наявність в Україні системи суб'єктів захисту кібернетичного простору держави в умовах воєнного стану та у оглядній перспективі сусідства з російським агресором не може в повній мірі забезпечити виконання збройними силами України їх основних функцій щодо захисту країни. Аргументується необхідність створення кібервійськ в державі з огляду на їх потенційний функціонал та його відмінність від того, що притаманний вже існуючим в Україні суб'єктам кібер захисту. Приділяється увага питанням підбору кадрів до майбутніх кібервійськ. Зазначаються їх форми та види з огляду на українські реалії та стан громадянського суспільства. Позначаються існуючі в державі проблеми співпраці державницьких інституцій з суб'єктами громадської ініціативи у сфері захисту кіберпростору. Наводяться приклади потенційних та реальних фактів порушень законодавства з боку правоохоронних органів по відношенню до представників громадської кібер спільноти.

Пропонуються підходи до формування кадрового резерву кібервійськ з урахуванням їх суб'єктності. В процесі дослідження аргументується твердження про те, що розвиток воєнної ситуації в країні обумовлює необхідність внесення коректив до плану реалізації Стратегії кібербезпеки України, затвердженої у 2021 році, з метою активізації розробки відповідного законопроекту зі створення кібервійськ.

Констатується, що відсутність належної динаміки у питанні законотворчості з цього питання позбавляє збройні сили України Міністерства оборони своєчасного створення і надання ним дієвого інструменту протидії ворогові за захисту країни. У висновку висловлюються пропозиції щодо можливих підходів у кадровому забезпеченні кібервійськ на підготовчому та проміжному етапах запуску цього державницького інституту.

Ключові слова: *Стратегія кібербезпеки, кібервійська Міністерства оборони України, кадрове забезпечення кібервійськ, законодавче забезпечення кібервійськ, співпраця державних органів з ІТ-фахівцями.*

Relevance of the study. Over the last 20 years of their existence in Ukraine, entities providing cyber protection and countering illegal manifestations in the field of information technologies have gone through various stages of development – from creation, filling with personnel potential to certain achievements. And although the system of cyber entities has acquired permanent features over the years, it did not meet the needs of our society in view of the threats brought by russian military aggression. The main problem was the improper

coordination of the actions of already existing subjects of combating cyber incidents in view of the need for operational support of the main subject of state protection in the conditions of martial law – the armed forces of Ukraine. The situation that developed at the beginning of 2022 made it impossible for the armed forces of Ukraine to effectively implement operations against the enemy using the cyber environment. Therefore, in conditions where objectively all signs point to a real cyber war with the participation of Ukraine, there was a need to create such a new entity as a cyber force in the structure of the armed forces of Ukraine with the subsequent need for their personnel support.

Hostilities on the territory of Ukraine with the Russian aggressor have been going on since 2014. However, in the issue of ensuring the security of the state's cyberspace, appropriate measures were taken rather slowly. That is why the full-scale invasion, which began after a series of cyber attacks, was so unexpected for the state leadership and so effective for the enemy. The effectiveness of domestic cyber defense actors at the beginning of this stage of hostilities left much to be desired. The formation of a new state strategy of cyber defense, which provided for the formation of cyber troops, on the eve of these events did not allow to fully resolve urgent issues with the formation of their personnel potential. In addition, the interaction of the military with existing subjects of cyber units would not allow to conduct defense cyber operations, military computer intelligence, combat use of information systems, conducting information operations in computer systems, or strategic information operations (which are not at all allow the expansion of the range of subjects of interaction in view of the need to preserve state and military secrets).

Therefore, in the conditions of martial law in Ukraine, there is an urgent need to find effective approaches to the recruitment of cyber troops units and the earliest possible start of their operation.

Recent publications review. The personnel policy of Ukraine regarding the training of specialists for various subjects of cyber defense was formed with an inherent national feature, which can be characterized as interdepartmental disparity and the absence of the necessary comprehensive state approach. At the same time, the borrowing of international experience can be characterized as having a fragmentary nature.

The issue of providing the personnel potential of domestic subjects of cyber units at various times was investigated in their works by scientists: M. Butuzov, A. Volobuev, V. Havlovskiy, V. Golubev, M. Gutsalyuk, K. Ismailov, V. Kudinov, M. Litvinov, O. Manzhai, A. Marushchak, L. Palamarchuk, S. Pekarskiy, K. Titunina, V. Khakhanovskiy, V. Tsimbalyuk, V. Chernei, S. Chernyavskiy, V. Shelomentsev and others.

However, the modern aspects of staffing cyber troops of Ukraine under martial law remain unexplored. Also, taking into account the novelty of the issue, there is a lack of works devoted to the formation of a personnel reserve and the strengthening of cyber protection and cybercrime countermeasures existing in Ukraine by specialists in the field of information technologies. All this determines the relevance of this article and determines its purpose.

The article's objective. The article is devoted to the study of issues of staffing of the cyber forces of Ukraine in the conditions of martial law and ways of solving problematic issues related to them at the stage of formation of the legal field.

Discussion. Russia's full-scale invasion of Ukraine was preceded by a series of global cyberattacks on our cyber infrastructure. About 100 government and state information resources and systems were attacked. In fact, we got a full-scale cyber war, which in the previous 8 years had a preparatory period on the part of the aggressor and many cyber attacks in relation to our country.

Anticipating such a scenario of development of events, certain measures were taken by state leaders. Thus, during 2021, a number of regulatory acts were issued. Among them are Decree of the President of Ukraine dated August 26, 2021 No. 446/2021 "On urgent measures for state cyber defense" and Decree of the President of Ukraine dated August 26, 2021 No. 447/2021 "On the Cybersecurity Strategy of Ukraine" [1, 2].

The specified normative acts introduced the creation of cyber troops in Ukraine. The recruitment of specialists in the field of IT was started in various forms: from anonymous through specialized chat-bots to centralized questionnaires with the formation of an appropriate database of specialists [3]. Although cyber troops will be part of the Ministry of Defense after the adoption of the relevant law, future cyber fighters are planned to be distributed among various structures responsible for cyber security: Security Service of Ukraine, State Special Communications, Cyber Police, National Security and Defense Council, National Bank of Ukraine, Ministry of

Digital Transformation, Ministry of Defense, Armed Forces of Ukraine and intelligence.

It should be emphasized that among the main reasons that led to the implementation of the initiative of specialists in the creation of cyber security in Ukraine is definitely the aggression of the russians in cyberspace in relation to our country, as well as the gradual and steady integration of the country into the alliance with NATO and the European Community. However, it is appropriate to note that the creation of cyber troops in the state and ensuring their effective functioning is not a matter of months, but of years. Yes, the United States Cyber Command or USCYBERCOM was officially formed in 2009, and unofficially – at least 20-30 years ago. The main tasks of USCYBERCOM are the centralized conduct of cyber warfare operations, management and protection of US military computer networks [4]. That is, the preparatory period for the official appearance took a period that Ukraine, taking into account the realities of the military situation, cannot afford. Currently, the US has 9,000 cyber troops, the UK has about 2,000, and russia has about 1,000.

At the start, according to various assessments of experts, the quality of the domestic cyber defense system during the war ranged from sufficient (in the eyes of government sector experts) to unsatisfactory (in the opinion of independent experts). In these conditions, the message that the help of IT specialists and the initiative implemented by the state would be extremely relevant is unconditional. However, in fact, we have a situation in which only dozens of specialists out of thousands who submitted questionnaires are involved in cooperation. The question arises why such a situation has arisen? Why have extremely valuable specialists for the country been in the deaf "reserve" for a year already, who cannot find a direct application to counter the enemy in cyberspace? Or are there not enough curators from the representatives of the state sector at specialized entities, or was the purpose of the questionnaire exactly the same as it was declared? There is a picture of establishing cooperation with representatives of the population. By the end of 2022, the result is minimal from possible.

Another problem became clear on the eve of a full-scale invasion. This is the opening of criminal proceedings against the most qualified domestic IT specialists who offered their services to the state in order to fight against scammers. After several attempts to establish constructive interaction and join forces with the relevant state structures, they were at least demoralized, and in fact neutralized in this direction [5]. A typical example of this is the Ukrainian Cyber Alliance (UKA) [6]. One of the co-founders of the company stated that after such actions on the part of the state authorities, the cyber alliance will not make any night calls for help, there will be no publications, there will be no consultations day and night for various state law enforcement agencies. Cooperation stopped [7]. Among the non-state entities that have declared war on the russian authorities is also the international hacker network Anonymous [8]. Currently, it also operates independently, demonstrating its unconditional effectiveness in the enemy's cyberspace [9].

During the years of military confrontation with Russia, we have many shameful facts of sabotage, collusion and treason on the part of representatives of various branches of the state sector (the non-military surrender of Crimea, the Ilovai cauldron for volunteer battalions, demining of passages to the Kherson region, storage of javelins in warehouses instead of the front line in February, 2022, etc.), which will receive their legal assessment after victory [10]. As for the protection of representatives of the Ukrainian Cyber Alliance from criminal prosecution, such attempts by representatives of the legislative authority have already taken place [11]. In our opinion, the situation requires immediate measures of influence on the part of international partners, who during the period of martial law actually ensure the existence of Ukraine as a state with their help.

The reason is that the sphere of cyber defense of the state in Ukraine, due to its specificity, is extremely conservative, closed and practically inaccessible for control by the domestic public. Undoubtedly, one of the possible options for the cooperation of cyber specialists with law enforcement structures can be implemented within the framework of confidentiality [12]. However, the specified examples so far testify to the opposite. In any case, the Ukrainian experience shows that the state system and bureaucracy do not allow state structures to be as mobile, operational and use social networks as patriotic hacker organizations [13, p. 120].

In the conditions of the continuation of military mobilization, a certain number of specialists in the field of information technologies will enter the ranks of the armed forces of Ukraine, for whom, in view of the state interest, the computer is a more rational weapon than any other. The mechanism of identifying and attracting such specialists to cyber troops or its reserve should work to prevent their possible loss on the battlefield.

According to O. Reznikov, cyber troops cannot be staffed through military commissars. Because they must have a high level of training and a high monetary maintenance, which corresponds to the market salaries of IT specialists, plus a social package, in order to be willing to serve in these troops. At the same time, he points out that Ukraine has a personnel reserve from which cyber troops can be formed, but it is not possible to limit oneself only to active military [14].

In our opinion, the above should be considered taking into account that the previous Cyber Security Strategy of 2016 had a number of gaps, and only 40 % of its goals were implemented. Therefore, corrections should be made to the Strategy Implementation Plan for 2021 based on the results of the activities of cyberspace entities, taking into account our achievements and experience gained even before the end of hostilities with the aggressor. Only then will Ukraine, as one of the main subjects of modern cyber warfare, have a chance not only to form its cyber armies, but also to become a trend of progressive changes in the formation of new international structures of collective security, including in cyberspace.

Conclusions. Therefore, it should be stated that staffing the future units of the cyber forces of the Ministry of Defense of Ukraine is one of the main components of the state's security in the period of military confrontation with the enemy, and the effectiveness of cyber forces is the key to victory over the enemy in cyberspace. At this stage, efficiency should be realized through constructive cooperation of law enforcement and military structures with the population – in our case, specialists in the IT field. However, the pace of development of the national draft law on the creation of cyber troops significantly lags behind the successes of the Armed Forces at the front, namely its adoption, entry into force and further implementation of the provisions in practice risks taking place already after Ukraine's victory over racism. Therefore, in our opinion, in the absence of legal norms, within the framework of which the Ukrainian cyber forces will eventually operate, at the current stage we can only talk about the formation of a personnel reserve, which in turn should be temporarily attached to the existing subjects of cyber defense of the state and go through their first stage of professional development.

Conflict of Interest and other Ethics Statements

The author declares no conflict of interest.

References

1. Указ Президента України від 26 серпня 2021 року №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави». URL : <https://www.president.gov.ua/documents/4462021-40009>.
2. Указ Президента України від 26 серпня 2021 року №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». URL : <https://www.president.gov.ua/documents/4472021-40013>.
3. Українців запросили долучитися до кібервійськ – заступник секретаря РНБО. URL : <https://fakty.com.ua/ua/ukraine/suspilstvo/20220217-ukrayincziv-zaprosyly-doluchytysya-do-kibervijsk-zastupnyk-sekretarya-rnbo/>.
4. РНБО видала розпорядження створити Кібервійська в Україні. Що це буде? URL : <https://www.ukrinform.ua/rubric-technology/3316171-rnbo-vidala-rozporadzenna-stvoriti-kibervijska-v-ukraini-so-ce-bude.html>.
5. Об украинских хактивистах, кибервойне и уязвимостях в госсекторе. Интервью с членом Ukrainian Cyber Alliance Андреем Барановичем. URL : <https://dou.ua/lenta/interviews/story-of-ukrainian-cyber-alliance/>.
6. Украинский киберальянс. URL : https://ru.wikipedia.org/wiki/%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D1%8F%D0%BD%D1%81.
7. Український киберальянс припиняє діяльність в Україні. URL : <https://sensor.net/ua/n3178085>.
8. Хакери Anonymous 3 березня обіцяють спустошити рахунки росіян і направити кошти на ЗСУ. URL : <https://uagit.tv/2022/2/28/16206-hakery-anonymous-3-bereznua-obitsyaout-spustoshyty-rahunky-rosiyan-i-naprayty-koshty-na-zsu-video>.
9. Хакери Anonymous збільшили атаки на офіційні сайти російських органів влади у два три рази. URL : <https://uagit.tv/2022/3/19/16641-hakery-anonymous-zbilshly-ataky-na-ofitsiyni-saytu-rosiyskyh-orhaniv-vlady-u-dva-try-razy>.
10. Рижков Е. В. Протидія корупції в ОВС / Е. В. Рижков, Є. А. Манченко. *Науковий вісник ДДУВС*. 2015. № 3. С. 19-24.
11. В ЕС требуют от власти прекратить преследование Украинского киберальянса. URL : <https://www.5.ua/ru/polytyka/v-es-trebuiut-ot-vlasty-prekratyt-presledovanye-ukraynsko-ho-kyberaliansa-209613.html>.

12. Рыжков Э. В., Маклаков Г. Ю. Особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий. Використання сучасних досягнень криміналістики у боротьбі зі злочинністю: Матеріали міжвузівської науково-практичної конференції студентів, курсантів і слухачів (м. Донецьк, 12 квітня 2002 року). Донецьк: ДІВС. 2002. С. 19-29.

13. Валушко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2016. 3/4(31-32). С. 117-124.

14. Нові кібервійська: де взяти гроші і як забезпечити кадрами? URL : dw.com/uk/нові-українські-кібервійська-де-взяти-на-них-гроші-і-як-забезпечити-кадрами/a-59028269.

Submitted: 29.11.2022

1. Ukaz Prezidenta Ukrayini vid 26 serpnya 2021 roku №446/2021 Pro rishennya Radi nacionalnoyi bezpeki i oboroni Ukrayini vid 14 travnya 2021 roku "Pro nevidkladni zahodi z kiberoboroni derzhavi" [Decree of the President of Ukraine ... "On urgent measures for cyber defense of the state"]. URL : <https://www.president.gov.ua/documents/4462021-40009>. [in Ukr.].

2. Ukaz Prezidenta Ukrayini vid 26 serpnya 2021 roku №447/2021 Pro rishennya Radi nacionalnoyi bezpeki i oboroni Ukrayini vid 14 travnya 2021 roku "Pro Strategiyu kiberbezpeki Ukrayini" [Decree of the President of Ukraine ... "On Cyber Security Strategy for Ukraine"]. URL : <https://www.president.gov.ua/documents/4472021-40013>. [in Ukr.].

3. Ukrayinciv zaprosili doluchitsya do kibervijsk – zastupnik sekretarya RNBO [Ukrainians were invited to join the cyber troops – 1 Deputy Secretary of the National Security Council]. URL: <https://fakty.com.ua/ua/ukraine/suspilstvo/20220217-ukrayincziv-zaprosyly-doluchytysya-do-kibervijsk-zastupnyk-sekretarya-rnbo/>. [in Ukr.].

4. RNBO vidala rozporjadzhennya stvoriti Kibervijska v Ukrayini. Sho ce bude? [The National Security Council issued an order to create a Cyber Army in Ukraine. What will it be?]. URL : <https://www.ukrinform.ua/rubric-technology/3316171-rnbo-vidala-rozporadzhennya-stvoriti-kibervijska-v-ukraini-so-ce-bude.html>. [in Ukr.].

5. Ob ukrainskih haktivistah, kibervojne i uyazvimostyah v gossektore. Intervyu s chlenom Ukrainian Cyber Alliance Andreem Baranovichem [About Ukrainian hacktivists, cyber warfare and vulnerabilities in the public sector. Interview with Ukrainian Cyber Alliance member Andrey Baranovych]. URL: <https://dou.ua/lenta/interviews/story-of-ukrainian-cyber-alliance/>.

6. Ukrayinskij Kiberalyans [Ukrainian Cyber Alliance]. URL: <https://ru.wikipedia.org/wiki/%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%81%D0%BA%D0%B8%D0%B9%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D1%8F%D0%BD%D1%81>.

7. "Ukrayinskij kiberalyans" pripinyaye diyalnist v Ukrayini ["Ukrainian Cyber Alliance" ceases its activity in Ukraine]. URL: <https://censor.net/ua/n3178085>.

8. Hakeri Anonymous 3 bereznaya obicyayut spustoshiti rahunki rosiyan i napraviti koshti na ZSU [Since March, Anonymous hackers have promised to empty the accounts of russians and send funds to the Ukrainian Armed Forces]. URL : <https://uagit.tv/2022/2/28/16206-hakery-anonymous-3-bereznaya-obitsyayut-spustoshity-rahunky-rosiyan-i-napravyty-koshty-na-zsu-video>. [in Ukr.].

9. Hakeri Anonymous zbilshili ataki na oficijni sajti rosijskih organiv vladi u dva-tri razi [Hackers Anonymous increased attacks on official websites of Russian authorities by two to three time]. URL : <https://uagit.tv/2022/3/19/16641-hakery-anonymous-zbilshyly-ataky-na-ofitsiyini-sayty-rosiyskyh-orhaniv-vlady-u-dva-try-razy>. [in Ukr.].

10. Rizhkov E. V. Protidiya korupciyi v OVS / E. V. Rizhkov, Ye.A. Manchenko. *Naukovij visnik DDUVS*. 2015. No. 3. P. 19-24. [in Ukr.].

11. V EU trebuyut ot vlasti prekratit presledovanie "Ukrainskogo kiberalyansa" [EU demand from authorities to stop persecution of "Ukrainian Cyber Alliance"]. URL : <https://www.5.ua/ru/polytyka/v-es-trebuyut-ot-vlasty-prekratyt-presledovanye-ukraynskoho-kyberaliansa-209613.html>.

12. Ryzhkov E. V., Maklakov G. Yu. Osobennosti operativno-rozysknoj deyatelnosti pri rassledovanii prestuplenij v sfere vysokih tehnologij [Peculiarities of investigative activity in the investigation of criminals in the field of high technologies]. Viktoristannya suchasnih dosyagnen kriminalistiki u borotbi zi zlochinnistyu: Materiali mizhvuzivskoyi nauково-praktichnoyi konferenciyi studentiv, kursantiv i sluhachiv. Doneck, 12.04.2002. Doneck: DIVS. 2002. P. 19-29.

13. Valyushko I. O. Kiberbezpeka Ukrayini: naukovy ta praktichni vimiri suchasnosti [Cyber security of Ukraine: scientific and practical dimensions of the 20th century]. *Visnik NTUU KPI. Politologiya. Sociologiya. Pravo.* 2016. 3/4(31-32). P. 117-124. [in Ukr.].

14. Novi kibervijska: de vzlyati groshi i yak zabezpechiti kadrami? [New cyber troops: where to get money and how to provide with staff]. URL : dw.com/uk/novi-ukrayinski-kibervijska-de-vzlyati-na-nih-groshi-i-yak-zabezpechiti-kadrami/a-59028269. [in Ukr.].

ABSTRACT

The article examines the prerequisites for the creation of cyber troops of the Ministry of Defense of Ukraine, the appearance of primary legal documents, which should in the future contribute to the development of the appropriate law and by-laws on this issue. It is emphasized that the presence in Ukraine

of a system of entities for the protection of the cyber space of the state in the conditions of martial law and in the perspective of the neighborhood with the Russian aggressor cannot fully ensure the fulfillment by the armed forces of Ukraine of their main functions regarding the protection of the country. The need to create cyber troops in the state is argued in view of their potential functionality and its difference from what is inherent in cyber defense entities already existing in Ukraine.

Attention is paid to the issues of recruiting personnel for future cyber troops. Their forms and types are noted in view of Ukrainian realities and the state of civil society. The problems of cooperation between state institutions and subjects of public initiative in the field of cyberspace protection in the state are indicated. Examples of potential and actual violations of legislation by law enforcement agencies in relation to representatives of the public cyber community are given. Approaches to the formation of the personnel reserve of cyber troops are proposed, taking into account their subjectivity. Signs of procrastination, unprofessionalism, bureaucracy, sabotage and treason on the part of representatives of state bodies, neutralization of efforts by representatives of the active cyber community, lack of proper consolidation of efforts with all sectors of society in matters of state protection in the field of information technologies are indicated.

In the course of the research, the statement that the development of the military situation in the country necessitates the need to make adjustments to the implementation plan of the Cybersecurity Strategy of Ukraine, approved in 2021, is argued in order to intensify the development of the corresponding draft law on the creation of cyber troops. It is noted that the lack of appropriate dynamics in the issue of law-making on this issue deprives the Armed Forces of Ukraine of the Ministry of Defense of the timely creation and provision of an effective tool for countering the enemy for the protection of the country. Proposals are made regarding possible approaches to the staffing of cyber troops at the preparatory and intermediate stages of the launch of this state institute.

Keywords: *Cyber Security Strategy, cyber army of the Ministry of Defense of Ukraine, personnel support of cyber army, legislative support of cyber army, cooperation of state bodies with IT specialists.*

UDC 340

DOI 10.31733/2078-3566-2022-5-60-65



Rostyslav MOLCHANOV[©]
Ph.D. (Law), Associate Professor
(Dnipropetrovsk State University
of Internal Affairs, Dnipro, Ukraine)

MUNICIPAL GUARDS IN UKRAINE: CURRENT STATE AND PROSPECTS OF ACTIVITY

Ростислав Молчанов. МУНІЦИПАЛЬНА ВАРТА В УКРАЇНІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ ДІЯЛЬНОСТІ. У статті досліджено проблему діяльності муніципальної варті в Україні та визначено перспективи її подальшої діяльності. Наголошено на тому, що поширеною європейською тенденцією сучасності є децентралізація поліції та реалізація принципу спільної відповідальності за стан публічної безпеки і порядку на території поліцейського обслуговування, що є втіленням загальної практики "Community policing". Остання успішно імплементована у діяльність поліцейських структур багатьох розвинутих країн світу.

Зроблено висновок, що це передбачає делегування окремих поліцейських функцій недержавним структурам, що дозволяє певною мірою "розвантажити" державну поліцію від розгляду і вирішення ординарних конфліктних ситуацій та типових правопорушень, що не вирізняються високим ступенем суспільної небезпеки. Для підтримання рівня правопорядку на належному рівні місцевими органами влади в Україні створюються принципово нові структури, наділені окремими поліцейськими функціями – муніципальна варта.

Обґрунтовано, що зосередження значних повноважень в межах однієї інституції на території громади матиме наслідком посилення корупційних ризиків та потенційних зловживань службовим становищем. А тому прерогативу муніципальної варті на здійснення охоронної діяльності доцільно

© Molchanov R., 2022

ORCID iD: <https://orcid.org/0000-0002-1751-9832>

appad404@gmail.com